BUKU REFERENSI

# BANKING ACCOUNTING

## IN THE DIGITAL ERA

### MODERN CONCEPTS AND APPLICATIONS

Dr. Jaime Soares, Lic-Eco., MBA (Advanced)., M.AP
Dr. Duarte Borges Loe, Lic. CSH., MA., M.Sc.
Dr. Cristino Gusmão, L.Agr.Ec., M.Ec.Dev.
Dr. Parso, S.E., M.Si., BKP.
Dr. Emi Lestari, S.E., M.M., CFP.

BUKU REFERENSI

# BANKING ACCOUNTING IN THE DIGITAL ERA

## MODERN CONCEPTS AND APPLICATIONS

**Dr. Jaime Soares, Lic-Eco., MBA (Advanced)., M.AP**
**Dr. Duarte Borges Loe, Lic. CSH., MA., M.Sc.**
**Dr. Cristino Gusmão, L.Agr.Ec., M.Ec.Dev.**
**Dr. Parso, S.E., M.Si., BKP.**
**Dr. Emi Lestari, S.E., M.M., CFP.**

# *BANKING ACCOUNTING IN THE DIGITAL ERA*
## *MODERN CONCEPTS AND APPLICATIONS*

Ditulis oleh:

**Dr. Jaime Soares, Lic-Eco., MBA (Advanced)., M.AP**
**Dr. Duarte Borges Loe, Lic. CSH., MA., M.Sc.**
**Dr. Cristino Gusmão, L.Agr.Ec., M.Ec.Dev.**
**Dr. Parso, S.E., M.Si., BKP.**
**Dr. Emi Lestari, S.E., M.M., CFP.**



ISBN: 978-6347-457-88-2
IV + 241 hlm; 18,2 x 25,7 cm.
Cetakan I, February 2026

**Desain Cover dan Tata Letak:**
Melvin Mirsal

Diterbitkan, dicetak, dan didistribusikan oleh
**PT Media Penerbit Indonesia**
Royal Suite No. 6C, Jalan Sedap Malam IX, Sempakata
Kecamatan Medan Selayang, Kota Medan 20131
Telp: 081362150605
Email: ptmediapenerbitindonesia@gmail.com
Web: https://mediapenerbitindonesia.com
Anggota IKAPI No.088/SUT/2024

# FOREWORD

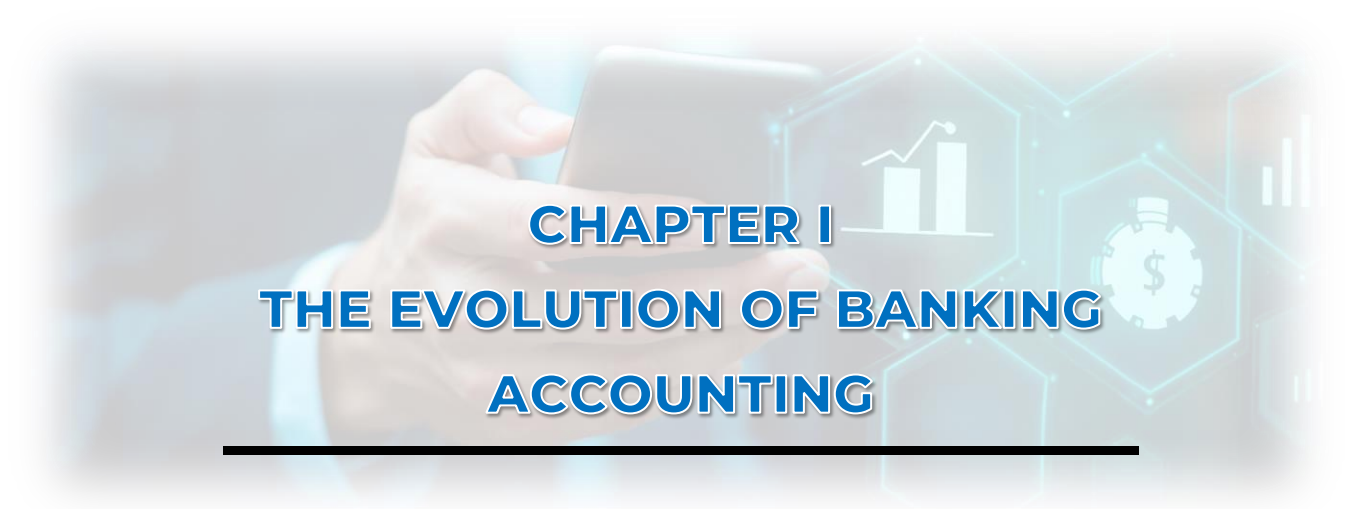
The rapid advancement of digital technology has profoundly transformed the banking industry, reshaping not only operational processes but also the fundamental practices of accounting and financial reporting. In this context, banking accounting is no longer limited to conventional recording and reporting functions; it has evolved into a strategic instrument that supports transparency, efficiency, risk management, and decision-making in an increasingly complex digital environment.

This book, Banking Accounting in the Digital Era: Modern Concepts and Applications, is designed to provide a comprehensive understanding of how accounting principles are applied within modern banking institutions amid digital transformation. It discusses both theoretical foundations and practical applications, integrating traditional banking accounting concepts with contemporary issues such as digital banking systems, financial technology (fintech), automation, data analytics, regulatory compliance, and information security.

The content of this book is systematically structured to serve students, academics, banking practitioners, and policymakers who seek to deepen their knowledge of banking accounting in the digital age. By combining conceptual explanations with real-world applications, this book aims to bridge the gap between theory and practice, enabling readers to respond effectively to the challenges and opportunities arising from technological innovation in the financial sector.

It is hoped that this book will contribute meaningfully to the development of knowledge and professional competence in banking accounting, while also encouraging critical thinking and adaptability in facing the dynamic changes of the digital era. Finally, appreciation is extended to all parties who have supported the preparation of this book. May this work provide valuable insights and serve as a useful reference for its readers.

# TABLE OF CONTENTS



# CHAPTER I
# THE EVOLUTION OF BANKING ACCOUNTING

The evolution of banking accounting reflects a dynamic journey shaped by economic development, technological innovation, and regulatory transformation. From early manual ledger systems used to record simple deposit and lending activities, banking accounting has progressed into a sophisticated, technology-driven discipline that supports complex financial products, real-time digital transactions, and global financial integration. As banks transitioned from traditional branch-based operations to digital platforms, the role of accounting expanded beyond record-keeping to ensuring transparency, risk management, regulatory compliance, and strategic decision-making. Today, in an era defined by fintech, artificial intelligence, blockchain, and open banking, understanding the evolution of banking accounting is essential for grasping how financial institutions maintain trust, integrity, and stability in an increasingly digital financial ecosystem.

## A. Historical Development of Banking Accounting

The historical development of banking accounting reflects the evolution of financial institutions, technological transformations, and regulatory reforms that have shaped the modern banking landscape. From ancient ledger-keeping to cloud-based, AI-supported accounting infrastructures, banking accounting has continuously adapted to the increasing complexity of financial transactions, globalization, and digitalization. As noted by Januszewski (2025), the trajectory of accounting in banking demonstrates a shift from paper-based stewardship to a highly automated, data-driven discipline integrated with advanced information systems. This section outlines the major stages of this development across four eras: early traditional banking,

industrial and regulatory expansion, global standardization, and digital transformation.

1. **Early Foundations: Manual Ledger Accounting (Ancient Times – 19th Century)**

The earliest foundations of banking accounting can be traced to primitive record-keeping practices developed by ancient civilizations such as Mesopotamia, Egypt, and Greece. In these societies, economic activities related to loans, deposits, grain storage, and commodity exchanges were documented using clay tablets, papyrus, and parchment. According to Mattessich (2019), these early accounting records were primarily single-entry in nature and focused on stewardship—ensuring that entrusted assets were properly recorded and safeguarded. Although rudimentary, these systems introduced the fundamental idea that financial transactions must be systematically documented to support trust between parties, an essential principle in banking activities.

A transformative milestone occurred in the late medieval period with the emergence of double-entry bookkeeping, which fundamentally reshaped banking accounting. The method was formally articulated by Luca Pacioli in his seminal work *Summa de Arithmetica* published in 1494. As explained by Sangster (2020), double-entry accounting provided a logical structure in which every transaction affected at least two accounts, ensuring internal consistency through the balancing of debits and credits. This innovation was rapidly adopted by prominent European banking centers such as Venice, Florence, and later Amsterdam, where banking houses managed increasingly complex activities including deposit-taking, credit extension, interest calculation, and foreign exchange transactions. Double-entry bookkeeping enabled bankers to monitor financial positions more accurately and to assess profitability and solvency in a systematic manner.

From the seventeenth to the nineteenth century, banking accounting practices remained entirely manual, relying on handwritten journals, ledgers, and passbooks. Daily transactions were recorded by clerks in teller journals and subsequently posted to general ledgers and individual customer accounts. Loan registers tracked principal

amounts, interest accruals, and repayment schedules, while deposit passbooks served as the primary interface between banks and customers. Despite its conceptual robustness, manual accounting was highly labor-intensive and prone to human error. Reconciliation processes often took weeks or months, limiting the timeliness of financial information. Ahmad and Hassan (2024) note that the absence of standardized accounting frameworks meant that each bank developed its own ledger formats and recognition practices, shaped by local legal systems and commercial customs.

This era was characterized by strong reliance on human supervision, including dual signatures and managerial oversight, as primary internal controls. Financial reporting was infrequent typically annual or semi-annual and lacked comparability across institutions. High exposure to clerical errors and fraud further constrained the scalability of banking operations. Nevertheless, as emphasized by Nobes (2021), the manual ledger era established the conceptual backbone of modern banking accounting by embedding principles of accountability, systematic recording, and financial control, which later enabled the transition toward mechanized and digital accounting systems.

## 2. Industrialization and Regulatory Accounting (Late 19th – Mid-20th Century)

The late nineteenth and early twentieth centuries marked a decisive transformation in banking accounting, driven by industrialization and the rapid expansion of financial institutions. The industrial revolution stimulated international trade, infrastructure development, and capital market growth, significantly increasing the scale and complexity of banking operations. Banks expanded beyond traditional deposit-taking and lending to offer services such as check clearing, trade finance, securities underwriting, and custodial services. This diversification required more sophisticated accounting systems capable of tracking large transaction volumes and multiple asset classes. As Jones and Aiken (2021) explain, ledger structures became increasingly standardized, particularly in the United Kingdom and the United States, where emerging banking laws required periodic financial reporting and greater transparency to support market confidence.

A critical feature of this era was the emergence of formal prudential regulation following severe banking crises. Events such as the Panic of 1907 in the United States and the global financial collapse during the Great Depression of 1930–1933 exposed systemic weaknesses in banking practices, including excessive leverage and inadequate risk recognition. In response, governments established central banks and supervisory authorities, such as the Federal Reserve System and strengthened banking departments in Europe. These institutions introduced minimum capital requirements, mandatory financial disclosures, standardized loan classification, and provisioning rules, as well as compulsory external audits. According to Turner (2023), these reforms institutionalized prudence as a foundational principle of banking accounting, particularly through conservative asset valuation and the systematic recognition of expected losses, which aimed to protect depositors and maintain financial stability.

Parallel to regulatory development, technological innovation began to reshape accounting operations. From the 1930s to the 1950s, banks increasingly adopted mechanical calculators, punch-card systems, and early tabulating machines to support bookkeeping and data processing. These technologies enabled faster posting of transactions, improved arithmetic accuracy, and more efficient reconciliation processes compared to fully manual systems. As Yates (2020) notes, although these machines did not eliminate human involvement, they significantly reduced clerical workload and operational errors, allowing banks to manage higher transaction volumes without proportional increases in staff.

The defining characteristics of this era included standardized national reporting formats, stronger prudential oversight, and partial mechanization of accounting processes. Operational risks related to arithmetic errors and delayed postings were reduced, yet accounting systems remained heavily dependent on manual controls and human judgment. Nevertheless, as emphasized by Macey and O'Hara (2022), the industrialization period established the regulatory and structural backbone of modern banking accounting by embedding supervisory discipline, standard reporting practices, and early automation. These developments created the institutional foundation upon which computerized and digital banking accounting systems would later be built.

### 3. Computerization, Core Banking, and Global Standardization (1970s – Early 2000s)

The period from the 1970s to the early 2000s marked a fundamental shift in banking accounting through the widespread adoption of computerized systems. The introduction of mainframe computers enabled banks to move away from paper-based bookkeeping toward fully electronic transaction processing. During this era, banks developed integrated core banking systems capable of recording deposits, managing loan portfolios, calculating interest automatically, and processing payment transactions across branches. According to Gozman, Liebenau, and Mangan (2018), computerized accounting fundamentally altered the role of accounting in banks, transforming it from a back-office recording function into a central component of operational and financial control.

A key operational innovation of this period was the shift to daily batch processing. Mainframe-based systems allowed banks to aggregate and post thousands later millions of transactions at the end of each business day. This replaced time-consuming manual postings and significantly improved both speed and accuracy. Errors could be detected through automated reconciliation routines, and account balances became more reliable and timely. The IFRS Foundation (2023) emphasizes that digital accounting systems enabled banks to transition from purely custodial record-keeping toward analytical financial management, supporting performance monitoring, risk assessment, and managerial decision-making on a much larger scale.

Alongside technological change, banking accounting became increasingly globalized through the development and adoption of international accounting standards. The establishment of the International Accounting Standards (IAS) and their evolution into International Financial Reporting Standards (IFRS) created a common financial reporting language for banks operating across borders. Key standards reshaped banking accounting practices: IFRS 7 introduced extensive disclosures on credit, market, and liquidity risks; IFRS 9 replaced incurred loss models with forward-looking Expected Credit Loss (ECL) frameworks; and IFRS 13 standardized fair value measurement across financial instruments. According to Schipper and Vincent (2024), these standards significantly enhanced transparency,

comparability, and investor confidence, but also required banks to invest in advanced valuation techniques, data infrastructure, and risk modeling capabilities.

This era also witnessed the rapid expansion of digital payment networks. The establishment of the Society for Worldwide Interbank Financial Telecommunication (SWIFT) in 1973, the proliferation of Automated Teller Machine (ATM) networks in the 1980s, and the growth of electronic funds transfer systems generated large volumes of real-time transactional data. These innovations demanded robust accounting frameworks to ensure accurate recognition, settlement, and reconciliation of interbank and customer transactions. As noted by Beccalli and Donzé (2021), the integration of payment systems with core banking platforms increased operational efficiency but also introduced new dependencies on information technology.

## 4. Digital Transformation and Intelligent Banking Accounting (2005 – Present)

Since the mid-2000s, banking accounting has undergone a profound digital transformation, evolving into an intelligent, technology-driven discipline. Modern banks increasingly operate on cloud-native and API-based platforms that enable seamless integration between core banking systems, treasury, risk management, credit engines, and customer-facing digital channels. These architectures support open banking initiatives, mobile applications, and near real-time transaction posting across multiple platforms. The Bank for International Settlements (BIS, 2024) highlights that cloud adoption significantly enhances scalability, processing speed, and cost efficiency, while simultaneously introducing new challenges related to data concentration, third-party dependency, and cyber resilience. Consequently, accounting and audit functions must now incorporate technology risk assessments into financial control frameworks.

Artificial intelligence, big data, and advanced analytics have become central to modern banking accounting. Machine learning models are widely applied in credit scoring, behavioral analytics, fraud detection, and the projection of Expected Credit Losses (ECL) under IFRS 9. Automated reconciliation tools and robotic process automation (RPA) further reduce manual intervention in high-volume accounting processes. Januszewski (2025) argues that the role of accountants has

shifted toward that of analytical supervisors and model validators, responsible for ensuring that AI-driven outputs align with accounting standards, remain explainable, and minimize embedded bias. This transformation has elevated accounting from a retrospective reporting function to a forward-looking, predictive decision-support role.

Blockchain and Digital Ledger Technology (DLT) have introduced additional complexity into banking accounting practices. The use of distributed ledgers enables immutable transaction records and supports innovations such as crypto-assets, tokenized deposits, and smart-contract-based financial products. These developments raise critical accounting questions regarding recognition, measurement, and disclosure, particularly for digital assets and automated execution of interest and fee calculations. The IFRS Foundation (2024) acknowledges that existing accounting frameworks must continue to evolve to address the unique characteristics of blockchain-based instruments, including valuation volatility, legal enforceability, and the interaction between on-chain data and traditional financial statements.

Another defining feature of this era is the shift toward real-time reporting and continuous auditing. Advanced digital infrastructures allow banks to generate intraday liquidity reports, real-time performance dashboards, and continuous control monitoring systems. Auditors increasingly rely on automated audit trails, anomaly detection algorithms, and continuous assurance models rather than solely on periodic, year-end testing. According to O'Halloran (2024), this approach enhances audit quality and timeliness while requiring new competencies in data analytics and information systems.

## B. Changing Roles of Accountants in The Digital Economy

The rapid acceleration of digital technologies such as artificial intelligence (AI), big data analytics, robotic process automation (RPA), blockchain, and cloud computing has significantly transformed the accounting profession, especially within the banking sector. As banks move toward digital-first and automation-driven operations, the role of accountants has shifted from traditional bookkeeping and compliance tasks to strategic, analytical, and technology-oriented functions. According to ACCA (2023), digital transformation has redefined accounting into a profession that integrates multidisciplinary skills,

including data literacy, digital ethics, cybersecurity awareness, and predictive analysis capabilities. This transformation is particularly evident in the banking industry, where accounting professionals must now navigate complex digital transaction environments, real-time reporting expectations, and data-intensive decision-making processes.

## 1. Shift from Manual Recording to Automation and Intelligence

Traditionally, the role of accountants in banking institutions was centered on manual bookkeeping, periodic reconciliation, regulatory reporting, and the maintenance of physical or semi-manual ledgers. These activities were labor-intensive, time-consuming, and highly dependent on human accuracy. However, the rapid advancement of automation technologies over the past two decades has fundamentally transformed this traditional role. Automation in banking accounting has replaced many repetitive, rule-based tasks with system-driven processes, significantly increasing efficiency and reliability. Moll and Yigitbasioglu (2023) emphasize that automation should not be viewed merely as task substitution, but as a comprehensive restructuring of accounting workflows that reshapes how financial information is produced, validated, and utilized within organizations.

Modern banking environments increasingly rely on intelligent automation tools such as robotic process automation (RPA), artificial intelligence (AI), and cloud-based accounting platforms. Automated reconciliation systems, for example, can instantly detect mismatches between internal records and external statements, dramatically reducing the time required for month-end or year-end closing processes. AI-based classification engines are capable of categorizing transactions in real time based on historical patterns and predefined accounting rules, minimizing manual intervention and reducing classification errors. According to Appelbaum, Kogan, and Vasarhelyi (2024), these technologies enhance data accuracy and consistency while enabling accountants to focus on exception handling rather than routine processing.

Cloud-based accounting platforms further accelerate this transformation by allowing multi-branch and multinational banks to synchronize financial data across locations in real time. Transactions

initiated in one branch or digital channel are immediately reflected in centralized accounting systems, supporting up-to-date financial reporting and integrated risk monitoring. This real-time data accessibility improves management responsiveness and strengthens internal control mechanisms. As noted by Deloitte (2023), cloud-enabled accounting infrastructures also support scalability and flexibility, allowing banks to adapt quickly to changing transaction volumes and regulatory requirements.

**2. Accountants as Data Analysts and Strategic Advisors**

In the digital economy, the role of accountants in banking institutions has expanded far beyond traditional financial reporting and compliance. The integration of big data analytics, artificial intelligence, and advanced information systems has transformed accountants into data-driven financial analysts and strategic advisors. Modern banks generate vast volumes of structured data from core banking systems and payment platforms, as well as unstructured data from customer interactions, digital channels, and external market sources. Within this environment, accountants are increasingly expected to extract meaningful insights from complex datasets to support informed managerial and strategic decision-making. According to Warren, Moffitt, and Byrnes (2023), analytical competence has become a core professional requirement, as accounting value now lies in interpretation and insight rather than mere data compilation.

One of the most significant areas in which accountants contribute as analysts is credit risk management. Predictive analytics models, often powered by machine learning, are used to assess borrower behavior, probability of default, and loss severity under various economic scenarios. Accountants play a crucial role in interpreting these model outputs, ensuring that assumptions are consistent with accounting standards such as IFRS 9, and that Expected Credit Loss (ECL) estimates are reasonable and transparent. As noted by Brown-Liburd, Issa, and Lombardi (2024), professional judgment is essential in translating complex statistical results into accounting estimates that are understandable to management, regulators, and investors.

In addition, real-time financial dashboards have become central tools for performance monitoring and liquidity management in digital banking. Accountants are increasingly involved in evaluating these

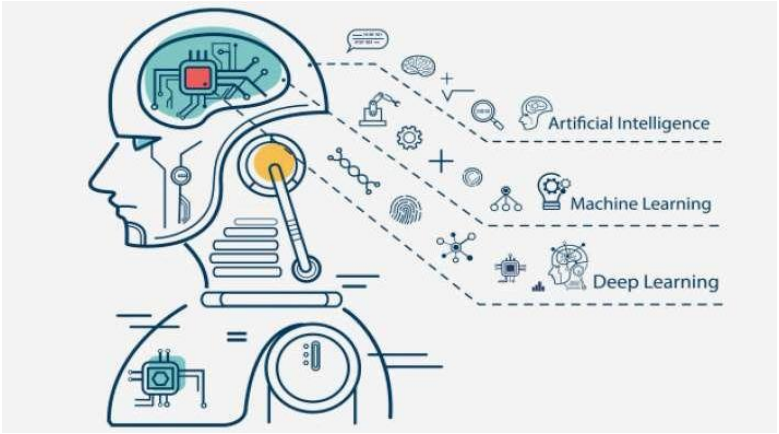
dashboards, identifying anomalies, and explaining variances in profitability, cost efficiency, and capital utilization. The ability to contextualize real-time metrics within broader financial and regulatory frameworks enhances the strategic relevance of the accounting function. McKinsey (2023) emphasizes that banks with analytically skilled accounting teams are better positioned to respond quickly to market volatility and regulatory changes.

### 3. Rise of Digital Ethics, Cybersecurity, and Governance Responsibilities

As banking accounting and financial reporting become increasingly digitized, the professional responsibilities of accountants have expanded into areas of digital ethics, cybersecurity, and technology governance. Traditional ethical concerns such as accuracy, objectivity, and compliance with accounting standards are now accompanied by new risks arising from cyber fraud, digital identity manipulation, and algorithm-driven decision-making. In highly automated banking environments, financial information is generated, processed, and reported by interconnected systems, making trust in data and algorithms a central concern. This shift requires accountants to engage actively in safeguarding digital integrity, not merely verifying numerical correctness.

One critical responsibility is the verification of data provenance within automated accounting systems. Modern banks rely on complex data pipelines that aggregate information from multiple internal and external sources, including APIs, cloud platforms, and third-party service providers. Accountants must ensure that data inputs are complete, authorized, and traceable throughout the processing lifecycle. According to IFAC (2022), maintaining reliable audit trails and validating the origin and transformation of data are essential to preserving confidence in automated financial reporting. Without such controls, even technically accurate reports may be undermined by questions about data authenticity.

Figure 1. Artificial Inteligence




Sumber: *Codepolitan*

Another emerging ethical challenge relates to the use of artificial intelligence in financial decision-making. AI-driven models influence credit approvals, Expected Credit Loss (ECL) estimates, fraud detection, and performance measurement. While these systems can enhance efficiency and consistency, they also introduce risks of algorithmic opacity and bias. Accountants are increasingly expected to evaluate the transparency and explainability of AI-based outputs, ensuring that financial decisions can be justified to regulators, auditors, and affected stakeholders. As highlighted by Floridi et al. (2023), ethical AI governance requires human oversight, clear accountability, and alignment with professional values such as fairness and prudence.

**4. Accountants as Digital System Architects and Innovators**

As banking operations become increasingly dependent on advanced digital infrastructures, the role of accountants has expanded into the design, validation, and continuous improvement of digital accounting systems. Modern banks operate on complex technological ecosystems that include core banking platforms, enterprise resource planning (ERP) systems, application programming interfaces (APIs), and, in some cases, blockchain-based ledgers. Within this environment, accountants no longer function solely as end users of accounting systems; instead, they collaborate closely with information technology specialists, system vendors, and risk managers to ensure that digital infrastructures accurately reflect financial reality and comply with accounting and regulatory requirements. Quattrone (2023) argues that accountants are now instrumental in shaping digital infrastructures

because system design choices directly influence how financial information is captured, processed, and interpreted.

One key area of contribution is the design of automated journal entry logic for digital transactions. In highly automated banking environments, transactions generated by payment systems, trading platforms, or digital channels must be translated into accounting entries without manual intervention. Accountants define recognition rules, account mappings, and posting logic to ensure consistency with accounting standards and internal policies. According to Granlund and Malmi (2022), errors in system configuration can lead to systematic misstatements, making accounting expertise essential during system design and implementation phases rather than only at the reporting stage.

Accountants are also increasingly involved in validating blockchain-based and smart contract–driven financial processes. Smart contracts can automatically execute interest payments, fees, or collateral transfers based on predefined conditions. While technically efficient, these mechanisms raise accounting questions related to timing, measurement, and legal enforceability. Accountants assess whether smart contract logic aligns with substance-over-form principles and whether on-chain transactions can be reliably integrated into off-chain financial statements. The IFRS Foundation (2024) highlights that professional judgment remains critical in interpreting automated financial flows generated by distributed ledger technologies.

## C. From Traditional to Technology-Driven Financial Reporting

Financial reporting in the banking industry has undergone a profound transformation due to advancements in digital technologies. What was once a linear, manual, and document-driven process has now evolved into an integrated, automated, and data-intelligent reporting ecosystem. This shift is driven by innovations such as cloud computing, artificial intelligence (AI), robotic process automation (RPA), blockchain, and advanced analytics, all of which reshape how financial information is captured, processed, validated, and communicated. According to PwC (2023), technology-driven reporting is not merely an enhancement of traditional methods; rather, it is a new paradigm that

prioritizes real-time accuracy, transparency, predictive insights, and compliance automation. For the banking sector characterized by high transaction volumes, strict regulations, and rapid digitalization this transformation is particularly significant.

### 1. Evolution from Manual Processes to Automation

Traditional financial reporting in banking institutions was historically grounded in manual processes that depended heavily on human intervention. Accountants were required to input data manually from multiple transaction sources, perform spreadsheet-based calculations, reconcile balances across systems, and follow sequential validation procedures before reports could be finalized. These workflows were time-consuming, vulnerable to clerical errors, and inherently retrospective in nature. As banking activities expanded in volume and complexity particularly with the rise of digital channels manual reporting processes became increasingly misaligned with the operational realities of high-frequency, real-time transactions. According to Power (2021), the limitations of manual reporting constrained both the timeliness and reliability of financial information used for managerial and regulatory decision-making.

The transition toward automation represents a structural shift in how financial reporting is produced and consumed. Modern banking reporting systems now integrate data directly from core banking platforms, payment systems, trading engines, and risk management applications through automated data pipelines. Robotic Process Automation (RPA) and artificial intelligence (AI) tools are widely deployed to replace repetitive and rules-based reporting tasks. Moll and Yigitbasioglu (2023) emphasize that these technologies generate substantial efficiency gains by automatically extracting financial data from multiple systems, performing reconciliations and variance checks within seconds, and producing standardized financial statements with minimal human intervention. This automation significantly reduces processing time while enhancing accuracy and consistency across reporting outputs.

A key benefit of automated reporting is the acceleration of reconciliation and validation processes. Automated controls embedded within reporting systems continuously compare transaction records, general ledger balances, and external confirmations, flagging

discrepancies in real time. AI-driven analytics further enhance this capability by identifying unusual patterns or deviations that may indicate errors or emerging risks. As noted by Appelbaum et al. (2024), intelligent automation enables accountants to shift from manual error detection to exception-based review, focusing professional judgment on high-risk or non-routine issues rather than routine data checks.

## 2. Transition to Real-Time and Continuous Reporting

The rapid advancement of digital banking infrastructure has fundamentally transformed the way financial information is captured and reported. The widespread adoption of core banking systems, digital payment platforms, and API-based integrations enables banks to record transactions instantly as they occur across multiple channels. Unlike traditional environments that relied on batch processing and periodic consolidation, modern banking systems generate a continuous stream of financial data. As a result, financial reporting is increasingly shifting from periodic cycles such as monthly or quarterly reporting toward real-time and continuous reporting models that better reflect the operational reality of digital finance.

Real-time reporting allows financial data to be updated immediately following each transaction, providing near-instant visibility into account balances, revenues, expenses, and risk positions. Continuous reporting extends this concept by embedding automated controls and validation mechanisms into reporting processes, ensuring that financial information remains accurate and reliable at all times. According to Vasarhelyi and Rozario (2022), the integration of real-time reporting with continuous auditing enables banks to detect anomalies as they emerge rather than after the fact. This capability significantly enhances fraud detection, error prevention, and operational resilience in high-volume digital environments.

One of the most tangible impacts of continuous reporting is the reduction of financial closing cycle times. Traditional month-end and quarter-end closing processes often required extensive reconciliations and manual adjustments, delaying the availability of financial information. In contrast, automated reconciliations and real-time ledger updates support fast-close or even zero-day close processes, where financial statements can be produced almost immediately at period end. As noted by Alles, Kogan, and Vasarhelyi (2023), this shift improves

both efficiency and confidence in reported figures, as discrepancies are addressed continuously rather than accumulated over time.

Real-time and continuous reporting also play a critical role in regulatory compliance and supervisory oversight. Regulators increasingly expect timely access to accurate financial data, particularly in areas such as liquidity management, capital adequacy, and risk exposure. Continuous reporting systems allow banks to provide up-to-date information on key prudential metrics, supporting more proactive and data-driven supervision. The Basel Committee on Banking Supervision (BCBS, 2023) highlights that timely financial data enhances the effectiveness of stress testing and early intervention frameworks.

### 3. Integration of AI and Predictive Analytics

The integration of artificial intelligence (AI) and predictive analytics into banking reporting systems represents a fundamental shift in the nature and purpose of financial reporting. Traditionally, financial reports primarily summarized historical performance, providing backward-looking information for compliance and stewardship. In contrast, AI-enabled reporting systems transform financial reporting into a forward-looking source of financial intelligence, supporting proactive risk management and strategic decision-making. As digital banking generates vast volumes of real-time data, AI and machine learning models have become essential tools for processing complexity and extracting predictive insights from continuously evolving datasets.

AI-enabled reporting supports predictive risk modeling by analyzing historical transaction data, customer behavior, and macroeconomic indicators to estimate future financial outcomes. In credit risk management, machine learning models are widely used to assess probability of default, loss given default, and exposure at default. These outputs feed directly into Expected Credit Loss (ECL) calculations under IFRS 9, enabling more timely and risk-sensitive provisioning. According to Warren, Moffitt, and Byrnes (2023), predictive analytics enhances both the accuracy and responsiveness of financial reporting by incorporating forward-looking information rather than relying solely on realized losses.

Beyond risk modeling, AI significantly improves the automation and consistency of transaction classification and financial data tagging. Intelligent algorithms can automatically classify large volumes of digital transactions, assign appropriate accounting codes, and apply standardized reporting tags such as XBRL or iXBRL. This reduces manual intervention and minimizes classification errors, particularly in complex digital banking environments with high transaction frequency. Appelbaum, Kogan, and Vasarhelyi (2024) note that automated tagging improves data comparability and supports seamless integration between internal reporting systems and external regulatory submissions.

Predictive analytics also plays a critical role in forecasting key financial indicators, including revenue streams, liquidity positions, and capital adequacy ratios. By continuously incorporating real-time transactional and market data, AI-driven models can generate dynamic forecasts that adjust as conditions change. These capabilities enable banks to anticipate liquidity shortfalls, assess the impact of strategic decisions, and evaluate compliance with regulatory capital requirements under various scenarios. As highlighted by the Basel Committee on Banking Supervision (BCBS, 2023), forward-looking analytics strengthen banks' ability to manage risk proactively and maintain financial stability.

## 4. Blockchain and Digital Ledger Technology (DLT) in Reporting

Blockchain and Digital Ledger Technology (DLT) are increasingly recognized as transformative tools in modern financial reporting, particularly within complex and highly interconnected banking environments. At their core, blockchain-based systems introduce trust, transparency, and immutability into the recording and sharing of financial information. Unlike traditional centralized databases, distributed ledgers record transactions across multiple synchronized nodes, ensuring that once a transaction is validated and added to the ledger, it cannot be altered without collective consensus. This structural characteristic significantly enhances the reliability and integrity of financial records used for reporting and assurance purposes.

One of the most significant reporting benefits of DLT is the reduction of reconciliation requirements. In traditional banking

systems, financial reporting often involves reconciling data across multiple internal systems and external counterparties, such as subsidiaries, clearing houses, and correspondent banks. Blockchain-based ledgers create a single, shared source of truth, where all authorized participants access the same validated transaction data. According to Deloitte (2023), this shared ledger architecture can eliminate redundant reconciliations, reduce processing delays, and lower the risk of discrepancies arising from inconsistent data versions.

Smart contracts further extend the reporting capabilities of blockchain by automating key accounting processes. These self-executing programs trigger financial events—such as revenue recognition, interest accrual, or settlement—when predefined conditions are met. In reporting contexts, smart contracts can ensure consistent application of accounting rules and reduce manual intervention in transaction processing. The OECD (2022) highlights that automated execution enhances operational efficiency and minimizes human error, while also raising important considerations regarding governance, control, and alignment with accounting standards.

Another critical contribution of DLT is the creation of immutable and transparent audit trails. Every transaction recorded on a blockchain is time-stamped, cryptographically secured, and traceable from initiation to settlement. This feature strengthens both internal controls and external assurance processes by providing auditors and regulators with direct access to verifiable transaction histories. As noted by Kogan, Alles, and Vasarhelyi (2023), immutable audit trails support continuous auditing models and increase confidence in the completeness and accuracy of reported financial information.

## D. Relevance in The Era of Digital Finance

The rapid expansion of digital finance characterized by digital banking, fintech platforms, blockchain-based assets, open banking ecosystems, and real-time global financial transactions has reshaped the relevance and importance of banking accounting in modern economies. In this new era, accounting plays a critical role not only in recording economic events but also in maintaining trust, ensuring regulatory compliance, supporting innovation, and enabling the safe functioning

of increasingly digital financial systems. According to IMF (2023) and World Bank (2023), digital finance has expanded access, efficiency, and competition in financial services worldwide, but it also introduces unprecedented risks and complexities that elevate the strategic importance of accurate, technology-driven accounting mechanisms.

## 1. Accounting as the Backbone of Digital Financial Integrity

Digital finance operates within an environment characterized by high-frequency, high-volume transaction flows across multiple interconnected platforms, including mobile banking, digital payments, online lending, and digital asset exchanges. In such an ecosystem, accounting functions as the backbone of digital financial integrity by ensuring that every transaction is accurately recorded, classified, and reported in real time. Unlike traditional financial systems that relied on periodic verification, digital finance requires continuous accounting processes capable of maintaining accurate customer balances, tracking digital value transfers, and supporting automated financial outputs. Without robust accounting frameworks, the speed and complexity of digital transactions would significantly increase the risk of errors, fraud, and systemic instability.

Accurate transaction recording is fundamental to preserving trust in digital financial systems. Each digital payment, loan disbursement, interest accrual, or asset transfer must be captured precisely at the moment it occurs and reflected consistently across all relevant systems. Modern accounting engines embedded within core banking and payment infrastructures ensure that transaction data flows seamlessly from operational systems into the general ledger. According to the Basel Committee on Banking Supervision (2023), strong accounting integration is essential to maintaining confidence in payment infrastructures and credit intermediation, as even minor inconsistencies can quickly propagate across digital networks and undermine financial stability.

Traceability of digital value transfers is another critical dimension of financial integrity. Digital finance often involves complex transaction chains that span multiple institutions, platforms, and jurisdictions. Accounting systems provide structured audit trails that link each transaction to its origin, authorization, and settlement outcome. These audit trails support regulatory oversight, dispute

resolution, and fraud investigation. As noted by Kogan, Alles, and Vasarhelyi (2023), transparent and traceable accounting records are central to effective governance in digital environments, where transactions are executed at machine speed and human intervention is limited.

Maintaining accurate customer balances in real time further underscores the importance of accounting in digital finance. Customers expect instant updates to account balances and transaction histories, particularly in 24/7 digital banking environments. Accounting systems continuously reconcile inflows and outflows, ensuring that balances remain correct despite high transaction volumes. This capability is especially critical for digital wallets, instant payments, and tokenized assets, where settlement finality and balance accuracy directly affect consumer trust.

## 2. Ensuring Transparency in Digital Banking and Fintech Ecosystems

Digital banking and fintech ecosystems are built on complex networks that connect banks, fintech startups, payment service providers, e-wallet operators, peer-to-peer (P2P) lending platforms, and various third-party service providers through APIs. While this interconnected architecture enables efficiency, innovation, and financial inclusion, it also increases operational complexity and opacity if not governed by transparent and harmonized accounting practices. In such an environment, accounting transparency becomes a critical mechanism for maintaining market discipline, regulatory oversight, and public trust.

Transparency is particularly essential because digital transactions often flow across multiple platforms and entities in real time. According to the Financial Stability Board (FSB, 2022), supervisors face significant challenges in monitoring cross-platform transactions when accounting standards, data definitions, and reporting formats differ across institutions. Harmonized accounting practices help ensure that financial information generated by digital banks and fintech firms is consistent, comparable, and verifiable. This comparability allows regulators to assess systemic risk, liquidity positions, and interconnected exposures more effectively, especially as

traditional banks and fintech firms increasingly operate within the same financial value chains.

Consistent accounting rules also play a vital role in creating a level playing field between digital and traditional financial institutions. The Indonesian Financial Services Authority (OJK, 2023) emphasizes that fintech companies must adhere to accounting and reporting standards equivalent to those applied to banks when they perform similar economic functions. Without such consistency, financial statements may present distorted views of profitability, asset quality, and risk exposure. This is particularly relevant for fintech business models that rely on fee-based income, platform intermediation, or embedded finance, where revenue recognition and cost allocation can be complex and subject to managerial discretion.

High-quality and transparent financial reporting directly contributes to consumer trust and investor confidence. Digital finance users often have limited visibility into how platforms manage funds, assess credit risk, or safeguard liquidity. Transparent accounting disclosures such as clear reporting of receivables, impairments, funding sources, and capital buffers help users and investors evaluate the financial soundness of digital financial service providers. Research by Gomber et al. (2023) shows that transparency in fintech reporting is positively associated with platform credibility and long-term sustainability.

### 3. Accounting Supports Innovation in Digital Financial Products

The rapid evolution of digital finance has given rise to a wide range of innovative financial products, including crypto-assets and stablecoins, tokenized securities, Central Bank Digital Currencies (CBDCs), digital micro-lending, and embedded finance services. While these innovations expand access, efficiency, and functionality in financial markets, they also introduce significant complexity in terms of measurement, recognition, and disclosure. In this context, accounting plays a critical enabling role by providing the conceptual and technical frameworks that allow these new products to be understood, trusted, and scaled within the formal financial system.

Each digital financial innovation carries distinct accounting implications that cannot be adequately addressed using traditional models alone. The IFRS Foundation (2023) highlights that crypto-

assets, for example, often do not meet the definition of cash or financial instruments under existing standards, requiring entities to apply specialized valuation and impairment approaches. Volatility, lack of observable markets, and varying rights attached to crypto holdings demand careful judgment to ensure fair representation in financial statements. Without clear accounting guidance, the financial position and risk exposure of institutions engaging in crypto-related activities would remain opaque, discouraging institutional participation and regulatory acceptance.

Tokenized securities further challenge conventional asset classification and ownership concepts. By representing equity, debt, or real assets on distributed ledgers, tokenization blurs the boundaries between traditional securities and digital assets. According to CPA Canada (2023), accountants must assess the underlying economic substance of tokenized instruments rather than their technological form. This requires determining whether such assets should be recognized as financial instruments, intangible assets, or inventory, as well as how rights, control, and transferability are evidenced in blockchain-based environments. Accounting frameworks thus provide the analytical tools needed to translate technological innovation into standardized financial reporting.

Smart contracts introduce another layer of complexity by automating contractual obligations, payments, and settlements based on predefined conditions. From an accounting perspective, these automated executions still represent enforceable economic obligations that must be recognized and measured appropriately. IFRS Foundation (2023) emphasizes that the use of smart contracts does not eliminate the need for professional judgment; instead, accountants must ensure that revenue recognition, expense matching, and liability recognition reflect the underlying economic reality of automated transactions.

CBDCs represent a further frontier in digital finance innovation, particularly for central banks and regulated financial institutions. The introduction of national digital currencies requires new accounting treatments for digital currency reserves, settlement balances, and liquidity management. Proper accounting frameworks are essential to integrate CBDCs into existing monetary and financial reporting systems without undermining transparency or comparability.

## 4. Strengthening Consumer Protection and Market Stability

The rapid expansion of digital finance has transformed how consumers interact with financial services, offering greater convenience, speed, and accessibility. However, this transformation also exposes consumers and financial markets to new and complex risks, including unauthorized digital transactions, algorithmic credit decisions, data privacy breaches, and increasingly sophisticated forms of digital fraud and cyberattacks. In this environment, robust accounting systems play a critical role not only in financial reporting but also in strengthening consumer protection and safeguarding overall market stability.

Accurate and timely accounting information forms the foundation of consumer trust in digital financial services. In highly automated systems, consumers rely on accounting records to ensure that their balances are correct, transactions are properly authorized, and fees are transparently disclosed. Automated accounting platforms enable real-time balance updates, detailed transaction histories, and immediate reconciliation of digital payments, reducing the likelihood of disputes and undetected errors. According to the OECD (2022), transparent and reliable accounting records are essential for protecting consumers in digital financial ecosystems where transactions occur continuously and at high volume.

Accounting systems also contribute to fair and responsible algorithmic decision-making, particularly in digital credit and lending platforms. Algorithmic credit scoring models depend on high-quality, well-structured financial data generated by accounting systems. When accounting data are accurate and consistently classified, they support more reliable credit assessments and reduce the risk of discriminatory or biased lending outcomes. Conversely, poor data quality can amplify model risk and undermine consumer protection. As noted by the Financial Stability Board (FSB, 2023), strong data governance and accounting controls are critical to ensuring that automated financial decisions remain transparent, explainable, and aligned with regulatory expectations.

In addition, modern accounting infrastructures increasingly incorporate advanced analytics for fraud detection and cyber risk management. By embedding anomaly detection tools and continuous monitoring into accounting processes, financial institutions can identify

unusual transaction patterns, unauthorized access, or potential cyber intrusions in real time. This proactive approach allows banks and fintech firms to intervene quickly, limiting consumer losses and preventing localized incidents from escalating into systemic disruptions. Such capabilities demonstrate how accounting has evolved from a passive record-keeping function into an active line of defense against digital financial crime.

# CHAPTER II
# BANKING INDUSTRY ECOSYSTEM AND REGULATORY FRAMEWORK

The banking industry ecosystem operates within a highly interconnected environment shaped by financial institutions, technological advancements, and regulatory authorities that ensure stability, transparency, and trust. As banks evolve from traditional branch-based models into digitally integrated platforms, the complexity of their operations increases, requiring strong governance mechanisms and comprehensive regulatory frameworks. National and international regulators such as OJK, Bank Indonesia, the Basel Committee, and the IFRS Foundation play a crucial role in establishing standards for risk management, financial reporting, and consumer protection. In the digital era, rapid innovation in payments, open banking, and financial technology has intensified the need for digital compliance tools and Regulatory Technology (RegTech) to support real-time monitoring and adaptive oversight. Understanding the structure, functions, and regulatory landscape of the banking ecosystem is essential for navigating modern financial systems and ensuring the resilience of digital banking operations.

## A. Structure and Types of Financial Institutions

Financial institutions form the backbone of the modern financial system, facilitating capital flow, managing risks, enabling payment systems, and supporting economic growth. The structure of financial institutions has evolved significantly in the digital era, integrating traditional banking models with innovative fintech-driven platforms. According to Mishkin & Eakins (2023), financial institutions can be broadly categorized into depository institutions, non-depository

institutions, investment intermediaries, insurance companies, and digital-native financial entities such as fintech firms and neobanks. Each type of institution plays a distinct role within the financial ecosystem, interactively contributing to credit allocation, liquidity creation, and financial stability. The following sections describe the main categories of financial institutions and their functions in contemporary banking environments.

### 1. Depository Institutions

Depository institutions form the core of the modern financial system by accepting deposits from the public and channeling these funds into loans and other financial services. Their primary function is financial intermediation mobilizing savings and allocating capital to households, businesses, and governments. Because they safeguard public funds and play a critical role in payment systems and credit creation, depository institutions are subject to stringent regulation and supervision. Their stability is closely linked to overall financial system resilience, monetary policy transmission, and economic growth.

Commercial banks represent the largest and most comprehensive category of depository institutions. They offer a wide range of services, including demand and time deposits, consumer and corporate lending, payment and settlement services, trade finance, and increasingly, wealth management and digital banking solutions. According to Rose and Hudgins (2022), commercial banks act as the primary intermediaries between surplus units such as households and firms with excess funds and deficit units that require financing for consumption, investment, and expansion. In contemporary economies, commercial banks also play a strategic role in supporting small and medium-sized enterprises (SMEs), facilitating international trade, and implementing monetary policy through credit channels. The digital transformation of commercial banks has further expanded their reach, allowing them to operate across borders and deliver real-time financial services while maintaining compliance with prudential regulations.

Savings banks constitute another important type of depository institution, traditionally oriented toward mobilizing household savings and financing long-term needs, particularly housing and local development. Historically, savings banks were established to promote thrift among the general population and to provide secure savings

instruments. Although financial liberalization and competition from commercial banks have reduced their prominence in some jurisdictions, savings banks continue to play a vital role in many regions. The European Central Bank (2023) emphasizes that savings banks contribute significantly to regional financial inclusion by serving local communities, small businesses, and households that may be underserved by large commercial banks. Their strong regional focus and relationship-based banking model help stabilize local economies, especially during periods of financial stress.

**2. Non-Depository Financial Institutions**

Non-depository financial institutions (NDFIs) play a vital role in modern financial systems by providing financial intermediation without accepting traditional public deposits. Instead of mobilizing funds through deposit accounts, these institutions rely on capital markets, insurance premiums, contractual savings, or wholesale funding to deliver financing, investment, and risk management services. As financial markets have become more complex and diversified, the importance of non-depository institutions has increased, particularly in supporting capital formation, market liquidity, and long-term investment. Although they are regulated differently from banks, NDFIs are integral to financial stability and economic development.

Finance companies represent one of the most prominent types of non-depository institutions. They specialize in providing consumer and business credit, including auto loans, installment financing, leasing, and equipment loans. Unlike commercial banks, finance companies often focus on market segments that are underserved or considered higher risk, such as small businesses, start-up enterprises, or consumers with limited credit histories. Fabozzi and Drake (2023) emphasize that finance companies thrive by using specialized credit assessment techniques and flexible underwriting standards, allowing them to respond more quickly to market demand. By expanding access to credit, finance companies contribute to consumption, entrepreneurship, and industrial productivity, although their activities require careful risk management due to higher default exposure.

Investment banks perform a fundamentally different intermediation function by connecting issuers of securities with investors in capital markets. They assist corporations and governments

in raising funds through equity and debt offerings, underwrite securities, and provide advisory services for mergers, acquisitions, and corporate restructuring. According to Saunders and Cornett (2022), investment banks are essential for capital formation and market efficiency, as they help price risk, allocate capital, and facilitate large-scale financial transactions. Their role becomes particularly significant during periods of economic expansion, when demand for investment capital and corporate restructuring increases.

Securities firms and brokerage houses support financial markets by enabling the buying and selling of financial instruments such as stocks, bonds, mutual funds, and derivatives. These institutions provide trading platforms, investment advice, and wealth management services for both retail and institutional investors. FINRA (2023) highlights that brokerage firms contribute to market transparency and efficiency by ensuring orderly trading, fair pricing, and investor protection through compliance with market conduct rules. Their technological infrastructure also supports high-frequency trading and digital investment services.

### 3. Digital and Fintech-Based Institutions

The digital revolution has reshaped the structure of the financial system by giving rise to technology-driven institutions that operate primarily through digital platforms. Unlike traditional financial institutions, these entities leverage advanced technologies such as cloud computing, artificial intelligence, big data analytics, and blockchain to deliver financial services with greater speed, efficiency, and accessibility. Digital and fintech-based institutions increasingly complement, and in some cases compete with, conventional banks by addressing unmet customer needs and reducing operational frictions.

Fintech companies represent the most diverse category within this segment. They integrate technological innovation into specific financial services to improve cost efficiency, customer experience, and process automation. Arner, Barberis, and Buckley (2022) classify fintech activities into key domains, including digital payments, alternative lending, wealth management (wealthtech), insurance technology (insurtech), regulatory technology (regtech), and blockchain-based financial services. By focusing on narrow value-chain segments, fintech firms are able to innovate rapidly and respond

to changing consumer expectations. Their solutions such as instant payments, algorithm-based investment advice, and automated compliance tools have pressured traditional institutions to accelerate their own digital transformation.

Digital banks, often referred to as neobanks, represent a more comprehensive fintech model. These institutions provide a full range of banking services such as deposits, payments, and lending without maintaining physical branch networks. Instead, they rely on mobile applications, cloud-native core banking systems, and data-driven customer analytics. According to KPMG (2023), neobanks benefit from significantly lower operating costs and enhanced customer accessibility, particularly among younger and digitally native users. However, they also face structural challenges, including achieving sustainable profitability, managing credit risk at scale, and meeting complex regulatory and compliance requirements comparable to those imposed on traditional banks.

Peer-to-peer (P2P) lending platforms constitute another important digital financial institution. These platforms connect borrowers directly with individual or institutional lenders through online marketplaces, bypassing traditional banking intermediaries. By using alternative data and digital credit assessment models, P2P platforms can expand credit access to small businesses and individuals who may be underserved by banks. Zhang et al. (2023) emphasize that P2P lending contributes to financial inclusion and competition in credit markets, although effective regulatory oversight is essential to manage default risk, consumer protection, and systemic exposure.

Crypto-asset service providers (CASPs) have emerged alongside the growth of blockchain and decentralized finance. These entities facilitate cryptocurrency trading, custody, token issuance, and related digital asset services. Their role has expanded rapidly as crypto-assets gain broader adoption for investment and payment purposes. The Financial Stability Board (FSB, 2023) highlights that CASPs introduce new risks, including cyber threats, asset price volatility, and governance challenges, necessitating robust regulatory frameworks. Collectively, digital and fintech-based institutions are redefining financial intermediation, driving innovation while simultaneously reshaping regulatory and accounting landscapes.

## 4. Islamic Financial Institutions

Islamic financial institutions constitute an important segment of the global financial system, particularly in jurisdictions with large Muslim populations and in regions where ethical and faith-based finance is increasingly valued. These institutions operate in accordance with Sharia principles, which prohibit interest (riba), excessive uncertainty (gharar), and speculative activities (maysir), while promoting risk-sharing, asset-backed transactions, and social justice. As a result, Islamic finance offers an alternative model of financial intermediation that aligns financial activities with ethical and religious values, while still supporting economic development and financial stability.

Islamic banks are the cornerstone of the Islamic financial system. Unlike conventional banks, Islamic banks do not charge or pay interest; instead, they structure financial products around profit-and-loss sharing and trade-based contracts. Common instruments include mudarabah, where one party provides capital and the other provides expertise with profits shared according to a pre-agreed ratio; murabahah, a cost-plus financing arrangement widely used for consumer and trade financing; and ijara, which is based on leasing assets. Sukuk, often referred to as Islamic bonds, represent another key instrument, allowing governments and corporations to raise funds through asset-backed structures that generate returns linked to underlying economic activities. According to the Islamic Financial Services Board (IFSB, 2023), Islamic banking assets continue to grow steadily, particularly in Southeast Asia, the Middle East, and parts of Africa, driven by supportive regulation, increasing financial inclusion, and demand for Sharia-compliant products. Islamic banks also emphasize ethical investment and social responsibility, often integrating zakat and social finance instruments into their operations.

Takaful operators represent the Islamic alternative to conventional insurance companies. Takaful is based on the concept of mutual assistance, where participants contribute to a common pool to share risks collectively rather than transferring risk to an insurer for profit. Contributions are managed according to Sharia principles, and any surplus after claims and expenses may be redistributed to participants or retained to strengthen the risk pool. Ismal and Achsani (2022) note that takaful has gained increasing popularity in Muslim-

majority countries due to its ethical foundations, transparency, and alignment with community values. Takaful products cover a wide range of risks, including health, life (family takaful), property, and business-related risks, and they play a growing role in supporting small and medium-sized enterprises and household financial security.

## B. Banking Operations and Transaction Processes

Banking operations encompass the core activities, workflows, and technological systems that enable financial institutions to deliver products and services efficiently, securely, and in compliance with regulatory standards. As banking transitions toward a fully digital ecosystem, traditional operational processes have been reengineered to support mobile banking, real-time payments, open banking APIs, and automated back-office functions. According to Heffernan (2023), modern banking operations must balance operational efficiency, customer experience, and robust risk management in an increasingly data-driven environment. Transaction processes, meanwhile, involve the end-to-end mechanisms through which financial transactions such as deposits, withdrawals, payments, transfers, and settlements are initiated, validated, executed, recorded, and monitored. These processes rely heavily on digital infrastructure, core banking systems, and compliance frameworks.

### 1. Core Functions of Banking Operations

Banking operations consist of a set of interrelated core functions that enable banks to perform their intermediary role efficiently while maintaining financial stability and customer trust. These operational functions support daily transactions, risk control, and regulatory compliance, forming the backbone of both traditional and digital banking models. According to Rose and Hudgins (2022), effective banking operations integrate funds mobilization, credit activities, payment services, risk management, treasury functions, and customer service into a cohesive operational framework.

Funds mobilization is the foundational function of banking operations. Banks collect funds from the public through various deposit instruments, including savings accounts, current accounts, and term deposits. These deposits provide banks with a stable source of funding

that supports credit creation and liquidity management. Efficient deposit mobilization allows banks to balance funding costs with interest income while maintaining sufficient liquidity buffers to meet withdrawal demands. In the digital era, online and mobile banking platforms have significantly enhanced deposit accessibility, enabling banks to attract and retain customers more effectively.

Credit operations represent the core revenue-generating activity of banks and are central to both profitability and risk management. This function involves evaluating borrower creditworthiness, assessing collateral, disbursing loans, and monitoring repayment performance. Saunders and Cornett (2022) emphasize that prudent credit operations are essential to controlling default risk and maintaining asset quality. Modern banks increasingly rely on data-driven credit scoring models and automated loan processing systems to improve efficiency while ensuring compliance with regulatory and accounting standards.

Payment and settlement services are another critical operational function. Banks facilitate a wide range of payment mechanisms, including ATM and debit card transactions, mobile and internet banking transfers, Real-Time Gross Settlement (RTGS), and national payment infrastructures such as BI-FAST in Indonesia. These systems must deliver transactions with high speed, accuracy, and security to support economic activity and customer confidence. As transaction volumes grow, operational resilience and cybersecurity have become key priorities in payment operations.

Risk management is embedded across all banking operations. Operational risk management focuses on identifying and mitigating threats such as fraud, cyberattacks, system failures, liquidity stress, and market volatility. The Basel Committee on Banking Supervision (BCBS, 2023) highlights the importance of real-time risk dashboards and continuous monitoring in digital banking environments to ensure timely detection and response to emerging risks.

Treasury and liquidity operations ensure that banks can meet short-term obligations and comply with regulatory requirements. Through interbank lending, asset-liability management, and foreign exchange operations, treasury units manage liquidity positions and interest rate exposure. These activities are essential for financial stability and effective balance sheet management.

## 2. Digital Transformation of Banking Operations

Digital transformation has fundamentally reshaped banking operations, shifting them from fragmented, manual processes into highly integrated, technology-driven systems. Advances in digital infrastructure, data analytics, and automation have enabled banks to improve efficiency, reduce operational risk, and deliver faster, more personalized services. According to Crosman (2023), modern banks increasingly operate on unified digital platforms that automate routine activities and generate real-time data flows, allowing operational decisions to be made with greater speed and accuracy.

At the core of this transformation are Core Banking Systems (CBS), which serve as centralized platforms for managing customer accounts, transactions, loans, and financial reporting. Unlike legacy systems that relied on batch processing, contemporary CBS operate on real-time architectures, ensuring that account balances, transaction records, and risk exposures are updated instantly. This real-time capability enhances transparency, supports regulatory reporting, and improves customer experience by enabling 24/7 access to banking services. Modern CBS also integrate multiple functional modules—such as treasury, credit, and risk management—creating a single source of truth for operational and accounting data.

API-based architecture has further expanded the scope of banking operations by enabling interoperability between banks, fintech companies, payment gateways, and third-party service providers. Through Application Programming Interfaces (APIs), banks can securely share data and services while maintaining control over access and compliance. This architectural shift underpins open banking and embedded finance models, allowing banks to extend their services beyond traditional channels. APIs also reduce system complexity and accelerate innovation by enabling modular system development and rapid integration of new digital services.

Artificial intelligence (AI) has become a critical enabler of intelligent banking operations. Banks increasingly deploy AI and machine learning algorithms to detect fraudulent transactions, assess credit risk, and automate customer service through chatbots and virtual assistants. These technologies enhance decision accuracy by analyzing large volumes of transactional and behavioral data in real time. As noted by Crosman (2023), AI-driven analytics allow banks to move

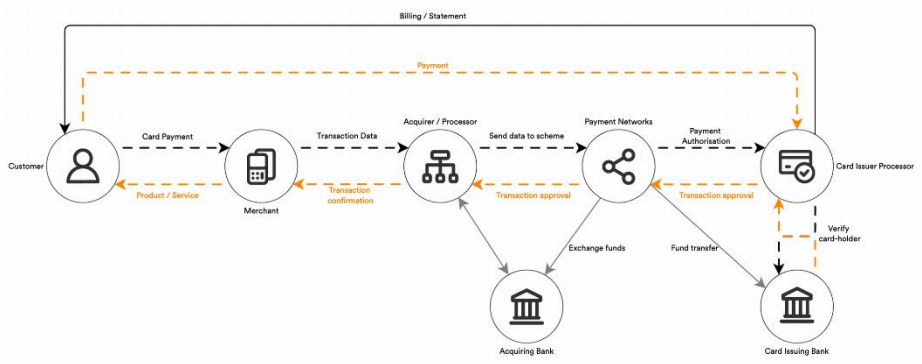
from reactive problem-solving to predictive operational management, particularly in areas such as fraud prevention and credit monitoring.

Robotic Process Automation (RPA) complements AI by automating repetitive, rule-based tasks that previously required significant manual effort. In banking operations, RPA is widely used for reconciliations, data validation, compliance checks, and report generation. By reducing human intervention in routine processes, RPA improves processing speed, minimizes errors, and allows employees to focus on higher-value activities such as risk analysis and customer relationship management.

## 3. Banking Transaction Processes

Transaction processing lies at the heart of banking operations, ensuring that the movement of funds and financial information occurs accurately, securely, and efficiently. In modern banking, each transaction follows a structured lifecycle that integrates technology, risk controls, and accounting validation. According to contemporary banking operations frameworks, a typical transaction proceeds through several key stages: initiation, authentication and authorization, processing and validation, clearing, settlement, and reconciliation.

Figure 2. Banking Transaction Processes




Sumber: *Money.com*

Transaction initiation marks the beginning of the process and occurs when a customer or institution requests a financial action. This can take place through multiple channels, including mobile banking applications, ATM machines, branch counters, internet banking platforms, or API-based requests such as e-commerce and embedded finance payments. The proliferation of digital channels has significantly increased transaction volumes and frequency, requiring banks to

support 24/7 availability and seamless user experiences while maintaining operational resilience.

Once a transaction is initiated, banks perform authentication and authorization to verify the identity of the user and confirm their permission to execute the transaction. Authentication mechanisms include passwords or PINs, biometric identifiers such as fingerprints or facial recognition, one-time passwords (OTPs), and digital certificates. The National Institute of Standards and Technology (NIST, 2023) emphasizes the importance of multi-factor authentication in digital banking to reduce the risk of unauthorized access and identity fraud. Effective authentication safeguards both customers and financial institutions against cyber threats.

Following authentication, the transaction enters the processing and validation stage within the core banking system. At this point, the system verifies account balances, transaction limits, and applicable compliance rules, including anti-money laundering (AML) and counter-financing of terrorism (CFT) requirements. Modern banks increasingly employ AI-powered validation tools to analyze transaction patterns and detect anomalies in real time, enabling early identification of potential fraud or suspicious activities before transactions are finalized.

Clearing is the next stage, involving the exchange of transaction information between financial institutions. This process determines the obligations of each participating bank and prepares transactions for final settlement. Clearing can occur through national clearing systems, payment gateway providers, or international card networks such as Visa and Mastercard. Efficient clearing mechanisms are essential for handling high transaction volumes and ensuring interoperability across different banking and payment platforms.

Settlement represents the actual transfer of funds between banks, completing the financial obligation. Settlement can occur through Real-Time Gross Settlement (RTGS), where transactions are settled individually and immediately, or Deferred Net Settlement (DNS), where transactions are aggregated and settled at specific intervals. The Bank for International Settlements (BIS, 2023) underscores the importance of settlement finality in minimizing systemic risk and preventing cascading failures within the financial system.

## 4. Retail vs Wholesale Banking Operations

Banking operations can be broadly categorized into retail and wholesale segments, each serving different customer groups and requiring distinct operational processes, risk management approaches, and technological infrastructures. While both segments rely on the same core banking principles, their scale, complexity, and service orientation differ significantly. Understanding these differences is essential for effective operational design and strategic management within banks.

Retail banking operations focus on providing financial services to individual consumers and small businesses. Key activities include deposit operations, consumer loan processing, card issuance and management, mobile and internet banking services, and customer onboarding. Retail operations are typically characterized by high transaction volumes, standardized products, and relatively low transaction values. Digital channels dominate this segment, driven by customer demand for speed, convenience, and 24/7 access to services. According to recent banking industry studies, mobile applications and online platforms have become the primary interface between retail banks and customers, enabling instant transfers, bill payments, and real-time balance monitoring. Automation plays a central role in retail operations, with digital onboarding supported by electronic Know Your Customer (e-KYC), AI-based credit scoring for consumer loans, and automated customer service through chatbots. These technologies improve operational efficiency while enhancing customer experience and reducing processing costs.

Wholesale banking operations, in contrast, serve large corporations, governments, and other financial institutions. This segment involves fewer transactions in volume but significantly higher values and greater complexity. Wholesale banking activities include syndicated loans, corporate treasury and cash management services, trade finance, foreign exchange operations, and capital market-related services. Transactions often require customized structuring, detailed documentation, and close relationship management. Risk assessment in wholesale banking is more complex, as exposures are larger and often involve cross-border elements, multiple currencies, and counterparty risks. As a result, wholesale operations place greater emphasis on credit analysis, legal documentation, and regulatory compliance.

Technological transformation is also reshaping wholesale banking operations. According to the International Capital Market Association (ICMA, 2023), wholesale banking increasingly relies on electronic trading platforms, digital trade documentation, and automated settlement systems. Electronic platforms facilitate real-time pricing, execution, and reporting of foreign exchange and securities transactions, improving market efficiency and transparency. In trade finance, digital documentation and blockchain-based solutions are reducing processing times and fraud risk by enhancing data integrity and traceability. Treasury operations have similarly benefited from advanced analytics and real-time liquidity management tools, allowing corporate clients to optimize cash positions across global accounts.

## C. Regulatory Bodies (OJK, BI, Basel Committee, IFRS Foundation)

Regulatory bodies play a critical role in maintaining the stability, integrity, and transparency of the global banking system. Their responsibilities include setting prudential standards, supervising financial institutions, ensuring consumer protection, and harmonizing accounting rules across jurisdictions. In the context of Indonesia, two domestic regulatory authorities Otoritas Jasa Keuangan (OJK) and Bank Indonesia (BI) form the backbone of financial oversight. On the global level, the Basel Committee on Banking Supervision (BCBS) and the IFRS Foundation act as international standard-setters for prudential regulation and financial reporting. According to Mishkin & Eakins (2023), effective regulatory governance is essential to preventing systemic risks, promoting market discipline, and enhancing public trust in the financial system. This section provides a detailed explanation of each regulatory body, its function, and its relevance in the digital era.

### 1. Otoritas Jasa Keuangan (OJK)

The Otoritas Jasa Keuangan (OJK), or the Financial Services Authority of Indonesia, is an independent regulatory institution established under Law No. 21 of 2011 with a broad mandate to regulate and supervise the national financial services sector. OJK was created to strengthen the resilience, transparency, and integrity of Indonesia's financial system by integrating oversight across banking, capital

markets, and non-bank financial institutions. In assuming supervisory functions previously held by Bank Indonesia and Bapepam-LK, OJK plays a central role in ensuring that financial intermediation supports sustainable economic growth while safeguarding financial stability and consumer interests.

According to the OJK Annual Report (2023), one of OJK's primary responsibilities is the regulation and supervision of a wide range of financial institutions, including commercial banks, insurance companies, securities firms, pension funds, and rapidly growing fintech operators. Through prudential regulation and ongoing supervision, OJK ensures that financial institutions maintain adequate capital, manage risks effectively, and comply with sound corporate governance principles. In addition, OJK is responsible for licensing and authorization processes, covering conventional financial institutions as well as digital banks, peer-to-peer (P2P) lending platforms, and investment managers. This licensing function is critical in maintaining market discipline and preventing the entry of unqualified or high-risk entities into the financial system.

Consumer protection is another core pillar of OJK's mandate. OJK implements market conduct supervision to ensure fair treatment of consumers, transparent disclosure of financial products, and ethical business practices. It also provides dispute resolution mechanisms and promotes financial literacy and inclusion through public education programs. The OJK Annual Report (2023) emphasizes that improving consumer awareness and trust is essential, particularly as financial products become more complex and technology-driven. Furthermore, OJK enforces compliance with anti–money laundering and counter-terrorism financing (AML/CFT) regulations to protect the integrity of the financial system and align Indonesia with international regulatory standards.

In the digital era, OJK has actively adapted its regulatory and supervisory approach to address the rapid transformation of financial services. The authority has issued specific regulations for digital banks through POJK No. 12/2021 and strengthened the supervision of fintech lending under POJK No. 10/2022. These regulations aim to balance innovation with risk mitigation, ensuring that digital financial services remain safe, transparent, and inclusive. OJK has also developed digital

consumer protection frameworks to address risks related to data privacy, cyber threats, and unfair digital practices.

**2. Bank Indonesia (BI)**

Bank Indonesia (BI), as the central bank of the Republic of Indonesia, plays a pivotal role in maintaining monetary stability and safeguarding the resilience of the national financial system. Established under the Central Bank Act (Law No. 23 of 1999), BI operates as an independent institution, free from government intervention in the formulation and implementation of its policies. This independence is essential to ensure the credibility and effectiveness of monetary policy, particularly in managing inflation, stabilizing the exchange rate, and responding to macroeconomic shocks. In addition to its traditional central banking mandate, BI has expanded its role to include payment system oversight and macroprudential regulation, reflecting the increasing complexity of modern financial systems.

According to the *Bank Indonesia Policy Review* (2023), one of BI's core functions is the formulation and implementation of monetary policy. This includes setting benchmark interest rates, determining reserve requirements for banks, and conducting open market operations to manage liquidity in the financial system. Through these instruments, BI seeks to maintain price stability while supporting sustainable economic growth. Another key responsibility is the management of Indonesia's foreign exchange reserves, which serves to strengthen external resilience, stabilize the rupiah exchange rate, and ensure the country's ability to meet international payment obligations. BI is also responsible for ensuring smooth cash circulation and currency management, including the issuance, distribution, and withdrawal of banknotes and coins to maintain public confidence in the national currency.

Beyond monetary policy, BI plays a critical role in maintaining financial system stability through macroprudential regulation. Instruments such as countercyclical capital buffers, loan-to-value (LTV) ratios, and liquidity requirements are designed to mitigate systemic risks arising from excessive credit growth and financial imbalances. The *Bank Indonesia Policy Review* (2023) emphasizes that macroprudential measures complement monetary policy by targeting

risks within the financial sector, thereby enhancing the overall resilience of the banking system.

In the area of payment systems, Bank Indonesia has assumed a strategic role in modernizing national payment infrastructure in response to rapid digitalization. Initiatives such as BI-FAST provide real-time retail payment services that are fast, secure, and affordable, while QRIS (Quick Response Code Indonesian Standard) promotes interoperability across digital payment platforms. In addition, the development of SNAP (National Open API Standard for Payment Systems) facilitates seamless integration between banks, fintech firms, and merchants. Wibowo (2023) notes that these innovations significantly improve efficiency, inclusivity, and accessibility within Indonesia's payment ecosystem.

### 3. Basel Committee on Banking Supervision (BCBS)

The Basel Committee on Banking Supervision (BCBS) is a central pillar of the global regulatory architecture for banking. Established in 1974 by the central bank governors of the G10 countries and operating under the auspices of the Bank for International Settlements (BIS), the BCBS was created in response to disruptions in international banking markets. Although the Committee does not possess formal legal authority, its standards and guidelines serve as the most influential global benchmarks for prudential banking regulation. National regulators voluntarily adopt and implement Basel standards, making the BCBS a key driver of regulatory harmonization and financial stability worldwide (BCBS, 2023).

Over time, the BCBS has developed successive Basel frameworks to address evolving risks in the banking sector. Basel I, introduced in 1988, established the first internationally agreed minimum capital requirements, focusing primarily on credit risk and setting a simple risk-weighted capital ratio. Basel II, released in 2004, expanded this approach by introducing a more risk-sensitive framework built on three pillars: minimum capital requirements, supervisory review, and market discipline through enhanced disclosure. This framework encouraged banks to improve internal risk management systems and align capital more closely with underlying risks. Following the 2008 global financial crisis, Basel III was introduced between 2010 and 2017 to strengthen the resilience of banks. It significantly enhanced

the quality and quantity of capital, introduced capital conservation and countercyclical buffers, and added global liquidity standards such as the Liquidity Coverage Ratio (LCR) and Net Stable Funding Ratio (NSFR), as well as a leverage ratio to constrain excessive balance sheet expansion (BCBS, 2023). The latest refinement, often referred to as Basel IV, implemented from 2023 onward, further improves the consistency of risk-weighted assets by revising credit and operational risk models and introducing an output floor to limit excessive variability in internal model outcomes.

The overarching objectives of the BCBS are to promote global financial system stability and to ensure a consistent and level playing field across international banking systems. By establishing uniform capital adequacy rules and encouraging sound risk management practices, the Committee aims to reduce regulatory arbitrage and enhance confidence in the global banking system. Transparency and comparability of banking disclosures are also core goals, enabling market participants and supervisors to better assess bank risk profiles and resilience.

In the digital era, the BCBS continues to adapt its standards to address emerging risks associated with technological innovation. The Committee has issued principles for managing cybersecurity risks (BCBS, 2021), prudential treatments for cryptoasset exposures (BCBS, 2022), and guidance on fintech-related risks and operational resilience (BCBS, 2023). According to Le Leslé and Avdjiev (2023), these evolving Basel standards reflect the need to safeguard banks against digital-era challenges, including cyber threats, the use of artificial intelligence in risk modeling, and exposure to cryptoassets and stablecoins. Through continuous adaptation, the BCBS remains a cornerstone institution in maintaining the stability and integrity of the global banking system.

### 4. IFRS Foundation

The IFRS Foundation is an independent, nonprofit organization that plays a central role in shaping the global financial reporting landscape. Established to promote transparency, accountability, and efficiency in capital markets, the Foundation is responsible for developing and maintaining International Financial Reporting Standards (IFRS), which are applied in more than 140 jurisdictions

worldwide. By providing a single set of high-quality, globally accepted accounting standards, the IFRS Foundation enhances the comparability and reliability of financial statements across borders, thereby supporting investor confidence and financial stability (IFRS Foundation, 2023).

One of the core responsibilities of the IFRS Foundation is the development of consistent and principle-based accounting standards that respond to evolving economic and financial conditions. Through its oversight of the International Accounting Standards Board (IASB), the Foundation ensures that standards are technically sound, globally relevant, and developed through transparent due process. In recent years, the IFRS Foundation has expanded its mandate to include sustainability and climate-related disclosures by establishing the International Sustainability Standards Board (ISSB). According to the IFRS Foundation (2023), this initiative reflects growing global demand for consistent, decision-useful information on environmental, social, and governance (ESG) risks that increasingly affect enterprise value and financial performance.

In the banking sector, IFRS standards are particularly critical due to the complexity and risk sensitivity of financial institutions' balance sheets. IFRS 9 – Financial Instruments is one of the most influential standards for banks, as it governs the classification and measurement of financial assets and liabilities and introduces the Expected Credit Loss (ECL) model. Unlike the incurred loss approach used previously, ECL requires banks to recognize credit losses based on forward-looking macroeconomic scenarios, significantly enhancing the timeliness and prudence of credit risk provisioning. PwC (2023) notes that IFRS 9 has fundamentally transformed how banks measure credit risk, integrate macroeconomic data, and align accounting with risk management practices. In addition, IFRS 13 – Fair Value Measurement provides a consistent framework for valuing financial instruments, while IFRS 15 – Revenue from Contracts with Customers and IFRS 10 – Consolidated Financial Statements ensure proper recognition of income and group-level financial transparency.

As digital finance continues to evolve, the IFRS Foundation has increasingly emphasized digital reporting and emerging financial instruments. The adoption of XBRL-based digital financial reporting enables machine-readable financial statements, reducing manual errors

and improving regulatory and investor analysis. Furthermore, the Foundation has engaged in guidance development and agenda consultations related to crypto-asset accounting, reflecting the growing relevance of digital assets in financial markets. Alongside this, the ISSB has issued global sustainability disclosure standards that integrate financial and non-financial data in a digitally structured format. According to ISSB (2023), digital reporting frameworks enhance comparability, analytical efficiency, and investor decision-making, reinforcing the IFRS Foundation's role as a cornerstone of transparent and future-oriented global financial reporting.

## D. Digital Compliance and Regulatory Tech (RegTech)

The rapid digitalization of banking has transformed how financial institutions manage compliance, monitor risks, and meet increasingly complex regulatory requirements. Regulatory Technology, commonly known as RegTech, has emerged as a critical innovation enabling banks to automate compliance tasks, improve transparency, reduce operational costs, and enhance real-time monitoring. According to Arner, Barberis, and Buckley (2021), the rise of RegTech is a direct response to the post-2008 financial crisis regulatory expansion, coupled with the accelerating digital economy. In the modern banking ecosystem, RegTech integrates data analytics, artificial intelligence (AI), machine learning (ML), natural language processing (NLP), blockchain, and cloud computing to deliver efficient and scalable compliance solutions.

### 1. Definition and Purpose of RegTech

Regulatory Technology (RegTech) refers to the application of advanced digital technologies to enhance the efficiency, accuracy, and effectiveness of regulatory compliance within financial institutions. As financial systems become increasingly complex and digitalized, traditional compliance approaches often reliant on manual processes and periodic reporting have proven insufficient to address real-time risks and rapidly evolving regulatory requirements. According to the Institute of International Finance (IIF, 2023), RegTech is designed to strengthen the accuracy and timeliness of compliance activities, reduce operational burdens, and improve transparency between regulated

entities and supervisory authorities. By embedding technology directly into compliance functions, RegTech transforms regulation from a reactive obligation into a proactive and integrated risk management capability.

The primary purpose of RegTech is to automate and streamline compliance processes that were historically labor-intensive and prone to human error. Financial institutions face an expanding volume of regulatory obligations across multiple jurisdictions, covering areas such as capital adequacy, consumer protection, data privacy, and financial crime prevention. RegTech solutions leverage technologies such as artificial intelligence, machine learning, big data analytics, cloud computing, and robotic process automation to monitor transactions, validate data, and generate regulatory reports in near real time. IIF (2023) emphasizes that automation not only reduces manual intervention but also significantly enhances data consistency and auditability, which are critical for meeting supervisory expectations.

Another key objective of RegTech is enabling real-time risk identification and monitoring. Unlike traditional compliance systems that rely on ex post reviews, RegTech tools continuously analyze large volumes of transactional and behavioral data to detect anomalies and potential breaches as they occur. This capability is particularly important in high-risk regulatory domains such as anti–money laundering (AML) and combating the financing of terrorism (CFT), where delayed detection can lead to substantial financial penalties and reputational damage. Deloitte (2023) notes that AI-driven transaction monitoring systems can identify suspicious patterns more accurately than rule-based approaches, thereby improving both compliance effectiveness and risk management outcomes.

## 2. Key Drivers of RegTech Adoption in Banking

The adoption of Regulatory Technology (RegTech) in the banking sector is driven by a combination of regulatory, technological, and operational pressures that have intensified alongside digital transformation. One of the most significant drivers is increasing regulatory complexity. In the aftermath of the global financial crisis, regulators introduced comprehensive reforms such as Basel III, IFRS 9, PSD2, and GDPR, complemented by jurisdiction-specific regulations issued by authorities such as OJK in Indonesia, the Monetary Authority

of Singapore (MAS), and the European Banking Authority (EBA). These frameworks impose detailed requirements on capital adequacy, risk management, consumer protection, data privacy, and reporting transparency. Mulligan (2020) observes that banks today must manage regulatory obligations that are not only expanding in volume but also becoming more granular and dynamic, making traditional manual compliance approaches increasingly unsustainable. RegTech tools help banks interpret, map, and implement these complex rules more efficiently.

A second key driver is the massive growth of digital transactions. The widespread use of mobile banking, e-wallets, contactless payments, instant payment systems, and API-based financial services has led to exponential increases in transaction volumes and data velocity. In such environments, manual transaction monitoring and post-event compliance reviews are no longer feasible. Automated AML, CFT, and fraud detection systems powered by AI and advanced analytics have become essential to identify suspicious activities in real time. According to BIS (2023), real-time transaction monitoring is critical to preserving trust and stability in highly digitalized payment ecosystems.

Cost pressure is another major factor accelerating RegTech adoption. Compliance has become one of the largest cost centers for global financial institutions. Deloitte (2022) estimates that banks collectively spend around USD 270 billion annually on compliance-related activities, including staffing, reporting, audits, and remediation. RegTech solutions reduce these costs by automating routine compliance tasks, minimizing manual errors, and streamlining regulatory reporting processes. Automation allows banks to scale compliance operations without proportionally increasing headcount, thereby improving cost efficiency while maintaining regulatory rigor.

## 3. Components and Technologies in RegTech

RegTech is built upon a set of advanced digital components and technologies that enable financial institutions to manage regulatory compliance more effectively in complex and data-intensive environments. Among the most influential components are artificial intelligence (AI) and machine learning (ML), which have transformed how banks detect risks and regulatory breaches. AI/ML models are

capable of analyzing massive volumes of structured and unstructured data to identify anomalies, suspicious behavioral patterns, and emerging compliance risks in real time. Compared to traditional rule-based systems, ML-driven anti–money laundering (AML) tools demonstrate higher accuracy and adaptability, as they continuously learn from new data and evolving typologies. Liu et al. (2023) find that ML-based AML systems significantly outperform static rule-based approaches by reducing false positives while improving the detection of genuinely suspicious transactions. Practical applications include predictive risk scoring, real-time fraud detection, and the automated generation of suspicious activity reports (SARs), which enhance both efficiency and regulatory responsiveness.

Another critical component of RegTech is natural language processing (NLP). Regulatory frameworks are often expressed in lengthy, complex, and frequently updated legal texts, creating challenges for consistent interpretation. NLP technologies help banks extract regulatory obligations, identify relevant compliance requirements, and map them to internal policies and controls. Gomber and Koch (2021) argue that NLP-based compliance tools reduce interpretation errors by systematically analyzing regulatory language, guidance notes, and supervisory communications. As regulatory updates accelerate, NLP enables faster adaptation and ensures that compliance teams remain aligned with current rules.

Blockchain and distributed ledger technology (DLT) also play an increasing role in RegTech architectures. DLT provides immutable, transparent, and tamper-resistant records, which are particularly valuable for audit trails, transaction verification, and identity management. According to FATF (2022), several jurisdictions are exploring blockchain-based Know Your Customer (KYC) utilities that allow financial institutions to share verified customer data securely, reducing duplication, onboarding costs, and fraud risks. The immutability of blockchain records strengthens trust among institutions and regulators.

Cloud computing underpins the scalability and flexibility of modern RegTech solutions. Cloud platforms enable banks to process large datasets, perform complex compliance analytics, and generate regulatory reports without heavy on-premise infrastructure. PwC (2023) reports that more than 70% of global banks now rely on cloud-

based solutions for compliance analytics, reflecting the cloud's role in cost efficiency, resilience, and rapid deployment.

## 4. Applications of RegTech in Banking

RegTech applications in banking have expanded rapidly as financial institutions seek to manage regulatory obligations more efficiently while operating in increasingly digital and high-risk environments. One of the most prominent applications is anti–money laundering (AML) and counter-financing of terrorism (CFT) monitoring. RegTech tools automate sanction list screening, transaction monitoring, customer risk scoring, and the filing of suspicious activity reports (SARs). Machine learning–driven AML systems continuously analyze transaction patterns and adapt to emerging typologies, significantly improving detection quality. Deloitte (2022) reports that banks adopting advanced AML analytics have achieved a 60–80% reduction in false positives, allowing compliance teams to focus on genuinely high-risk cases while reducing operational costs and investigation fatigue.

Another critical application of RegTech lies in Know Your Customer (KYC) and digital identity verification. Modern KYC platforms integrate biometric technologies, optical character recognition (OCR), national digital identity systems such as Indonesia's e-KTP, digital signatures, and facial recognition. These technologies enable secure and remote customer onboarding while maintaining regulatory standards. According to OJK (2023), the adoption of electronic KYC (e-KYC) has reduced customer onboarding time from several days to just a few minutes, significantly enhancing customer experience while improving data accuracy and auditability. Automated KYC also supports ongoing customer due diligence by continuously updating risk profiles as customer behavior evolves.

Fraud detection systems represent another major RegTech application. These solutions analyze behavioral patterns, device fingerprints, transaction histories, and geolocation data to identify anomalies indicative of fraud. AI-based fraud engines operate in real time, generating instant alerts that allow banks to block suspicious transactions before losses escalate. PwC (2023) notes that real-time fraud analytics are particularly critical in digital banking environments, where transaction speed leaves little room for manual intervention.

RegTech also plays a vital role in regulatory reporting automation. Banks are required to submit thousands of reports annually to regulators under frameworks such as IFRS, Basel III, and national supervisory regimes. RegTech platforms standardize data, map accounting entries, validate consistency across systems, and automatically generate regulator-ready reports. This automation reduces reporting errors, shortens reporting cycles, and enhances transparency (EY, 2023).

# CHAPTER III
# DIGITALIZATION OF BANKING OPERATIONS

The digitalization of banking operations represents a fundamental transformation in how banks design processes, deliver services, and manage financial information in an increasingly technology-driven environment. Advancements in core banking systems, cloud computing, application programming interfaces (APIs), and data analytics have shifted banking from manual, branch-centric operations to real-time, platform-based digital ecosystems. This transformation enables faster transaction processing, enhanced customer experiences, and greater operational efficiency, while also introducing new challenges related to system integration, cybersecurity, regulatory compliance, and accounting accuracy. Understanding the digitalization of banking operations is essential for comprehending how modern banks sustain competitiveness, manage risk, and ensure reliable financial reporting in the era of digital finance.

## A. Core Banking Systems and Digital Architecture

Core Banking Systems (CBS) constitute the technological and operational backbone of modern banking institutions. In the context of digital transformation, these systems no longer function merely as centralized transaction-processing engines, but as strategic digital platforms that integrate accounting, risk management, regulatory compliance, and customer-facing services. The shift toward digital banking characterized by real-time transactions, omnichannel service delivery, open ecosystems, and data-driven decision-making has fundamentally reshaped the architecture of core banking systems. According to Rose and Hudgins (2022), the effectiveness of a bank's core banking infrastructure directly influences operational efficiency, financial transparency, and the institution's ability to innovate.

Therefore, understanding the evolution, structure, and implications of digital core banking architecture is essential for analyzing modern banking operations and accounting practices.

### 1. Definition and Functions of Core Banking Systems

Core Banking Systems (CBS) are the technological backbone of modern banking operations, designed to support a bank's core financial activities in an integrated and centralized manner. At a fundamental level, CBS manage deposit accounts, loan portfolios, interest calculations, payment transactions, and the automatic generation of accounting records. By maintaining a single source of truth for customer and transaction data, core banking systems ensure consistency, accuracy, and reliability across multiple service channels, including physical branches, ATMs, internet banking, and mobile applications. Rose and Hudgins (2022) emphasize that this centralized architecture allows banks to deliver uniform services to customers while simultaneously supporting internal controls and standardized financial reporting.

The primary functions of a core banking system extend beyond simple transaction processing. CBS are responsible for real-time balance updates, automated posting to sub-ledgers and the general ledger, interest accruals, fee calculations, and end-of-day or intraday reconciliations. These functions are essential for maintaining accurate financial positions and ensuring compliance with accounting and regulatory requirements. According to the Basel Committee on Banking Supervision (BCBS, 2023), reliable core systems are critical for sound risk management, as they provide timely and granular data needed for liquidity monitoring, credit exposure measurement, and capital adequacy assessments.

In the digital era, the role of core banking systems has expanded significantly due to technological advancements and changing customer expectations. Modern CBS are increasingly built on cloud-native architectures and designed to support real-time or near–real-time transaction processing. This enables banks to operate on a 24/7 basis, which is particularly important for digital banks and fintech-driven payment ecosystems. Deloitte (2023) notes that contemporary core banking platforms now integrate regulatory compliance checks—such as AML/CFT screening and transaction monitoring—directly into

transaction workflows, reducing operational risk and enhancing regulatory responsiveness.

Another critical function of modern CBS is their ability to integrate seamlessly with external systems through application programming interfaces (APIs). API-enabled core banking systems allow banks to connect with fintech partners, payment gateways, digital wallets, and open banking ecosystems. This integration supports rapid product development, such as embedded finance solutions, real-time payments, and personalized financial services. KPMG (2023) highlights that API-driven CBS architectures also facilitate advanced data analytics, enabling banks to leverage transactional data for customer insights, risk modeling, and strategic decision-making.

## 2. Evolution from Legacy Systems to Digital Core Architecture

The evolution of core banking systems from legacy platforms to digital core architectures reflects a fundamental transformation in how banks design, operate, and scale their technological infrastructures. Historically, core banking systems were built on monolithic architectures hosted on on-premise mainframe computers. These legacy systems were engineered primarily for stability, security, and high-volume transaction processing. Transactions were typically processed using batch-based methods, where data accumulated throughout the day and was posted to sub-ledgers and the general ledger at predefined end-of-day cycles. While this approach ensured reliability and control, it significantly constrained operational agility. As noted by Bunea, Kogan, and Stolin (2020), modifying legacy systems to accommodate new products, regulatory requirements, or digital channels was costly, time-consuming, and often risky.

As banking environments became more competitive and digitally driven, the limitations of legacy cores became increasingly evident. The rise of real-time payments, mobile banking, fintech competition, and rapidly evolving regulatory standards required systems that could respond instantly and scale dynamically. This pressure catalyzed the transition toward digital core architectures built on modular design principles. Modern core banking platforms increasingly adopt microservices architectures, in which discrete banking functions such as customer onboarding, account management, payments processing, interest accrual, and reporting are developed as

independent services. These services communicate through standardized application programming interfaces (APIs), allowing banks to modify or upgrade specific components without disrupting the entire system (McKinsey, 2023).

Cloud computing has played a critical role in enabling this architectural shift. By moving core banking workloads to cloud or hybrid environments, banks gain access to elastic computing resources that can scale automatically in response to transaction volumes and customer demand. Cloud-native cores also support faster development and deployment cycles through DevOps and continuous integration/continuous deployment (CI/CD) practices. According to Gartner (2023), cloud-based core banking systems significantly reduce infrastructure costs while improving system availability and resilience. Enhanced disaster recovery, geographic redundancy, and automated backups further strengthen operational continuity.

## 3. Key Components of Digital Core Banking Architecture

A modern digital core banking architecture is designed as a layered and modular system that integrates operational efficiency, accounting integrity, and technological flexibility. This architectural approach enables banks to respond rapidly to digital innovation while preserving the reliability and control required for financial reporting and regulatory compliance. According to Accenture (2024), the separation of functions into interconnected layers allows banks to modernize customer-facing services without destabilizing core accounting and ledger processes.

At the outermost level, the channel layer provides the primary interfaces through which customers and partners interact with the bank. This layer includes mobile banking applications, internet banking platforms, ATMs, branch systems, and third-party channels such as e-commerce platforms or fintech applications. The channel layer is designed for usability, speed, and omnichannel consistency, ensuring that customers experience seamless access to banking services regardless of the device or platform used. As KPMG (2023) notes, customer expectations for real-time responsiveness and personalization make this layer a critical driver of competitive differentiation.

Beneath the channel layer lies the integration and API layer, which acts as the connective tissue of the digital core. API gateways

manage data exchange between internal systems and external partners, enforcing security protocols, authentication standards, and data normalization rules. This layer is essential for open banking and embedded finance models, as it enables controlled data sharing while preserving system integrity. According to McKinsey (2023), robust API management reduces operational risk and enhances scalability by decoupling front-end innovation from back-end complexity.

The business services layer forms the functional heart of the digital core. It consists of microservices dedicated to specific banking activities such as deposit management, loan processing, card services, payments, and fee calculations. Each microservice operates independently but follows standardized business rules and accounting logic. This modularity allows banks to introduce new products or modify existing services with minimal disruption, significantly reducing time-to-market (Deloitte, 2024).

At the center of the architecture is the core ledger and accounting engine. This component records all financial transactions, generates double-entry accounting records, maintains customer and institutional balances, and ensures compliance with accounting standards such as IFRS or local GAAP. PwC (2023) emphasizes that despite extensive digitalization, the integrity of the core ledger remains non-negotiable, as it underpins financial reporting, regulatory submissions, and audit assurance.

## 4. Accounting and Internal Control Implications

The digitalization of core banking systems has fundamentally reshaped accounting practices and internal control frameworks within financial institutions. Unlike traditional environments that relied on periodic posting and manual reconciliation, digital core platforms enable real-time or near-real-time accounting. Transactions are automatically captured, validated, and posted to sub-ledgers and the general ledger as they occur, allowing financial information to be immediately reflected in management dashboards and regulatory reports. According to KPMG (2023), this capability significantly accelerates financial closing cycles, enhances transparency, and supports more timely and informed decision-making by management and regulators.

Real-time accounting also improves the consistency and traceability of financial data. Automated posting reduces the risk of human error associated with manual data entry and reconciliation, while standardized accounting rules embedded within the system ensure uniform treatment of transactions across products and channels. PwC (2023) notes that digital cores strengthen auditability by generating detailed system logs and transaction histories that can be reviewed continuously rather than only at period end. This shift aligns accounting more closely with operational reality, particularly in digital banking environments characterized by high transaction volumes and 24/7 activity.

However, the benefits of automation are accompanied by new and complex risks. In digital core banking systems, accounting logic is embedded in system configurations, algorithms, and business rules. If these configurations are flawed, errors can be propagated rapidly and at scale, potentially affecting thousands or millions of transactions before detection. Appelbaum et al. (2021) emphasize that automation amplifies both efficiency and risk, making strong preventive and detective controls essential. As a result, internal control frameworks must evolve from manual, after-the-fact checks to proactive and technology-enabled safeguards.

Effective governance over system design and change management becomes a critical control objective. Any modification to accounting rules, product parameters, or integration interfaces must follow rigorous approval, testing, and documentation procedures. According to COSO (2022), segregation of duties should be enforced not only at the transaction level but also at the system configuration level, ensuring that no single individual can design, implement, and approve critical accounting logic. Role-based access controls, privileged access monitoring, and periodic user access reviews are therefore central to digital control environments.

## B. Open Banking, Open Finance and API-Based Integration

The digitalization of banking operations has accelerated the transition from closed, institution-centric models toward open, interconnected financial ecosystems. Open Banking and Open Finance represent paradigm shifts in how financial data and services are

accessed, shared, and monetized across institutional boundaries. Enabled by Application Programming Interfaces (APIs), these models allow banks to securely share customer-consented data with third-party providers and to integrate banking services into broader digital platforms. According to Zetzsche, Buckley, Arner, and Barberis (2020), Open Banking is not merely a technological innovation, but a regulatory and structural transformation that redefines competition, customer empowerment, and the role of banks within the financial system. Understanding Open Banking, Open Finance, and API-based integration is therefore essential for analyzing modern banking operations, accounting processes, and regulatory compliance in the digital era.

## 1. Concept and Scope of Open Banking

Open Banking represents a fundamental shift in the structure and philosophy of the modern financial system, redefining how financial data and services are accessed, shared, and monetized. Conceptually, Open Banking refers to a regulatory and technological framework that obliges or enables banks to provide secure and standardized access to customer-authorized account data and payment services to licensed third-party providers (TPPs) through application programming interfaces (APIs). The core objective of this framework is to stimulate innovation, enhance competition, and improve efficiency in financial services by reducing information asymmetry and dismantling traditional data monopolies held by incumbent banks (OECD, 2023).

The scope of Open Banking extends beyond simple data sharing to encompass a broad ecosystem of financial services. With explicit customer consent, TPPs can access account information such as balances, transaction histories, and payment details, enabling services including account aggregation, payment initiation, personal financial management tools, and cash-flow analytics. More advanced applications include alternative credit scoring models that leverage transactional data to assess creditworthiness for underbanked individuals and small businesses. According to the World Bank (2024), Open Banking has the potential to expand financial inclusion by enabling more accurate risk assessments and tailored financial products, particularly in emerging markets.

A defining principle of Open Banking is customer data ownership and control. Customers retain full authority over who can access their financial data, for what purpose, and for how long. Consent management mechanisms are therefore central to Open Banking architectures, requiring banks to implement robust authentication, authorization, and revocation processes. The European Central Bank (2023) emphasizes that effective consent frameworks are essential to maintaining trust and safeguarding consumer rights in increasingly interconnected financial ecosystems.

From an operational perspective, Open Banking transforms the traditional role of banks. Rather than acting solely as proprietary service providers, banks increasingly function as data custodians and digital platforms. This shift necessitates significant changes in internal governance, including data standardization, API lifecycle management, cybersecurity controls, and service-level monitoring. Accenture (2024) notes that successful Open Banking implementation requires banks to adopt platform-oriented operating models that balance openness with resilience and risk management.

## 2. Open Finance as an Extension of Open Banking

Open Finance represents the next evolutionary stage of data sharing and platformization in the financial sector, building directly upon the foundations established by Open Banking. Conceptually, Open Finance extends the principles of secure, consent-based data access and interoperability beyond traditional banking products to encompass a much broader range of financial services, including insurance, investments, pensions, wealth management, and capital markets. While Open Banking primarily focuses on payment accounts and transaction data held by banks, Open Finance seeks to integrate financial information across multiple sectors, enabling a comprehensive and unified view of an individual's or organization's overall financial position (Zetzsche et al., 2020).

The core rationale behind Open Finance lies in its ability to reduce fragmentation in financial data and services. In traditional financial systems, customer information is often siloed across institutions and product categories, limiting the accuracy of risk assessments and the effectiveness of financial advice. By enabling

standardized and customer-authorized access to diverse datasets such as insurance policies, investment portfolios, pension entitlements, and credit exposures Open Finance supports more holistic financial analysis and decision-making. The World Economic Forum (2022) emphasizes that such integration can significantly enhance consumer outcomes by enabling personalized financial planning, improved product matching, and more transparent cost comparisons across providers.

From the perspective of financial inclusion, Open Finance offers substantial potential benefits. By aggregating data from multiple financial domains, lenders and insurers can develop more accurate and nuanced risk models, particularly for individuals and small enterprises with limited traditional credit histories. According to the OECD (2023), Open Finance can facilitate access to credit, insurance, and investment products for underserved populations by leveraging alternative data sources and reducing information asymmetries. This, in turn, supports more inclusive and competitive financial markets.

However, the expanded scope of Open Finance also introduces greater complexity and risk. Unlike Open Banking, which operates within relatively harmonized regulatory frameworks in many jurisdictions, Open Finance spans multiple sectors with distinct legal, regulatory, and accounting regimes. Insurance contracts, investment instruments, and pension products are governed by different disclosure requirements, valuation methods, and consumer protection rules. As noted by the European Commission (2023), this diversity necessitates the development of interoperable data standards and consistent governance principles to ensure reliability, comparability, and fairness across the ecosystem.

### 3. API-Based Integration and Digital Banking Ecosystems

Application Programming Interfaces (APIs) constitute the technological backbone of Open Banking and Open Finance, enabling secure, standardized, and automated interactions between banking institutions and external digital services. In modern digital banking architectures, APIs function as controlled gateways that expose specific banking capabilities such as account balance inquiries, payment initiation, transaction history retrieval, or digital identity verification without providing third parties with direct access to core banking systems. This layered access model significantly enhances security and

governance, as data sharing is limited to predefined scopes and subject to customer consent and regulatory requirements (OECD, 2023).

The adoption of API-based integration has fundamentally transformed banks from vertically integrated service providers into platform-based organizations embedded within broader digital ecosystems. Through APIs, banks can collaborate with fintech firms, e-commerce platforms, payment service providers, and even non-financial digital platforms to deliver integrated and customer-centric services. Accenture (2024) notes that API-driven ecosystems allow banks to decouple product manufacturing such as deposit accounts, lending products, and payment services from distribution channels. As a result, banks can rapidly scale their offerings through partners while focusing internal resources on core competencies such as risk management, balance sheet optimization, and regulatory compliance.

From an innovation perspective, APIs significantly reduce development time and costs. Standardized interfaces enable third-party developers to build, test, and deploy new financial applications without extensive customization of legacy systems. McKinsey (2023) highlights that banks leveraging open APIs can accelerate product launches and respond more effectively to changing customer expectations, particularly in areas such as embedded finance, digital wallets, and contextual lending. This agility is essential in competitive markets where fintech firms and big technology companies continuously introduce new digital financial solutions.

API-based integration also has important implications for accounting, operations, and financial control. Real-time data exchange between internal systems and external platforms enables automated transaction posting, near-real-time reconciliation, and more accurate consolidation of financial data across multiple channels. According to Deloitte (2023), API-enabled architectures support straight-through processing, reducing manual interventions and operational errors in accounting workflows. This enhances data accuracy, shortens financial closing cycles, and improves the reliability of management reporting and regulatory submissions.

## 4. Operational and Accounting Implications of Open Banking

The adoption of Open Banking and API-based integration has far-reaching operational and accounting implications for modern banks,

as financial services increasingly involve multiple platforms, third-party providers, and real-time data exchanges. From an operational perspective, transactions initiated through licensed third-party providers such as payment initiation service providers or account information service providers must be processed with the same level of accuracy, security, and reliability as transactions originating from a bank's own channels. This requires robust authentication mechanisms, real-time authorization controls, standardized data formats, and seamless synchronization between external APIs and internal core banking and accounting systems (Accenture, 2024).

Operational workflows in Open Banking environments become more complex due to the involvement of external parties in customer journeys. Banks must ensure that transaction validation, settlement, and exception handling processes operate in real time to prevent inconsistencies between operational records and the core ledger. According to Deloitte (2023), API-enabled straight-through processing reduces manual intervention but increases dependence on system configuration and data quality. As a result, banks must strengthen operational governance, monitoring tools, and service-level agreements to manage risks related to outages, latency, and data integrity across interconnected systems.

From an accounting perspective, Open Banking introduces new and often non-traditional revenue models. Banks may generate income from API usage fees charged to third-party providers, revenue-sharing arrangements with fintech partners, or value-added services such as data analytics and embedded financial products. Determining the appropriate accounting treatment for these revenues requires careful identification of performance obligations, transaction prices, and revenue recognition timing in accordance with IFRS 15. PwC (2023) emphasizes that banks must assess whether they act as principals or agents in Open Banking arrangements, as this distinction significantly affects revenue presentation and measurement.

In addition to revenue recognition, Open Banking affects cost allocation and profitability analysis. Investments in API infrastructure, cybersecurity, consent management, and system integration must be capitalized or expensed appropriately under applicable accounting standards. KPMG (2023) notes that granular cost tracking is increasingly important to evaluate the economic viability of Open

Banking initiatives and to support management decision-making in platform-based business models.

## C. Digital Customer Lifecycle and Digital Transaction Flow

The digitalization of banking operations has fundamentally transformed how banks acquire, serve, and retain customers, as well as how financial transactions are initiated, processed, and recorded. Unlike traditional banking models that relied heavily on physical branches and manual interactions, digital banking emphasizes continuous customer engagement through digital channels supported by automated workflows and real-time data processing. The concept of the digital customer lifecycle captures the end-to-end journey of customers in a digital banking environment, while digital transaction flow describes the technological and operational processes through which financial transactions are executed and recognized. According to Verhoef et al. (2021), effective management of the digital customer lifecycle and transaction flow is essential for delivering customer-centric services, maintaining operational efficiency, and ensuring accurate accounting and regulatory compliance in modern banking.

### 1. The Digital Customer Lifecycle in Banking

The digital customer lifecycle in banking describes the end-to-end journey of a customer's relationship with a bank, managed and optimized through digital technologies and data-driven processes. Unlike traditional banking models that relied heavily on physical branches and linear customer interactions, the digital customer lifecycle is continuous, dynamic, and highly personalized. It reflects the transformation of banks into digital service platforms that engage customers across multiple touchpoints, including mobile applications, internet banking, social media, and integrated third-party platforms. According to Kotarba (2023), the digital customer lifecycle is increasingly iterative rather than sequential, as customer data and behavioral insights are constantly analyzed to refine products, services, and engagement strategies in real time.

The lifecycle begins with customer acquisition and digital engagement, where banks use digital marketing, social media, search engines, and data-driven targeting to attract potential customers.

Advanced analytics and artificial intelligence enable banks to identify customer needs, predict preferences, and deliver personalized offers even before account opening. McKinsey (2023) emphasizes that effective digital acquisition strategies significantly reduce customer acquisition costs while improving conversion rates, as interactions are tailored to individual profiles and life events. At this stage, customer experience and ease of access are critical in shaping first impressions and trust.

The second stage is digital onboarding and identity verification, which has become a cornerstone of modern banking operations. Through e-KYC processes, banks integrate biometrics, optical character recognition, digital signatures, and government identity databases to verify customer identities remotely. According to OJK (2023), digital onboarding not only accelerates account opening but also enhances compliance with AML and CFT regulations by improving data accuracy and traceability. This stage demonstrates how regulatory compliance and customer convenience can be achieved simultaneously through digital solutions.

Account activation and product usage represent the transition from onboarding to value creation. Customers begin using core banking products such as payment accounts, savings, loans, and digital wallets. Core banking systems and real-time analytics monitor usage patterns to ensure seamless transactions and identify opportunities for cross-selling or upselling. Deloitte (2023) notes that early engagement during this phase is crucial, as customers who actively use digital features within the first few weeks are more likely to remain loyal over the long term.

## 2. Digital Customer Acquisition and Onboarding

Digital customer acquisition and onboarding represent a critical front-end process in modern banking, reflecting the broader shift toward data-driven, technology-enabled financial services. Digital customer acquisition relies heavily on online channels such as social media platforms, search engines, mobile applications, and fintech marketplaces to reach prospective customers efficiently and at scale. Unlike traditional mass marketing, digital acquisition strategies leverage advanced analytics and artificial intelligence to identify, segment, and target potential customers based on behavioral data, transaction patterns, demographic attributes, and life-cycle indicators.

McKinsey (2023) emphasizes that AI-driven acquisition models significantly improve conversion rates and marketing efficiency by delivering personalized offers at the right time and through the most effective digital channels.

Once a prospective customer expresses interest, the process transitions seamlessly into digital onboarding, which replaces conventional in-branch account opening with fully remote and automated procedures. Digital onboarding is designed to minimize friction while maintaining high standards of security, regulatory compliance, and data integrity. At the core of this process is electronic Know Your Customer (e-KYC), which integrates multiple technologies to verify customer identity and assess risk. Optical character recognition (OCR) is used to extract data from identity documents, while biometric verification such as facial recognition or fingerprint scanning ensures that the applicant is the legitimate owner of the submitted documents. Liveness detection further enhances security by confirming that the biometric sample is captured from a real, present individual rather than a static image or video.

In parallel, automated screening systems check customer information against sanctions lists, politically exposed person (PEP) databases, and adverse media sources. These controls enable banks to comply with anti–money laundering and counter–terrorism financing (AML/CFT) regulations in real time. The Financial Action Task Force (FATF, 2022) acknowledges that digital identity and e-KYC solutions can be highly effective for customer due diligence when implemented under a risk-based approach, allowing financial institutions to apply enhanced or simplified measures depending on the customer's risk profile. This flexibility is particularly important in supporting financial inclusion while maintaining robust safeguards against financial crime.

### 3. Account Activation, Usage and Customer Engagement

Following successful digital onboarding, the customer enters the account activation and usage phase, which marks the beginning of active participation in the banking ecosystem. Account activation typically involves the initial setup of credentials, activation of mobile and internet banking access, issuance of debit or virtual cards, and linkage to payment instruments such as digital wallets and QR-based payment systems. In digital banking environments, this process is

designed to be seamless and immediate, enabling customers to transact almost instantly after approval. According to Deloitte (2023), rapid account activation is a key determinant of early customer engagement and significantly influences long-term usage behavior.

Once activated, customers begin using a range of banking products, including deposit accounts, payment and transfer services, card transactions, savings tools, and value-added digital features. Customer engagement in this phase is continuous and largely mediated through mobile applications and online platforms rather than physical branches. Every interaction such as balance inquiries, transfers, bill payments, or card usage generates transactional and behavioral data that can be analyzed in real time. Banks increasingly rely on advanced analytics and artificial intelligence to transform this data into actionable insights, enabling personalized offers, contextual notifications, and proactive financial advice. McKinsey (2023) notes that data-driven personalization improves product adoption and deepens customer relationships by aligning services with individual needs and financial goals.

Digital engagement also supports cross-selling and up-selling strategies. For example, spending patterns may trigger personalized savings recommendations, installment offers, or credit products, while consistent account balances may lead to tailored investment or wealth management propositions. Verhoef et al. (2021) emphasize that such digitally enabled engagement enhances customer satisfaction and lifetime value by delivering services that are timely, relevant, and convenient. Moreover, interactive features such as in-app financial dashboards, budgeting tools, and real-time alerts increase transparency and customer trust, reinforcing long-term retention.

### 4. Digital Transaction Flow in Modern Banking

Digital transaction flow in modern banking refers to the integrated, end-to-end process through which financial transactions are executed within a fully digital environment. Unlike traditional banking models that relied heavily on batch processing and end-of-day posting, contemporary digital banking systems operate in real time or near real time, enabling instant fund availability, immediate account updates, and continuous monitoring. This transformation is driven by advances in core banking platforms, real-time payment infrastructures, and API-

based connectivity. According to the Bank for International Settlements (BIS, 2023), real-time transaction processing enhances efficiency and liquidity management but also demands higher standards of operational resilience and cybersecurity.

The digital transaction flow begins with transaction initiation, where a customer or institution triggers a payment or transfer through digital channels such as mobile banking applications, internet banking portals, ATMs, point-of-sale devices, or third-party platforms connected via APIs. At this stage, transaction details including amount, recipient, channel, and timing are captured and transmitted securely to the bank's core systems. The widespread adoption of mobile and instant payments has significantly increased transaction frequency and velocity, requiring systems that can process large volumes without latency (McKinsey, 2023).

Following initiation, the transaction enters the authentication and authorization stage. The bank verifies the identity of the user and the legitimacy of the transaction using multi-factor authentication methods such as PINs, biometrics, one-time passwords, and device recognition. Risk-based authentication mechanisms dynamically adjust security requirements based on transaction value, behavior patterns, and contextual risk indicators. NIST (2023) emphasizes that strong authentication is critical in mitigating fraud and unauthorized access in digital financial services.

The next stage involves processing and validation, where the transaction is assessed against predefined business rules. The core banking system checks account balances, transaction limits, and product conditions while simultaneously applying compliance filters related to anti-money laundering (AML), counter-terrorism financing (CFT), and sanctions screening. Advanced analytics and artificial intelligence increasingly support this phase by detecting anomalies and potential fraud in real time (Deloitte, 2023). Transactions that fail validation are rejected or flagged for further review, while compliant transactions proceed automatically.

Once validated, the transaction moves to clearing and settlement. Clearing involves the exchange of transaction information between participating financial institutions or payment networks, while settlement represents the final transfer of funds. Modern infrastructures such as real-time gross settlement (RTGS) systems and instant payment

schemes enable immediate and irrevocable settlement, reducing counterparty and liquidity risk. BIS (2023) highlights settlement finality as a cornerstone of financial stability in high-speed payment environments.

The final stage is accounting recognition and notification. The transaction is automatically posted to sub-ledgers and the general ledger, updating customer balances and generating accounting records in accordance with applicable standards. Customers receive real-time notifications confirming transaction completion, enhancing transparency and trust. KPMG (2023) notes that real-time accounting integration is essential to support digital transaction flows while maintaining accurate financial reporting and auditability.

## D. Embedded Finance and Banking-as-a-Service (BaaS)

The digitalization of banking operations has expanded beyond traditional financial institutions to include non-bank platforms that embed financial services directly into their ecosystems. Embedded finance and Banking-as-a-Service (BaaS) represent two closely related models that redefine how financial products are delivered, consumed, and accounted for. Rather than customers accessing banking services exclusively through bank-owned channels, financial functionalities such as payments, lending, and savings are increasingly integrated into digital platforms operated by fintech firms, e-commerce companies, and technology providers. According to Gomber, Koch, and Siering (2023), embedded finance and BaaS are among the most transformative developments in modern banking, as they blur the boundaries between banks and non-financial service providers while reshaping operational, regulatory, and accounting practices.

### 1. Concept and Characteristics of Embedded Finance

Embedded finance represents a structural transformation in the delivery of financial services, whereby banking and financial functionalities are seamlessly integrated into non-financial digital platforms such as e-commerce marketplaces, ride-hailing applications, social media platforms, and software-as-a-service ecosystems. Rather than requiring customers to access a bank's standalone channels, embedded finance allows payments, lending, insurance, and savings

products to be consumed directly within the digital activities where economic value is created. This integration fundamentally alters how users perceive and interact with financial services, making finance an enabling layer rather than a separate destination. According to Zetzsche et al. (2022), embedded finance reflects a shift from institution-centric banking to activity-centric financial intermediation, aligning financial services more closely with customer journeys and digital consumption patterns.

A defining characteristic of embedded finance is contextual integration. Financial services are offered precisely at the moment they are needed, such as instant credit during online checkout, automatic insurance coverage when purchasing travel services, or embedded wallets within mobility platforms. This context-driven delivery enhances customer convenience and conversion rates while reducing friction in digital transactions. McKinsey (2023) emphasizes that contextual finance significantly increases user engagement because financial decisions are made within familiar digital environments, supported by real-time data and automated decision engines.

Another core characteristic is the concept of invisible banking. In embedded finance models, customers may not be explicitly aware that a regulated financial institution is providing the underlying service. Payments, credit approvals, or balance updates occur instantly in the background, supported by automated risk assessments and real-time processing. While this invisibility enhances user experience, it increases operational and accounting complexity for banks, which remain responsible for regulatory compliance, risk management, and accurate financial reporting (BIS, 2023).

Technologically, embedded finance is enabled by API-driven architectures that allow secure, standardized, and real-time connectivity between banks, fintech providers, and digital platforms. APIs facilitate functions such as payment initiation, balance verification, credit scoring, and transaction settlement without exposing core banking systems directly. Accenture (2024) notes that API-based integration allows banks to scale embedded finance offerings across multiple partners while maintaining control over data, risk parameters, and accounting rules.

## 2. Banking-as-a-Service (BaaS): Definition and Business Model

Banking-as-a-Service (BaaS) is an operating and technological model in which licensed banks expose core banking functionalities such as deposit accounts, payment processing, card issuing, and lending through standardized application programming interfaces (APIs) to third-party providers. In this arrangement, fintech firms, digital platforms, or non-financial companies control the customer interface and user experience, while the licensed bank retains responsibility for regulatory compliance, prudential requirements, and balance sheet management. As noted by Accenture (2023), BaaS allows banks to reposition themselves from traditional retail distributors to infrastructure providers that enable innovation across broader digital ecosystems.

At the core of the BaaS business model is the separation between product manufacturing and service distribution. Licensed banks act as regulated manufacturers of financial products, ensuring compliance with banking regulations, capital adequacy rules, anti-money laundering (AML) standards, and consumer protection requirements. Meanwhile, frontend partners focus on designing digital experiences tailored to specific customer segments, such as e-commerce users, gig-economy workers, or small businesses. Technology providers play a critical intermediary role by offering middleware platforms that manage API connectivity, security, data standardization, and transaction orchestration (Deloitte, 2023). This three-layer structure enhances scalability, as banks can serve multiple partners simultaneously without duplicating customer-facing infrastructure.

From a strategic perspective, BaaS enables banks to monetize existing assets, including banking licenses, core systems, and compliance capabilities. Rather than competing directly with fintech firms, banks collaborate with them by providing "plug-and-play" banking services. According to McKinsey (2023), this model creates new revenue streams through API usage fees, transaction-based pricing, and revenue-sharing arrangements, while also reducing customer acquisition costs for banks. For fintech partners, BaaS significantly lowers barriers to entry by eliminating the need to obtain a banking license or build complex compliance frameworks.

### 3. Operational and Accounting Implications

Embedded finance and Banking-as-a-Service (BaaS) models introduce profound operational and accounting implications for banks, fundamentally reshaping how transactions are processed, recorded, and reported. Operationally, banks no longer interact directly with customers at the point of transaction. Instead, financial activities such as payments, lending, or account usage are initiated through third-party digital platforms, including e-commerce sites, ride-hailing applications, or fintech marketplaces. Despite this disintermediation at the customer interface, banks remain responsible for ensuring that every transaction is captured accurately and in real time within their core banking systems. According to Deloitte (2023), real-time integration between third-party platforms and core banking infrastructures is essential to maintain consistency between operational transaction data and official financial records.

From an accounting perspective, the complexity of revenue recognition increases significantly under embedded finance and BaaS arrangements. Banks frequently enter into revenue-sharing agreements with platform partners, where fees, interest income, or interchange revenues are split based on contractual terms. In such cases, banks must assess the nature of their role in the transaction—whether they act as principals, controlling the underlying financial service, or as agents, facilitating services on behalf of another party. The IFRS Foundation (2023) emphasizes that this principal–agent assessment under IFRS 15 is critical, as it determines whether revenue is recognized on a gross basis or net of partner shares. Misclassification can materially distort reported income and profitability.

In addition, embedded finance generates extremely high volumes of micro-transactions, often occurring continuously across digital channels. Accounting systems must therefore be capable of handling automated, high-frequency postings to sub-ledgers and general ledgers without manual intervention. KPMG (2023) notes that banks increasingly rely on event-driven accounting architectures, where each digital transaction triggers automatic journal entries and updates to customer balances. This automation supports faster financial closing and more timely management reporting but also amplifies the impact of system configuration errors, which can propagate rapidly across large transaction volumes.

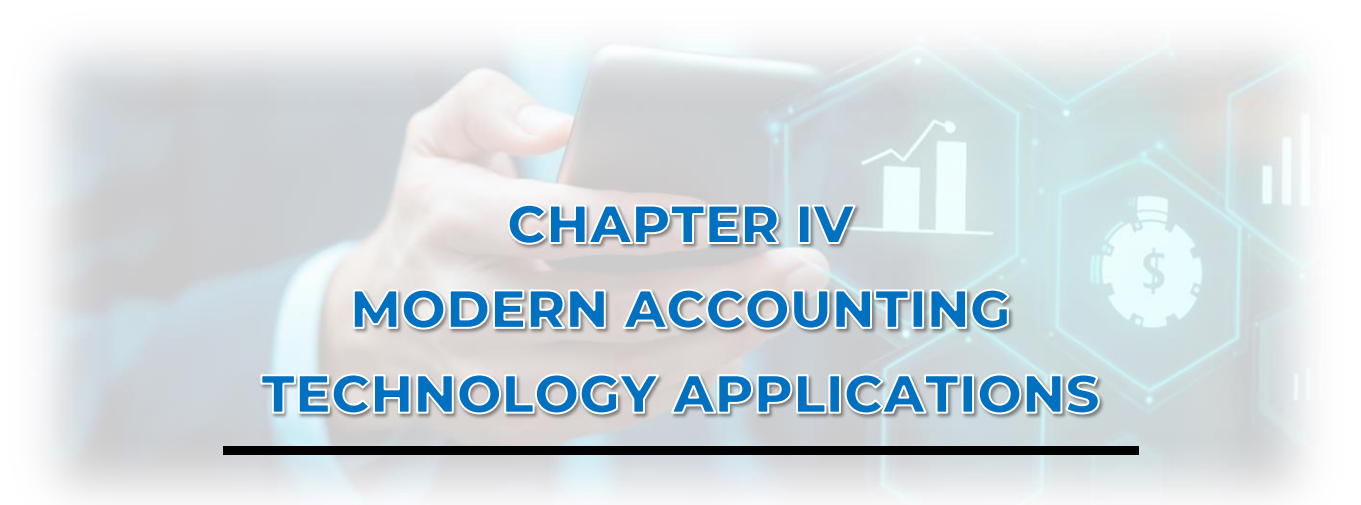
## 4. Risk Management and Regulatory Considerations

The rapid expansion of embedded finance and Banking-as-a-Service (BaaS) models significantly intensifies risk management and regulatory challenges for banks. Although customer-facing services are delivered through third-party digital platforms, banks remain fully accountable for regulatory compliance, financial integrity, and customer protection. This accountability extends across anti–money laundering and counter-terrorism financing (AML/CFT), consumer protection, prudential regulation, and data privacy requirements. According to the Basel Committee on Banking Supervision (BCBS, 2023), outsourcing and third-party arrangements do not transfer responsibility away from banks; instead, they require enhanced governance frameworks, comprehensive risk assessments, and continuous oversight throughout the lifecycle of the partnership.

Operational risk is one of the most critical concerns in embedded finance ecosystems. Transactions are executed in real time across interconnected systems, increasing exposure to system failures, processing errors, and service disruptions. A failure at a third-party platform such as downtime, inaccurate transaction processing, or weak access controls can directly affect the bank's core systems and customer accounts. The BCBS (2023) highlights the importance of operational resilience, urging banks to identify critical services, map interdependencies with third parties, and establish robust business continuity and disaster recovery arrangements. From a practical standpoint, this requires banks to implement redundancy, stress testing, and incident response mechanisms that extend beyond their internal IT environment.

Compliance risk is equally significant, particularly in relation to AML/CFT and customer due diligence. Even when customer interactions occur outside the bank's channels, banks must ensure that embedded finance partners apply equivalent standards for identity verification, transaction monitoring, and sanctions screening. The Financial Action Task Force (FATF, 2022) underscores that reliance on third parties for customer due diligence must be accompanied by clear accountability, access to underlying data, and the ability to conduct independent audits. Failure to meet these standards can result in regulatory sanctions and reputational damage.

Cybersecurity and data-sharing risks are also amplified, as sensitive financial and personal data flow across organizational boundaries through APIs and cloud-based infrastructures. According to ENISA (2023), weak API security, inadequate encryption, and insufficient monitoring can expose banks to data breaches and cyberattacks. To mitigate these risks, banks must establish strong contractual arrangements, including service-level agreements (SLAs) that define security requirements, data ownership, incident reporting obligations, and audit rights. Continuous monitoring of third-party performance and security controls is essential to ensure compliance with regulatory expectations.



# CHAPTER IV
# MODERN ACCOUNTING TECHNOLOGY APPLICATIONS

Modern accounting technology applications represent a transformative shift in how financial information is recorded, processed, analyzed, and reported in the banking industry. Advances in artificial intelligence, blockchain, robotic process automation, big data analytics, and cloud computing have moved accounting beyond manual, periodic reporting toward automated, real-time, and insight-driven systems. These technologies enhance accuracy, transparency, efficiency, and regulatory compliance, while simultaneously introducing new challenges related to data governance, cybersecurity, ethical use, and professional judgment. Understanding modern accounting technology applications is essential for appreciating how accounting functions support strategic decision-making, risk management, and trust in an increasingly digital financial ecosystem.

## A. AI, Machine Learning and Big Data in Financial Reporting

Financial reporting in the banking industry has undergone a profound transformation with the adoption of artificial intelligence (AI), machine learning (ML), and big data analytics. Traditional financial reporting systems were primarily designed to process historical, structured financial data and produce periodic reports. In contrast, modern digital banking environments generate massive volumes of real-time transactional and non-financial data that exceed the capacity of conventional accounting systems. According to Marr (2022), AI-driven analytics enable organizations to move from descriptive reporting toward predictive and prescriptive insights, significantly enhancing the relevance and timeliness of financial information. In banking, where accuracy, transparency, and regulatory

compliance are critical, AI, ML, and big data have become essential tools for improving reporting quality and decision-making.

## 1. Artificial Intelligence in Financial Reporting

Artificial Intelligence (AI) has become an increasingly important enabler of transformation in financial reporting, particularly within complex and data-intensive environments such as banking and large financial institutions. AI refers to computer-based systems that are capable of learning from data, recognizing patterns, and making decisions or recommendations that traditionally relied on human judgment. In the context of financial reporting, AI is not intended to replace professional accountants, but rather to augment their capabilities by automating routine processes, improving data quality, and supporting more informed and timely decision-making.

One of the most significant applications of AI in financial reporting is the automation of transaction classification and journal entry generation. Modern AI-driven accounting systems use machine learning algorithms to analyze large volumes of transaction data and map them to appropriate accounts based on historical patterns, accounting rules, and organizational policies. As transaction volumes grow due to digital payments, APIs, and platform-based banking models, manual processing becomes increasingly impractical. Appelbaum et al. (2021) emphasize that AI-based systems enhance consistency and accuracy in financial data processing, especially in high-frequency transaction environments, by reducing human errors and subjective inconsistencies in account classification.

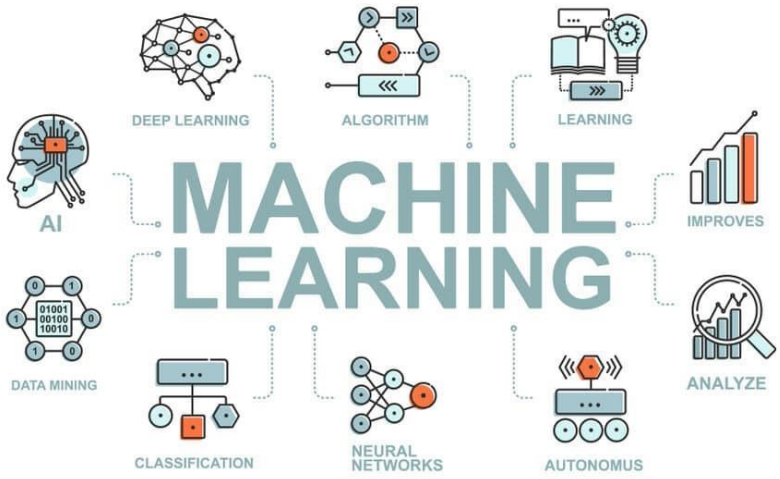
Beyond routine bookkeeping, AI plays a crucial role in anomaly detection and fraud identification, which directly affects the reliability of financial reports. AI models can continuously monitor transactions, balances, and adjustments in real time to identify deviations from normal patterns. These anomalies may signal posting errors, control weaknesses, earnings management, or fraudulent behavior. Unlike traditional rule-based internal controls that rely on predefined thresholds, AI systems learn dynamically and can adapt to new fraud techniques and evolving risk profiles. According to KPMG (2023), AI-powered continuous monitoring significantly strengthens the integrity

of financial reporting by enabling earlier detection of irregularities and reducing the risk of material misstatements.

## 2. Machine Learning and Accounting Estimates

Machine learning (ML), as a core subset of artificial intelligence, has become increasingly influential in the preparation of accounting estimates, particularly in sectors characterized by high uncertainty and data intensity such as banking. Unlike traditional rule-based systems, ML algorithms learn from historical and real-time data to identify patterns, relationships, and trends, enabling them to continuously improve predictive performance without explicit reprogramming. In financial reporting, this capability is especially valuable for accounting estimates that require significant judgment and forward-looking assumptions, which are central to modern accounting standards.

Figure 3. Machine Learning




Sumber: *Codepolitan*

One of the most prominent applications of ML in banking accounting is the estimation of Expected Credit Losses (ECL) under IFRS 9. ECL measurement requires banks to incorporate historical loss experience, current conditions, and forward-looking macroeconomic information. ML models can process large and diverse datasets such as borrower transaction behavior, payment histories, industry trends, and

macroeconomic indicators to generate more granular and risk-sensitive credit loss forecasts. According to KPMG (2023), ML-based ECL models enhance prediction accuracy by capturing nonlinear relationships and early warning signals that are often missed by traditional statistical models. This leads to more timely recognition of credit deterioration and improves the relevance of financial statements.

Beyond ECL, ML is widely used in loan loss provisioning and credit risk assessment. By continuously learning from new default and recovery data, ML models support dynamic risk scoring and scenario analysis, enabling banks to adjust provisions as economic conditions evolve. ML techniques are also applied in fair value measurement of financial instruments, particularly for complex or illiquid assets where observable market prices are limited. By analyzing historical pricing data, market volatility, and comparable instruments, ML models assist in generating valuation inputs that are consistent with fair value principles. In addition, ML supports forecasting of interest income and liquidity needs by modeling customer behavior, prepayment patterns, and interest rate movements, thereby strengthening financial planning and disclosure quality (PwC, 2024).

## 3. Big Data and the Transformation of Financial Reporting

Big data has fundamentally transformed the way financial reporting is produced, interpreted, and used in the banking industry. Big data refers to datasets with high volume, velocity, and variety, encompassing both structured data such as transaction records and accounting entries and unstructured data, including customer interactions, call center logs, social media content, and external market information. In digital banking environments, these diverse data sources are generated continuously and at scale, creating new opportunities to enrich traditional financial reporting with deeper analytical insights.

Figure 4. Big Data


Sumber: *Corporate Traning*

The integration of big data into financial reporting enables banks to move beyond a purely historical and compliance-oriented perspective toward more forward-looking and decision-relevant reporting. Traditional financial statements primarily summarize past transactions, while big data analytics allows management and stakeholders to understand the underlying drivers of financial performance and risk. Chen, Chiang, and Storey (2012) argue that big data analytics significantly enhances the informational value of accounting reports by linking financial outcomes with operational, behavioral, and market data. More recent studies confirm that data-enriched reporting supports better strategic decision-making and risk awareness in complex financial institutions (Deloitte, 2023).

One important application of big data in financial reporting is improved segment reporting. By analyzing customer-level transaction data, usage patterns, and cost allocation information, banks can generate more accurate profitability analyses across products, regions, and customer segments. This supports more transparent disclosures and helps management identify value-creating and value-destroying activities. Big data analytics also plays a critical role in stress testing and scenario analysis, where large datasets are used to simulate the impact of adverse macroeconomic conditions on capital adequacy, liquidity, and earnings. According to the Basel Committee on Banking Supervision (BCBS, 2023), data-driven stress testing enhances the credibility of financial disclosures and strengthens market discipline.

## 4. Continuous Reporting and Real-Time Analytics

Continuous reporting and real-time analytics represent a fundamental shift in financial reporting practices, driven by advances in artificial intelligence (AI), big data, and digital banking infrastructure. Traditionally, financial reporting has relied on periodic cycles monthly, quarterly, or annually where financial data are collected, adjusted, and reported after the fact. In contrast, continuous reporting systems leverage real-time data processing and AI-driven analytics to update financial information as transactions occur, enabling stakeholders to access near-real-time insights into an institution's financial position and performance.

In the banking sector, continuous reporting is enabled by the integration of core banking systems, data platforms, and advanced analytics engines. Transactions generated through digital channels are automatically captured, validated, and posted to sub-ledgers and general ledgers in real time. AI algorithms then aggregate and analyze these data to produce dashboards, alerts, and automated reports. Vasarhelyi, Kogan, and Tuttle (2015) emphasize that continuous reporting enhances transparency and reduces information asymmetry by narrowing the time gap between economic events and their financial disclosure. More recent studies highlight that real-time analytics also improve management responsiveness in volatile and highly regulated financial environments (Deloitte, 2023).

For banks, the benefits of continuous reporting are particularly significant in areas such as liquidity management, capital adequacy, and regulatory compliance. Real-time visibility into cash flows, funding positions, and risk-weighted assets allows treasury and risk management functions to respond more quickly to market stress or operational disruptions. According to the Bank for International Settlements (BIS, 2023), timely access to granular financial data strengthens banks' ability to meet prudential requirements and supports more effective supervisory oversight. Continuous reporting also supports intraday monitoring of key ratios, such as liquidity coverage ratios and large exposure limits, which are increasingly relevant in fast-moving financial markets.

However, the shift toward continuous and real-time reporting also introduces new challenges. The speed and volume of data increase the risk that errors, system misconfigurations, or flawed accounting logic can propagate rapidly across financial reports. Therefore, strong data governance frameworks are essential. These include clear data ownership, standardized data definitions, automated validation controls, and continuous monitoring of data quality. KPMG (2023) notes that internal control systems in a continuous reporting environment must evolve from periodic, manual reviews to automated, preventive, and detective controls embedded within digital processes.

## B. Blockchain, Digital Ledger Technology (DLT) and Smart Contracts

Blockchain and other forms of Digital Ledger Technology (DLT) represent one of the most disruptive technological innovations affecting accounting and financial reporting in the banking industry. Unlike traditional centralized accounting systems, blockchain-based ledgers operate on decentralized networks where transactions are recorded, verified, and stored collectively by multiple participants. This technological shift challenges conventional assumptions about transaction recording, verification, and auditability. According to Dai and Vasarhelyi (2017), blockchain has the potential to fundamentally transform accounting from a retrospective, document-based system into a real-time, continuously verified information infrastructure. In banking, the integration of DLT and smart contracts introduces new possibilities for automation, transparency, and trust, while also raising complex accounting, regulatory, and governance issues.

### 1. Concept and Characteristics of Blockchain and DLT

Distributed Ledger Technology (DLT) refers to a broad category of digital systems that enable the recording, sharing, and synchronization of data across multiple participants in a network without relying on a single centralized authority. Blockchain is the most well-known and widely implemented form of DLT, in which transactions are grouped into blocks that are cryptographically linked in a chronological chain. Each participant, or node, maintains a copy of the ledger, ensuring that records are replicated and continuously

updated across the network. This architectural design fundamentally changes how trust, verification, and record-keeping are established in digital environments (Narayanan et al., 2016).

One of the defining characteristics of blockchain and DLT is decentralization. Unlike traditional databases managed by a central institution, DLT distributes control among multiple participants. This reduces single points of failure and limits the ability of any one party to unilaterally manipulate records. In financial and accounting contexts, decentralization enhances system resilience and can strengthen confidence in shared transaction records, particularly in multi-party environments such as interbank settlements, supply chains, or consortium-based platforms (Yaga et al., 2019).

Immutability is another core feature. Once a transaction is validated and added to the ledger, it becomes extremely difficult to alter or delete. Cryptographic hashing links each block to the previous one, meaning that any modification would require altering all subsequent blocks and gaining consensus from the network. This characteristic significantly enhances data integrity and auditability. From an accounting perspective, immutable records reduce the risk of unauthorized adjustments, retroactive manipulation, and fraud, thereby strengthening the reliability of financial information (Schmitz & Leoni, 2019).

Transparency and traceability are also central to blockchain-based systems. Authorized participants can view transaction histories in near real time, enabling end-to-end tracking of assets and obligations. Depending on system design public, private, or permissioned access rights can be tailored to meet confidentiality and regulatory requirements. In regulated financial environments, permissioned blockchains are commonly used to balance transparency with data privacy and compliance obligations (OECD, 2023).

Consensus-based validation replaces traditional centralized verification mechanisms. Transactions are validated through agreed protocols, such as Practical Byzantine Fault Tolerance (PBFT) or Proof-of-Authority in permissioned networks. These mechanisms ensure that only legitimate transactions are recorded, reducing reliance on intermediaries and manual reconciliation processes. According to Narayanan et al. (2016), consensus mechanisms are essential for

establishing trust in decentralized systems where participants may not fully trust one another.

## 2. Blockchain-Based Accounting Systems

Blockchain-based accounting systems represent a significant evolution from traditional, centrally managed accounting information systems. In conventional environments, each party to a transaction maintains its own ledger, and consistency is achieved through periodic reconciliation, confirmations, and audits. This fragmented approach often results in time lags, operational inefficiencies, and reconciliation differences. Blockchain-based accounting systems seek to address these limitations by providing a shared, distributed ledger in which transactions are recorded once and simultaneously reflected for all authorized participants, thereby creating a common and synchronized record of economic events (Dai & Vasarhelyi, 2017).

A foundational concept in blockchain-based accounting is triple-entry accounting, as proposed by Dai and Vasarhelyi (2017). In this model, traditional debit and credit entries are complemented by a third, cryptographically secured entry recorded on a blockchain. This third entry serves as a neutral and verifiable confirmation of the transaction agreed upon by the transacting parties. In banking, triple-entry accounting can significantly streamline interbank processes such as payment clearing, securities settlement, and asset transfers, where reconciliation between multiple institutions is traditionally complex and resource intensive. By relying on a shared ledger, banks can reduce the need for bilateral confirmations and post-transaction adjustments.

From a financial reporting perspective, blockchain-based accounting systems enhance timeliness by enabling near-real-time recording of transactions. Once a transaction is validated through the network's consensus mechanism, it is immediately reflected in the distributed ledger. This real-time or near-real-time capability supports faster financial closing processes and more up-to-date management and regulatory reporting. Accenture (2023) notes that real-time accounting infrastructures are increasingly aligned with the demands of digital banking and continuous reporting models.

Accuracy is also improved through reduced manual intervention. Blockchain-based systems rely on automated validation rules and smart contracts to enforce predefined business logic and

accounting rules. By minimizing human input in transaction recording, the risk of clerical errors and inconsistent data treatment across entities is significantly reduced. However, the quality of accounting outcomes remains highly dependent on the correctness of system configuration and the underlying accounting policies embedded in smart contracts (Schmitz & Leoni, 2019).

Auditability is one of the most frequently cited advantages of blockchain-based accounting. Each transaction is time-stamped, cryptographically secured, and linked to prior records, creating an immutable audit trail. For auditors, this enables continuous audit approaches and more efficient verification of transaction existence and completeness. Nevertheless, auditors must still assess valuation, classification, and disclosure judgments, which cannot be fully automated (Appelbaum et al., 2021).

## 3. Smart Contracts and Accounting Automation

Smart contracts are programmable scripts embedded in blockchain networks that automatically execute contractual obligations once predefined conditions are satisfied. Originally conceptualized by Szabo in the 1990s and further developed in modern blockchain platforms, smart contracts translate legal and economic agreements into executable code. In contemporary banking and accounting environments, smart contracts function as automated control mechanisms that can initiate, validate, and record transactions without continuous human involvement, thereby reshaping how financial agreements are operationalized and accounted for (Werbach & Cornell, 2017).

In banking operations, smart contracts are increasingly applied to automate interest accrual and payment processes for loans and deposits. By embedding interest rate formulas, payment schedules, and penalty conditions into code, smart contracts can calculate and post interest in real time or at predetermined intervals. This automation reduces manual calculations and ensures consistent application of contractual terms across large portfolios of financial instruments. Deloitte (2023) notes that such automation is particularly valuable in high-volume retail and wholesale banking environments, where even minor calculation errors can accumulate into material misstatements.

Smart contracts also support automation in revenue recognition, especially for service-based and usage-based contracts. When performance obligations and pricing mechanisms are clearly defined, smart contracts can recognize revenue automatically as services are delivered or milestones are achieved. This capability aligns with the principles of IFRS 15, which require revenue to be recognized when control of goods or services transfers to the customer. However, determining whether contractual conditions are sufficiently objective and measurable remains a professional judgment that must be exercised before embedding accounting logic into code (PwC, 2023).

In the context of leases and complex financial instruments, smart contracts can automate recurring payments, adjustments, and settlements. For example, lease payment schedules under IFRS 16 or derivative settlements linked to market prices can be managed through smart contracts connected to trusted data sources, known as oracles. By automating these processes, banks can enhance timeliness and accuracy while reducing settlement risk and operational costs (Accenture, 2024).

## 4. Implications for Financial Reporting and Audit

Blockchain and Distributed Ledger Technology (DLT) have significant implications for financial reporting and auditing, fundamentally altering how accountants and auditors approach transaction verification and assurance. One of the most transformative aspects of blockchain is its ability to provide immutable, time-stamped records of all transactions, creating a permanent audit trail that can be accessed and verified by authorized parties. Unlike traditional accounting systems, which rely on periodic reconciliations and sample-based audit testing, blockchain enables continuous auditing, offering real-time visibility into financial activities (Vasarhelyi et al., 2015). This capability is particularly critical for banks and financial institutions, where high transaction volumes and complex interbank settlements make conventional audit approaches time-consuming and prone to oversight.

The adoption of blockchain enhances audit quality by allowing auditors to perform full-population testing. Every transaction can be traced, validated, and cross-checked against smart contract logic, reducing the risk of errors, omissions, or intentional manipulation. Additionally, the transparency and standardization of blockchain

records support more consistent application of accounting policies and compliance with regulatory reporting requirements. Continuous monitoring facilitated by DLT also enables early detection of anomalies, fraudulent activities, or operational inefficiencies, thereby strengthening internal control frameworks and financial governance.

Despite these benefits, blockchain introduces several challenges that impact financial reporting and audit practices. Valuation of digital assets recorded on distributed ledgers remains complex, particularly when market prices are volatile or illiquid. Similarly, determining the appropriate accounting treatment for crypto-assets and tokenized instruments requires careful alignment with existing accounting standards, such as IFRS 9 and IFRS 13, and often necessitates professional judgment (IFRS Foundation, 2023). Data privacy and confidentiality also present concerns, especially in shared ledgers where multiple parties have access; sensitive financial information must be protected while maintaining transparency for audit purposes.

## C. Robotic Process Automation (RPA) in Accounting Processes

Robotic Process Automation (RPA) has emerged as a key enabling technology in the digital transformation of accounting functions, particularly within the banking sector where transaction volumes are high and process accuracy is critical. RPA refers to the use of software robots that emulate human actions to execute structured, rule-based tasks across digital systems. Unlike artificial intelligence, RPA does not involve learning or cognitive capabilities; instead, it operates according to predefined business rules and workflows. According to Lacity and Willcocks (2021), RPA offers a practical and scalable approach to automation that allows organizations to enhance efficiency, reduce operational risk, and improve compliance without extensive system redesign. In banking accounting, RPA plays a vital role in automating repetitive processes while enabling accountants to focus on higher-value analytical and judgment-based activities.

### 1. Scope and Applications of RPA in Accounting

Robotic Process Automation (RPA) has emerged as a transformative technology in accounting, particularly in the banking sector, where high-volume, repetitive, and rules-based processes are

prevalent. RPA refers to software robots or "bots" that can perform structured tasks by interacting with digital systems in the same way a human would, but with higher speed, accuracy, and consistency. In accounting operations, RPA is extensively applied to processes such as accounts payable and receivable management, where bots can automatically capture invoice data, match it with purchase orders, and initiate payments, thereby reducing manual effort and the risk of errors. Similarly, inter-system and bank reconciliations benefit from RPA, as bots can retrieve transaction data from multiple systems, compare balances, and flag discrepancies without human intervention (Deloitte, 2023).

Another critical application of RPA is in journal entry posting and validation. Bots can automatically generate recurring journal entries, verify coding accuracy, and post them into the general ledger, ensuring compliance with accounting policies and standards. Additionally, RPA facilitates data extraction for financial and regulatory reporting by aggregating information from disparate systems, structuring it according to reporting requirements, and even populating regulatory templates. This capability is particularly valuable in banks, where regulatory reporting obligations such as IFRS, Basel III, and local central bank submissions demand timely and accurate data consolidation.

RPA also supports master data management by automating updates to customer accounts, product codes, and vendor information, which reduces inconsistencies and enhances data integrity across systems. By minimizing manual intervention, RPA not only improves processing efficiency but also allows accounting personnel to focus on higher-value analytical and strategic tasks, such as financial analysis, variance investigation, and decision support.

## 2. Benefits of RPA for Accounting Efficiency and Accuracy

Robotic Process Automation (RPA) offers substantial benefits in enhancing accounting efficiency and accuracy, particularly in high-volume, rule-based banking environments. One of the most significant advantages of RPA is its ability to streamline operations without requiring fundamental changes to existing IT infrastructure. Software robots can operate continuously, executing repetitive accounting tasks faster and with greater consistency than human staff. This capability

directly contributes to faster financial closing cycles, as RPA can automatically post journal entries, reconcile accounts, and validate transactions in near-real-time, reducing the delays traditionally associated with manual processing (PwC, 2022).

In addition to speed, RPA enhances data consistency and reliability. Since bots follow predefined rules and standardized workflows, they eliminate variability caused by human errors, such as miskeyed entries, missed approvals, or inconsistent application of accounting policies. This results in higher-quality financial data that can be confidently used for internal management reporting and regulatory submissions. Furthermore, the automation of repetitive tasks reduces operational costs by decreasing the need for manual labor and allowing finance teams to focus on higher-value activities, such as analysis, forecasting, and decision support.

Another critical benefit of RPA is improved auditability. Every action performed by a bot is recorded in detailed system logs, providing a transparent, time-stamped trail of activities. This audit trail simplifies both internal and external audits by enabling auditors to trace transactions, verify compliance with internal policies, and assess controls without extensive manual effort. PwC (2022) highlights that this aspect of RPA supports regulatory compliance and strengthens governance frameworks, ensuring that accounting operations are both efficient and defensible.

## 3. Internal Control and Governance Implications

The implementation of Robotic Process Automation (RPA) in accounting brings substantial efficiency and accuracy benefits but simultaneously introduces critical internal control and governance considerations. Because RPA bots operate with system-level access and process high volumes of transactions, robust control mechanisms are essential to prevent errors, unauthorized activity, or misuse. According to the Committee of Sponsoring Organizations of the Treadway Commission (COSO, 2023), automation must be embedded within an organization's internal control framework to maintain accountability, ensure compliance, and uphold the integrity of financial reporting.

A central governance consideration is the segregation of duties. To reduce operational and fraud risks, organizations should separate responsibilities among bot developers, deployment teams, and

operational users. This segregation ensures that no single individual can both create and execute automated processes without oversight. Periodic review and validation of RPA workflows are also necessary to confirm that bots continue to perform tasks in line with accounting policies, regulatory requirements, and changing business conditions. Such reviews help identify and correct potential errors, system misconfigurations, or outdated logic that could compromise financial data quality.

Exception handling and escalation mechanisms form another critical aspect of governance. Even highly reliable RPA systems encounter scenarios that require human intervention, such as unusual transactions, processing errors, or system alerts. Establishing clear procedures for handling these exceptions ensures timely resolution and reduces the risk of unaddressed discrepancies affecting financial statements. Furthermore, detailed documentation and auditability of RPA processes are essential. Comprehensive records of bot design, operational parameters, transaction logs, and change histories provide transparency for internal and external auditors, supporting regulatory compliance and organizational accountability.

## 4. Limitations and Risks of RPA Implementation

While Robotic Process Automation (RPA) offers significant efficiency and accuracy benefits in accounting, its implementation is not without limitations and risks that require careful management. RPA is inherently best suited for environments where processes are stable, standardized, and rule-based. When underlying systems, data formats, or business rules change, automated workflows can fail or produce incorrect results, potentially causing errors to propagate across large volumes of transactions. Lacity and Willcocks (2021) emphasize that without timely updates and process monitoring, even minor disruptions can lead to significant operational and financial consequences.

Operational risks are a primary concern. Bot failures or system downtime can interrupt transaction processing, delay reporting, and disrupt financial operations. Additionally, because RPA can execute tasks at high speed and volume, errors can propagate rapidly if the bot logic is flawed or misconfigured. Over-reliance on automation without sufficient human oversight may exacerbate these risks, as discrepancies may remain undetected until they affect financial statements or

regulatory reports. Therefore, human supervision, exception handling, and periodic validation of bot performance are essential components of a resilient RPA strategy.

Another limitation of RPA is its dependency on existing IT infrastructure and system stability. RPA tools generally mimic user interactions with applications rather than altering underlying processes, which makes them sensitive to changes in software interfaces, updates, or security patches. Any modification in upstream systems may require reconfiguration or redeployment of bots, increasing maintenance effort and cost. Furthermore, RPA does not inherently provide analytical judgment or complex decision-making capabilities, meaning that tasks involving interpretation, estimation, or professional judgment still require human intervention.

## D. Cloud Computing and Cyber Resilience

Cloud computing has become a foundational technology in the digital transformation of banking accounting systems. By enabling on-demand access to shared computing resources, cloud platforms support real-time financial reporting, scalability, and integration with advanced analytics and automation tools. However, the increasing reliance on cloud-based systems also exposes banks to heightened cyber risks, including data breaches, system disruptions, and third-party vulnerabilities. As financial information is among the most sensitive and regulated data, cyber resilience the ability to prevent, withstand, respond to, and recover from cyber incidents has emerged as a critical concern for accounting governance. According to the Basel Committee on Banking Supervision (BCBS, 2023), cyber resilience is essential for maintaining operational continuity, financial stability, and confidence in digital banking systems.

### 1. Cloud Computing Models in Banking Accounting

Cloud computing has become a pivotal enabler of modern banking accounting, offering scalable, flexible, and cost-efficient IT infrastructure and services. In the banking sector, cloud adoption typically follows three main service models: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). IaaS provides virtualized computing resources, such as servers, storage,

and networking, allowing banks to host core accounting systems and financial databases without investing heavily in physical infrastructure. PaaS supports the development, testing, and deployment of accounting applications and analytical tools, enabling finance teams to customize workflows, automate reporting, and integrate with other financial systems efficiently. SaaS delivers fully managed cloud-based accounting, enterprise resource planning (ERP), and financial reporting applications that can be accessed through web browsers or mobile platforms, reducing the need for on-premise software installation and maintenance (Gartner, 2024).

The adoption of cloud computing in banking accounting offers multiple operational and strategic advantages. By leveraging IaaS, banks can quickly scale computing resources to handle peak transaction volumes or complex financial analyses, without the delays and costs associated with procuring and configuring new hardware. PaaS allows accounting teams to innovate rapidly, deploying new applications for regulatory reporting, risk assessment, or predictive financial analytics while maintaining consistency and integration with existing systems. SaaS solutions, meanwhile, provide banks with standardized, continuously updated accounting software, ensuring compliance with the latest financial regulations and accounting standards such as IFRS and local banking rules (PwC, 2023).

Cloud computing also supports collaboration and remote access, which have become critical in distributed banking environments where accounting, audit, and compliance teams may operate from multiple locations. Real-time access to centralized financial data enhances accuracy, consistency, and transparency in reporting, while automated updates reduce the risk of outdated or inconsistent accounting records. Furthermore, cloud-based systems improve disaster recovery and business continuity capabilities by storing financial data redundantly across multiple data centers, thereby safeguarding critical information against system failures or cyberattacks.

## 2. Benefits of Cloud Computing for Financial Reporting

Cloud computing offers significant benefits for financial reporting in modern banking, fundamentally transforming how accounting data is processed, consolidated, and analyzed. By hosting accounting systems and financial data on cloud platforms, banks gain

the ability to perform real-time or near-real-time processing of transactions, enabling timely and continuous financial reporting. This capability allows management to access up-to-date dashboards, monitor key performance indicators, and respond promptly to emerging financial risks or regulatory developments (Deloitte, 2023).

One of the most important advantages of cloud computing is improved data consistency across multiple systems and business units. Centralized cloud-based repositories ensure that all accounting entries, transaction data, and financial statements are standardized and synchronized, reducing errors that often occur in decentralized or legacy systems. This consistency supports reliable financial analysis, regulatory compliance, and audit processes, as all stakeholders operate from a single source of truth. Furthermore, cloud platforms facilitate automated consolidation of financial information from various subsidiaries or departments, streamlining reporting for multinational banks or institutions with complex organizational structures.

Cloud computing also accelerates the financial close and reconciliation processes. Traditional accounting systems often involve labor-intensive, manual procedures that delay monthly or quarterly closings. With cloud-enabled systems, automated workflows, real-time posting of transactions, and integrated reconciliation tools reduce the time and effort required to close books, freeing accounting teams to focus on higher-value analytical and strategic tasks. Additionally, these platforms integrate seamlessly with emerging technologies such as artificial intelligence (AI), robotic process automation (RPA), and advanced analytics. AI-powered predictive insights, RPA-driven transaction processing, and data analytics dashboards enhance decision-making, support scenario analysis, and improve the accuracy and completeness of financial reports (PwC, 2023).

## 3. Cybersecurity Risks in Cloud-Based Accounting Systems

While cloud computing offers significant benefits for accounting and financial reporting in banking, it also introduces substantial cybersecurity risks that can affect data integrity, operational continuity, and regulatory compliance. Cloud-based accounting systems centralize critical financial information, making them attractive targets for cyberattacks, including unauthorized access, ransomware, data exfiltration, and denial-of-service attacks. Such incidents can

compromise the accuracy and completeness of financial records, disrupt reporting processes, and result in financial losses or operational downtime. In addition, reliance on third-party cloud service providers creates dependency risks, as any failure, vulnerability, or security breach on the provider's side can directly impact the bank's accounting systems and reporting capabilities (PwC, 2023).

Cybersecurity risks in cloud accounting are further compounded by concentration in the cloud services market. As multiple financial institutions increasingly rely on a limited number of major providers, systemic risk emerges. The International Organization of Securities Commissions (IOSCO, 2023) highlights that this cloud concentration can amplify the impact of a single provider's outage or security incident across the banking sector, potentially affecting liquidity, settlement processes, and regulatory compliance. For banks, such systemic vulnerabilities necessitate rigorous third-party risk management, including vendor due diligence, contractual security obligations, continuous monitoring, and contingency planning.

From an accounting perspective, cybersecurity incidents carry direct implications for financial reporting. Banks may need to recognize losses resulting from fraud, data breaches, or operational disruptions, and in certain cases, record impairments on affected assets. Furthermore, incidents may trigger disclosure requirements under accounting standards such as IFRS or local regulations, particularly concerning contingencies, risk exposures, or operational disruptions. Internal controls over cloud-based accounting processes must therefore integrate cybersecurity considerations, including access management, encryption, activity monitoring, and automated anomaly detection, to ensure that financial data remains reliable and auditable.

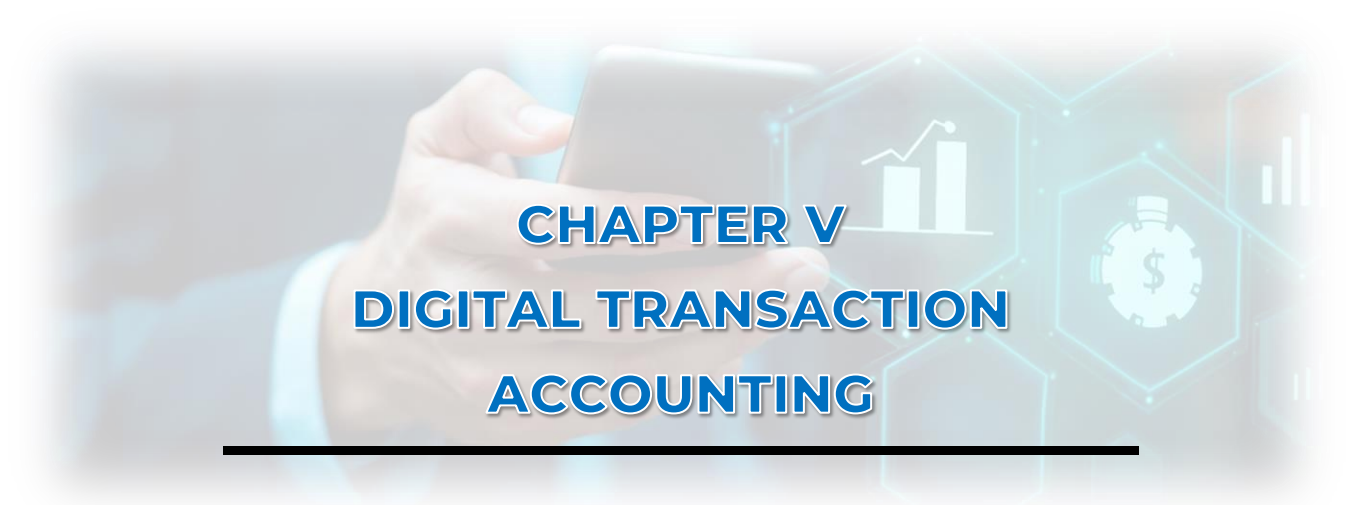
### 4. Cyber Resilience and Internal Control Over Financial Reporting

Cyber resilience in banking accounting goes beyond traditional IT security measures, encompassing a holistic approach that integrates governance, risk management, and recovery capabilities to ensure the continuous accuracy, availability, and reliability of financial data. In the context of cloud-based and digital accounting systems, cyber resilience is critical because these platforms centralize sensitive financial information and enable real-time transaction processing, making them

potentially vulnerable to cyberattacks, system failures, and operational disruptions. As such, resilience measures must protect not only data confidentiality but also the integrity and availability of accounting records, which are essential for financial reporting and regulatory compliance (COSO, 2023).

The Committee of Sponsoring Organizations of the Treadway Commission (COSO, 2023) emphasizes the integration of technology risk management into internal control over financial reporting (ICFR). Effective cyber resilience starts with strong access controls and identity management, ensuring that only authorized personnel can initiate, approve, or modify accounting transactions. This includes multi-factor authentication, role-based access, and periodic review of user permissions. Data encryption and secure backup mechanisms provide additional layers of protection, safeguarding sensitive financial information both in transit and at rest, and ensuring rapid recovery in the event of data corruption or loss.

Continuous system monitoring and real-time incident detection are also essential components of cyber-resilient accounting. Automated monitoring tools, anomaly detection algorithms, and alert systems allow banks to identify irregular activities, operational anomalies, or potential cyber threats before they affect financial reporting. These capabilities enable timely intervention, reducing the risk of misstatements or unauthorized transactions. In parallel, comprehensive business continuity and disaster recovery plans ensure that accounting operations can resume quickly after disruptions, maintaining both operational efficiency and regulatory compliance.



# CHAPTER V
# DIGITAL TRANSACTION ACCOUNTING

Digital Transaction Accounting represents a fundamental shift in the way financial transactions are recognized, recorded, and reported within modern banking and financial institutions. Driven by the rapid expansion of e-banking, digital payments, crypto-assets, and real-time processing technologies, transaction accounting has evolved from periodic, manual recording toward continuous, automated, and system-integrated processes. In digital finance environments, transactions occur instantly, in high volumes, and across complex technological ecosystems, requiring accounting systems that emphasize accuracy, timeliness, transparency, and strong internal controls. As noted by Vasarhelyi, Kogan, and Tuttle (2015) and reaffirmed by recent digital finance studies (BIS, 2023; IFRS Foundation, 2023), digital transaction accounting plays a critical role in ensuring reliable financial reporting, regulatory compliance, and stakeholder trust in an increasingly technology-driven banking landscape.

## A. E-Banking and Mobile Banking Transaction Recording

The rapid adoption of e-banking and mobile banking has reshaped the way financial transactions are initiated, processed, and recorded within banking institutions. Unlike traditional branch-based transactions that rely on manual inputs and batch processing, digital banking transactions occur continuously, remotely, and in high volumes. This transformation demands accounting systems capable of real-time processing, automated recognition, and seamless integration with core banking platforms. According to Vasarhelyi, Kogan, and Tuttle (2015), digital transaction environments require accounting mechanisms that are embedded within operational systems to ensure accuracy, timeliness, and reliability of financial information.

Consequently, understanding how e-banking and mobile banking transactions are recorded is fundamental to modern banking accounting in the digital era.

## 1. Characteristics of E-Banking and Mobile Banking Transactions

E-banking and mobile banking transactions are distinguished by their electronic and automated nature, enabling customers to perform financial activities such as fund transfers, bill payments, loan repayments, and balance inquiries through web portals or mobile applications. Unlike traditional banking, these digital transactions operate continuously, providing 24/7 access without the constraints of physical branch hours, and are executed instantly once authorized by the customer. This immediacy is supported by underlying core banking systems that integrate payment processing, account management, and compliance checks in real time, ensuring both operational efficiency and regulatory adherence.

From an accounting perspective, e-banking and mobile banking transactions exhibit several defining characteristics. First, they generate a high volume of transactions with relatively low individual monetary value, particularly in retail banking segments. This creates a need for automated recording, validation, and reconciliation processes to maintain accuracy and timeliness in financial reporting. Second, these transactions rely heavily on system-driven controls, including automated authorization, fraud detection, and exception handling, which reduce the risk of human error and enhance internal control frameworks. Third, digital transactions produce extensive electronic audit trails, providing detailed time-stamped records that support both internal monitoring and regulatory compliance (BIS, 2023).

The widespread adoption of mobile and e-banking has transformed the operational landscape of banking. According to BIS (2023), in many jurisdictions, the volume of digital retail transactions has now exceeded that of traditional over-the-counter transactions, highlighting the critical role of automated systems in ensuring the integrity of accounting and reporting processes. Real-time processing not only improves customer experience but also allows banks to maintain accurate account balances, promptly recognize revenue and fees, and detect anomalies in transactional patterns. Furthermore, the

integration of e-banking platforms with core accounting systems supports timely financial statement preparation, regulatory reporting, and management decision-making.

## 2. Digital Transaction Flow in E-Banking Systems

In e-banking and mobile banking systems, the digital transaction flow is a highly structured and automated process integrated within the bank's core banking infrastructure. The workflow begins when a customer initiates a transaction through a digital channel, such as a mobile application or online banking portal. At this stage, the system captures transaction details, including the source and destination accounts, transaction amount, and type of operation, ensuring that all necessary information is accurately recorded. Following initiation, the transaction undergoes authentication and authorization, which typically involves multi-factor authentication techniques to verify the identity of the customer and confirm their permission to execute the transaction. This step is critical in preventing unauthorized access and ensuring security in digital financial operations (BIS, 2023).

Once authentication is successful, the transaction proceeds to validation. This stage includes checking account balances, verifying transaction limits, and applying compliance rules, such as anti-money laundering (AML) and fraud detection protocols. Automated business rules embedded in the core banking system ensure that only legitimate and authorized transactions are approved for further processing. After validation, the transaction is processed and posted within the core banking system. This involves updating the relevant sub-ledgers and the general ledger in real time, reflecting the economic impact of the transaction on the bank's financial statements. By integrating posting with accounting systems, banks can maintain accurate and timely financial records while minimizing manual intervention and errors (IFRS Foundation, 2023).

Upon successful posting, the system generates accounting recognition, automatically adjusting asset, liability, revenue, or expense accounts in accordance with the transaction's economic substance. This ensures that the bank's books reflect a precise financial position at all times. Finally, the system communicates confirmation and notifications to the customer, completing the transaction cycle and providing transparency and assurance of completion.

### 3. Accounting Recognition and Measurement

In e-banking and mobile banking systems, accounting recognition and measurement follow established accrual accounting principles, ensuring that all digital transactions are accurately reflected in the bank's financial statements. When a customer initiates a fund transfer, the bank records a simultaneous reduction in the sending customer's deposit liability and an increase in the receiving customer's deposit liability. Importantly, such transactions do not affect the bank's net assets, as they represent internal movements of customer funds. This dual-entry approach ensures that the bank's books remain balanced and that each transaction's economic substance is properly captured (KPMG, 2022).

Revenue from digital banking services, including fees for transfers, account maintenance, and other value-added services, is recognized at the point when the service is rendered, in accordance with IFRS 15. This revenue recognition framework emphasizes identifying performance obligations and allocating transaction prices based on the services delivered. By adhering to these principles, banks ensure that income is recognized consistently and transparently, providing accurate information for management, regulators, and stakeholders. For instance, a fee charged for an instant payment service would be recorded as revenue immediately upon completion of the transaction rather than at the time of cash collection.

Measurement of e-banking transactions is generally conducted at nominal or face value, given that most transactions involve cash or cash-equivalent balances. This simplifies recording while maintaining accuracy in the general ledger and sub-ledgers. However, the timing of authorization, processing, and settlement can create temporary differences in accounting recognition. For example, a transfer initiated late in the day may be authorized but not settled until the next business day. In such cases, suspense or clearing accounts are used to temporarily hold the transaction, ensuring that financial reporting reflects the correct period of economic activity. These mechanisms help maintain the integrity of period-end reporting and prevent misstatement of assets and liabilities (KPMG, 2022).

### 4. Integration with Core Banking and General Ledger Systems

In contemporary banking environments, the integration of digital transaction channels with core banking and general ledger systems is a critical enabler of efficiency, accuracy, and transparency in financial reporting. When customers conduct transactions via e-banking or mobile banking platforms, these transactions are automatically captured and processed through the bank's core banking system, which in turn updates the general ledger in real time. This end-to-end integration supports straight-through processing (STP), where transactions flow seamlessly from initiation to accounting recognition without manual intervention, significantly reducing the likelihood of errors and delays (Deloitte, 2023).

STP is particularly valuable in high-volume banking operations, where millions of transactions occur daily. Automated posting rules are configured to ensure that each transaction whether a fund transfer, payment, or fee charge triggers standardized accounting entries according to predefined policies. For example, a customer transfer automatically debits one deposit account and credits another, while fees for digital services are posted as income in accordance with IFRS 15 revenue recognition standards. This automation not only enhances efficiency but also ensures that financial statements accurately reflect the bank's position and performance at any given moment (IFRS Foundation, 2023).

The integration also strengthens auditability and internal control. Because all transactions are recorded systematically and in real time, audit trails are complete, time-stamped, and verifiable, allowing auditors to trace individual transactions from initiation through final ledger posting. This reduces the risk of misstatements and simplifies both internal audits and regulatory examinations. Moreover, integrated systems facilitate timely reconciliation between sub-ledgers and the general ledger, preventing discrepancies and enhancing the reliability of management and regulatory reporting.

## B. Accounting for Digital Payments & E-Wallet Platforms

The rapid growth of digital payments and e-wallet platforms has significantly transformed the payment landscape within the banking and financial services industry. Digital payments enable cashless

transactions through electronic channels, while e-wallet platforms facilitate the storage and transfer of monetary value in digital form. These innovations have expanded financial inclusion, increased transaction speed, and enhanced customer convenience. However, they also introduce complex accounting challenges related to recognition, measurement, revenue allocation, and regulatory compliance. According to McKinsey (2023), digital wallets and instant payment systems now account for a substantial share of retail transactions globally, making their accurate accounting treatment critical for banks and payment service providers.

## 1. Overview of Digital Payment Systems and E-Wallet Platforms

Digital payment systems have revolutionized the way individuals and businesses conduct financial transactions, encompassing a variety of mechanisms such as card-based payments, QR code payments, instant fund transfers, and mobile-based payment applications. These systems enable users to perform payments quickly, securely, and conveniently without relying on traditional cash or physical banking channels. Complementing these systems, e-wallet platforms serve as digital repositories for customer funds, allowing seamless peer-to-peer transfers, merchant payments, bill settlements, and even integration with loyalty or rewards programs. In many cases, banks partner with fintech companies to deliver e-wallet services, assuming roles that range from issuing the wallet and safeguarding customer funds to facilitating settlement and reconciliation of transactions (BIS, 2023).

From an accounting perspective, the digital payment ecosystem presents unique considerations that differ from traditional banking operations. One of the critical aspects is understanding the business model and the bank's role within the transaction flow. When a bank acts as a principal owning the funds, bearing the credit risk, and providing payment services directly it must recognize revenue and related assets in accordance with its control over the transaction. Conversely, if the bank functions primarily as an agent, merely facilitating payments on behalf of third parties, revenue recognition may be limited to fee-based income for services rendered, consistent with the guidance in IFRS 15 (IFRS Foundation, 2023).

Moreover, digital payments generate a high volume of low-value transactions that require real-time processing, accurate recording, and integration with core banking and accounting systems. Accounting systems must be capable of handling these transactional flows, ensuring that each payment is properly authorized, validated, and reflected in both customer balances and financial statements. E-wallets, in particular, involve liability recognition for stored customer funds, requiring banks to distinguish between funds held in trust and their own assets, as well as to implement proper internal controls and reconciliation procedures to prevent misstatement or misuse (PwC, 2022).

**2. Recognition of Customer Funds in E-Wallets**

In e-wallet platforms, customer balances represent amounts held by the issuing or custodial institution on behalf of the users, creating a clear liability rather than an asset for the institution. These funds are not economically owned by the bank or fintech operator but are maintained to facilitate payments, transfers, and other digital transactions at the customer's direction. As such, in the statement of financial position, customer balances are recorded as liabilities, reflecting the institution's obligation to honor the funds upon demand or as specified by the e-wallet agreement. This treatment ensures that financial statements accurately represent the economic reality of the institution's relationship with its customers (EY, 2022).

The recognition of customer funds aligns with the principles outlined in the IFRS Conceptual Framework, which emphasizes control and obligation over mere physical possession in determining the accounting treatment. Since the institution controls the process of safeguarding and processing payments but does not bear ownership risks or benefits of the underlying funds, the balances are appropriately classified as a financial liability. This distinction is critical for maintaining both transparency and compliance, as it prevents the misstatement of assets and provides regulators and stakeholders with an accurate depiction of the institution's financial position.

Additionally, proper accounting for e-wallet funds requires strict segregation between customer funds and the institution's own assets. EY (2022) notes that failure to maintain separate accounts can lead to regulatory breaches and create difficulties in reconciliations,

audits, and reporting. Segregated accounts also enhance operational controls, ensuring that customer funds are not inadvertently used for operational expenses or other institutional purposes, which could compromise liquidity management and customer trust.

### 3. Accounting Treatment of Digital Payment Transactions

The accounting treatment of digital payment transactions involves accurately capturing the flow of funds between customers, merchants, and payment service providers while ensuring compliance with applicable financial reporting standards. In e-wallet or digital payment systems, each transaction triggers multiple accounting entries that reflect changes in customer balances, settlement obligations, and revenue recognition. When a customer initiates a payment, the first step is to reduce the customer's e-wallet balance, which is recorded as a decrease in the institution's liability to the customer. Simultaneously, a corresponding liability is recognized for the merchant or payee, representing the obligation to settle the transaction amount on behalf of the customer. This ensures that the financial position of the payment institution correctly reflects its role as a custodian of funds rather than an owner of the transferred amounts (IFRS Foundation, 2023).

Revenue recognition arises primarily from transaction fees, service charges, or commissions associated with the digital payment. Under IFRS 15, revenue is recognized when the performance obligation is satisfied, which, in the context of digital payments, occurs when the payment service is executed successfully, and the transaction is completed. For instance, a processing fee charged to a merchant or customer is recorded as income at the point of transaction settlement. If the bank operates within a Banking-as-a-Service (BaaS) or e-wallet ecosystem with third-party fintech partners, revenue-sharing arrangements must be carefully evaluated. The recognition of income depends on whether the bank acts as a principal controlling the service or as an agent facilitating a third-party service. In a principal relationship, the institution recognizes the full fee as revenue and records any amounts payable to partners as expenses, whereas in an agent relationship, only the net fee retained is recognized as income (PwC, 2023).

Furthermore, accurate accounting treatment requires real-time integration with core banking and general ledger systems to maintain

consistency between operational records and financial statements. Automated posting rules help capture high-volume, low-value transactions characteristic of digital payments while supporting internal control and auditability. Suspense accounts may also be employed to temporarily record pending transactions until settlement is confirmed, ensuring proper period-end reporting.

### 4. Settlement, Clearing, and Reconciliation Processes

In digital payment systems, settlement, clearing, and reconciliation processes are essential to ensure that transactions are accurately completed, recorded, and reflected in the financial statements. Unlike traditional banking, digital payments often involve multiple intermediaries, including payment gateways, clearinghouses, merchant acquirers, and banks, each of which plays a role in the movement of funds. When a customer initiates a payment through an e-wallet or online platform, the transaction may not settle immediately; instead, the amount passes through temporary accounts, such as clearing or suspense accounts, until confirmation of successful fund transfer is received. These accounts act as interim holders of funds, ensuring that assets and liabilities are appropriately tracked and preventing misstatement in financial reporting (IFRS Foundation, 2023).

The settlement process finalizes the movement of funds between parties, while clearing involves the calculation and validation of obligations between financial institutions. In modern digital payment ecosystems, these steps are often automated and occur in near real time, reducing settlement risk and enhancing operational efficiency. For instance, real-time gross settlement (RTGS) systems allow banks and payment providers to settle transactions individually as they occur, whereas batch-based clearing systems aggregate multiple transactions for periodic settlement. Accurate recording of these transactions during both settlement and clearing is crucial to maintaining the integrity of the general ledger and customer accounts (EY, 2022).

Reconciliation is the process that ensures consistency between transaction records, settlement accounts, and the general ledger. In high-volume digital environments, manual reconciliation is impractical and prone to error. Deloitte (2023) highlights the use of automated reconciliation tools that leverage rules-based matching and artificial

intelligence to compare transaction records across systems, detect discrepancies, and flag exceptions for review. These systems enhance accuracy, reduce processing time, and provide auditable trails for regulatory compliance. AI-driven reconciliation can adapt to evolving transaction patterns, further reducing the risk of undetected errors or fraud.

## C. Accounting Treatment of Crypto-Assets and Tokenized Instruments

The emergence of crypto-assets and tokenized instruments represents one of the most disruptive developments in modern financial systems. Unlike traditional financial assets, crypto-assets are created, transferred, and stored using distributed ledger technology (DLT), often without centralized intermediaries. Tokenized instruments further extend this innovation by digitally representing real-world assets such as securities, deposits, or commodities on blockchain platforms. While these innovations offer efficiency, transparency, and programmability, they pose significant challenges for accounting recognition, measurement, and disclosure. According to the Financial Stability Board (FSB, 2023), the lack of uniform economic characteristics and regulatory treatment of crypto-assets requires careful professional judgment in accounting practices. This section examines how banks and financial institutions account for crypto-assets and tokenized instruments within existing accounting frameworks.

### 1. Definition and Classification of Crypto-Assets

Crypto-assets represent a diverse class of digital assets that leverage cryptography and distributed ledger technology to facilitate ownership, transfer, and verification. They encompass cryptocurrencies such as Bitcoin and Ethereum, stablecoins pegged to fiat currencies, utility tokens that provide access to digital services, and security tokens that represent investment contracts or ownership rights. From an accounting perspective, accurate classification of crypto-assets is essential because it directly influences how they are measured, reported, and disclosed in financial statements. Under current International Financial Reporting Standards (IFRS), most crypto-assets do not qualify as cash or cash equivalents because they are not legal tender and

are not widely accepted as a medium of exchange (IFRS Foundation, 2023). Consequently, their treatment differs significantly from traditional fiat holdings or cash balances.

The IFRS Interpretations Committee has clarified that cryptocurrencies held for investment or operational purposes are generally classified as intangible assets under IAS 38. As intangible assets, they are recognized at cost initially and subsequently measured using either a cost model or a revaluation model, depending on the entity's accounting policy and the availability of an active market. This classification emphasizes that such holdings lack physical substance but provide the potential for future economic benefits through price appreciation or operational utility (IFRS Interpretations Committee, 2019). However, when crypto-assets are held for sale in the ordinary course of business, such as by broker-traders or digital asset exchanges, they may be considered inventory under IAS 2. In this scenario, measurement is at fair value less costs to sell, reflecting their status as goods held for short-term resale and highlighting the volatility and market-driven nature of these instruments.

Beyond classification, crypto-assets pose unique accounting challenges, including determining fair value in markets with low liquidity, recognizing impairment losses, and disclosing risks related to price volatility, regulatory uncertainty, and cybersecurity. The IFRS Foundation (2023) notes that transparent reporting and careful judgment are critical to ensure that financial statements faithfully represent the economic reality of these digital assets. Moreover, organizations must maintain robust internal controls and documentation to track acquisitions, disposals, and transfers, especially given the irreversibility of many blockchain transactions.

## 2. Initial Recognition and Measurement

Initial recognition and measurement of crypto-assets are critical steps in ensuring accurate financial reporting and compliance with accounting standards. At the point of acquisition, crypto-assets are recognized at cost, which comprises the purchase price paid and any directly attributable expenses necessary to acquire the asset, such as transaction fees or custody costs. This principle aligns with the general recognition criteria under IFRS, which emphasize that an asset should be recognized when the entity controls the resource and expects future

economic benefits to flow from it (IFRS Foundation, 2023). In the context of banks or financial institutions engaged in crypto-asset activities, assets generated through mining, staking, or transaction validation are recognized only when control is established—that is, when the entity has the ability to direct the use of the asset and derive benefits from it.

The initial measurement must reflect the fair value of the consideration given or received at the transaction date. Given the high volatility of crypto markets, selecting an appropriate valuation methodology is paramount. Market prices on active exchanges are generally considered the most reliable indicators of fair value, provided that the market is sufficiently active and liquid. In cases where quoted prices are unavailable or markets are illiquid, banks must apply alternative valuation techniques, such as recent transaction prices or models based on observable inputs, while ensuring transparency and consistency in methodology (KPMG, 2023). Accurate initial measurement not only affects subsequent accounting treatment but also provides a baseline for impairment assessment, fair value re-measurements, and financial reporting disclosures.

Additionally, initial recognition requires careful documentation of the transaction and associated costs. Banks must maintain detailed records of acquisition dates, purchase prices, fees, and source of crypto-assets, whether through purchase, mining, or other means. This supports auditability, internal controls, and compliance with regulatory expectations. Robust processes for initial recognition and measurement also help mitigate operational and valuation risks, particularly in environments characterized by rapid price fluctuations and emerging regulatory frameworks.

### 3. Subsequent Measurement and Impairment

Subsequent measurement of crypto-assets is a critical aspect of financial reporting, as it determines how changes in value are reflected in the financial statements over time. The accounting treatment depends primarily on the classification and intended use of the crypto-asset. For crypto-assets classified as intangible assets under IAS 38, particularly those with indefinite useful lives, amortization is not applied. Instead, these assets are subject to annual impairment testing or more frequent assessments when indicators of impairment are present, such as

significant price declines or technological obsolescence. Impairment losses are recognized in profit or loss to reflect the decline in recoverable amount, ensuring that the carrying value of the asset does not exceed its recoverable value. Although IAS 38 allows revaluation to fair value if an active market exists, this is often impractical for many crypto-assets due to market fragmentation and low liquidity, limiting the scope for upward adjustments (IFRS Foundation, 2023).

In contrast, crypto-assets held for trading or investment purposes are generally measured at fair value with changes recognized in profit or loss, consistent with IFRS 9 principles. This approach provides timely and relevant information to financial statement users, reflecting the volatile nature of crypto markets. According to Deloitte (2023), fair value measurement enhances the relevance of financial reporting by presenting up-to-date valuations, which is particularly useful for investors and stakeholders seeking insights into the current financial position and risk exposure of banks holding crypto-assets. The use of fair value also supports risk management by highlighting unrealized gains and losses that could affect liquidity and capital adequacy.

From an accounting control perspective, subsequent measurement requires robust systems for tracking market prices, calculating gains and losses, and maintaining audit trails. Banks must ensure that fair value inputs are derived from reliable, observable market data whenever possible, and that valuation models for less liquid assets are well-documented, consistent, and periodically reviewed. Additionally, management judgment plays a key role in assessing impairment indicators, selecting appropriate valuation techniques, and ensuring compliance with accounting standards and disclosure requirements.

### 4. Accounting for Stablecoins and Crypto-Related Liabilities

Accounting for stablecoins and crypto-related liabilities presents unique challenges due to their hybrid characteristics, combining aspects of digital assets and financial instruments. Stablecoins are typically designed to maintain a stable value by being backed with fiat currency, commodities, or other financial assets, creating an explicit obligation for the issuer to redeem the coins at a predetermined rate. From an accounting perspective, this redemption

obligation generally classifies stablecoins as financial liabilities on the issuer's balance sheet, reflecting a present obligation to transfer economic resources. The corresponding backing assets, whether cash, reserves, or other investments, must be clearly identified and measured at fair value or amortized cost, depending on the applicable accounting framework (BIS, 2023). Any mismatch between the value of backing assets and the stablecoin liability requires careful monitoring, as it can create potential financial risks and impact both solvency assessments and disclosure requirements.

For banks or financial institutions acting as holders, custodians, or intermediaries, the accounting treatment depends on the contractual rights attached to the stablecoins. If the arrangement does not meet the definition of a financial instrument—where the holder has a contractual right to receive cash or another financial asset—stablecoins may be classified as intangible assets under IAS 38. In this scenario, the bank records the stablecoin at cost initially, with subsequent measurement determined by either cost or fair value, depending on the business model and regulatory guidance. Fair value measurement is often preferred for liquidity management and risk monitoring due to the volatility and market dynamics of crypto-assets, even for stablecoins with ostensibly fixed values (EY, 2023).

Moreover, stablecoins introduce operational and regulatory considerations that influence accounting. Banks must ensure segregation of customer funds when acting as custodians, maintain transparent records of holdings, and manage any associated liabilities from transactional activities such as payments, lending, or staking. Disclosure requirements are particularly important to provide users, investors, and regulators with insights into the backing mechanisms, associated risks, and the institution's exposure to stablecoin fluctuations.

## D. Real-Time Transaction Validation and Digital Audit Trails

The shift toward digital and instant financial services has elevated real-time transaction validation and digital audit trails from operational features to foundational elements of modern banking accounting. In environments characterized by high-frequency transactions, instant payments, and automated execution, traditional

batch-based validation and periodic audits are no longer sufficient. Real-time transaction validation ensures that transactions are authorized, accurate, and compliant at the moment they occur, while digital audit trails provide continuous, immutable records of transaction lifecycles. According to Vasarhelyi, Kogan, and Tuttle (2015), these mechanisms underpin the transition from retrospective accounting to continuous accounting and assurance, strengthening trust, transparency, and regulatory compliance in digital finance.

## 1. Concept of Real-Time Transaction Validation

Real-time transaction validation is a critical process in modern digital banking, referring to the automated verification of transactions as they are initiated and executed. This process ensures that each transaction complies with predefined rules and is legitimate before being processed further. Core validation checks include verifying customer identity through authentication mechanisms, ensuring account balance sufficiency, assessing transaction limits, screening against compliance requirements such as anti-money laundering (AML) and sanctions lists, and checking system integrity controls to prevent technical errors. In digital banking ecosystems, these validations are integrated into core banking platforms, payment engines, and financial messaging systems, enabling straight-through processing (STP) without requiring manual intervention, which accelerates transaction processing and enhances operational efficiency (BIS, 2023).

From an accounting perspective, real-time validation is fundamental for ensuring the accuracy and reliability of financial records. By confirming that only authorized and complete transactions are captured, banks can significantly reduce posting errors and minimize the occurrence of discrepancies that require reconciliation. This capability is particularly important in high-volume transaction environments such as retail payments, interbank transfers, and instant settlement systems, where even small errors can have amplified effects on liquidity and reporting accuracy. Moreover, automated validation provides a structured audit trail, as each transaction is checked against rules and logged at the point of initiation, thereby enhancing transparency and traceability for internal and external audits.

Real-time validation also plays a crucial role in risk management. According to the Bank for International Settlements (BIS, 2023), instant verification of liquidity sufficiency and compliance reduces settlement and operational risks, supporting financial stability in fast-paced payment networks. For example, in instant payment systems, the validation engine ensures that funds are available and that transactions comply with legal and regulatory requirements before final settlement, mitigating the risk of overdrafts, fraud, or failed payments.

**2. Integration with Accounting and General Ledger Systems**

In modern banking systems, the integration of transaction validation engines with accounting and general ledger modules has become a fundamental aspect of operational and financial efficiency. Once a transaction successfully passes real-time validation checks such as authentication, balance verification, compliance screening, and system integrity controls predefined posting rules automatically generate the corresponding accounting entries. This seamless integration ensures that account balances, sub-ledgers, and the general ledger are continuously updated, reflecting the real-time economic impact of every transaction. As a result, banks can maintain an accurate and up-to-date view of financial positions, which is particularly critical in high-volume digital environments where thousands of transactions may occur simultaneously (Deloitte, 2023).

From an accounting perspective, this integration reinforces the principles of accrual accounting. Economic events are recognized at the moment when control over assets or obligations changes, ensuring that revenues, expenses, assets, and liabilities are accurately recorded without delay. For example, a customer payment processed through a mobile banking app immediately reduces the payer's account liability and increases the payee's balance, while any transaction fees are simultaneously recognized as revenue. This real-time recognition enhances the reliability of financial statements and reduces the reliance on manual reconciliations or end-of-period adjustments, which historically introduced errors and reporting delays.

Additionally, integration with accounting and general ledger systems strengthens internal controls and auditability. Automated posting rules ensure consistency in how transactions are recorded, while detailed logs of each validation and posting event provide an immutable

trail for internal reviews and external audits. Such automation not only mitigates the risk of human error but also supports compliance with regulatory standards and reporting obligations. Banks can more readily demonstrate that financial data are complete, accurate, and processed according to established accounting policies.

### 3. Digital Audit Trails and Transaction Traceability

Digital audit trails represent a cornerstone of modern accounting and internal control in banking, providing a comprehensive, time-stamped record of every transaction throughout its lifecycle. From initiation and authorization to processing, settlement, and financial reporting, digital audit trails capture critical metadata, including user IDs, timestamps, system logs, and authentication credentials. Unlike traditional paper-based trails, which were prone to gaps, delays, or manual errors, digital audit trails are automatically generated and continuously maintained by core banking systems, payment engines, and accounting software (COSO, 2023). This automation ensures that every action taken on a transaction is recorded accurately and immutably, creating a reliable record for both internal oversight and external audit purposes.

The traceability offered by digital audit trails allows banks to link source transactions directly to financial statement line items. For instance, a customer fund transfer executed through a mobile banking app can be traced from the initial authorization through system validation, ledger posting, and final settlement. Every intermediate step, including exception handling or automated adjustments, is captured in the audit trail. This level of transparency enables accountants and auditors to verify the completeness and accuracy of recorded transactions and supports the assessment of internal control effectiveness. As emphasized by COSO (2023), such traceability is essential for mitigating risks associated with fraud, operational errors, and compliance breaches, particularly in high-volume digital environments where manual monitoring is impractical.

Moreover, digital audit trails facilitate real-time or near-real-time auditing and monitoring. Advanced analytics tools can continuously review transaction logs to identify anomalies, unusual patterns, or policy violations, enabling proactive risk management and faster remediation. This capability enhances the reliability of financial

reporting by ensuring that discrepancies or irregularities are detected and addressed promptly, rather than relying solely on periodic audits. Additionally, digital audit trails support regulatory compliance by providing verifiable evidence for supervisory reviews, reporting obligations, and internal governance requirements.

**4. Continuous Auditing and Assurance**

Continuous auditing represents a transformative approach in modern accounting and auditing practices, enabled by real-time data access, digital audit trails, and advanced automation tools. Unlike traditional audit methods that rely on periodic sampling and retrospective review, continuous auditing allows auditors to monitor and assess transactions on an ongoing basis. In digital banking environments, where millions of transactions occur daily across multiple channels—such as mobile apps, online banking portals, and payment gateways—continuous auditing ensures that the integrity, completeness, and accuracy of financial records are maintained in near real time. Automated audit systems can analyze transaction flows, identify anomalies, and flag exceptions immediately for further investigation, reducing the risk of undetected errors or fraud (Vasarhelyi et al., 2015).

The core advantage of continuous auditing lies in its ability to assess entire populations of transactions rather than relying on selective sampling. This full-population testing enhances audit quality by providing comprehensive assurance over financial data, increasing both internal and external stakeholder confidence. For example, real-time monitoring can detect unusual patterns in fund transfers, reconcile discrepancies between subsidiary ledgers and the general ledger, and verify compliance with internal control policies and regulatory requirements. This proactive approach also enables auditors to respond promptly to irregularities, reducing potential financial and reputational risks associated with delayed detection (Vasarhelyi et al., 2015).

Continuous auditing also integrates seamlessly with accounting systems through digital audit trails, which capture time-stamped, user-specific, and system-verified records of all transactional activities. This integration allows auditors to trace every transaction from initiation to posting and reporting, supporting both operational oversight and financial statement assurance. Advanced analytics and artificial

intelligence can further enhance continuous auditing by identifying patterns, predicting potential risks, and prioritizing transactions for review, making the audit process more efficient and targeted (Vasarhelyi et al., 2015).

# CHAPTER VI
# FINANCIAL REPORTING AND DIGITAL-BASED ANALYSIS

Financial Reporting and Digital-Based Analysis has become a cornerstone of modern banking as digital transformation reshapes how financial information is generated, analyzed, and utilized. In an environment characterized by real-time transactions, complex digital products, and heightened regulatory scrutiny, traditional financial reporting models are increasingly supplemented by automated systems and advanced analytics. Digital-based analysis enables banks to integrate IFRS- and PSAK-compliant reporting with data-driven insights, supporting not only historical accountability but also forward-looking decision-making and risk management. As emphasized by the IFRS Foundation (2023) and BIS (2023), the convergence of financial reporting and digital analytics enhances transparency, accuracy, and strategic relevance in an increasingly data-intensive banking landscape.

## A. IFRS and PSAK-Based Reporting in Digital Banking

Banks operating in a digital environment must apply the same recognition, measurement and disclosure principles found in IFRS (and in Indonesia, PSAK) as they would in traditional operations but they must do so in a world of real-time transactions, platform business models, new product types (e-wallets, APIs, tokenised instruments), and automated accounting engines. This combination raises practical and governance challenges (data quality, model risk, timing of recognition, principal/agent assessments) and opportunities (machine-readable reporting, continuous disclosure). The remainder of this section explains how core IFRS/PSAK requirements apply to digital banking, highlights the key implementation issues, describes evolving digital reporting tools (taxonomies/XBRL), and offers practical guidance for accountants and preparers. (IFRS Foundation)

## 1. Core Accounting Framework — Applicability and Unchanged Principles

The core accounting framework remains fully applicable in the context of digital banking, embedded finance, and other technology-driven financial services, with underlying principles largely unchanged. The adoption of digital delivery channels or platforms does not alter the fundamental rules for recognition, measurement, or presentation of financial information. Economic substance over form continues to be the guiding principle, ensuring that the nature of transactions determines accounting treatment rather than the medium through which they are conducted. For instance, customer deposits collected via mobile applications are still recognized as financial liabilities, while loans originated through online portals remain financial assets. Preparers of financial statements are therefore required to consistently map digital business events to existing standards to ensure faithful representation and comparability of financial information (IFRS Foundation, 2023).

Several key accounting standards are immediately relevant in digital and platform-based environments. IFRS 9 (or PSAK 109 in Indonesia) governs financial instruments, addressing classification, measurement, expected credit loss (ECL) calculations, and hedge accounting, even when financial assets and liabilities are created, processed, or managed through digital systems. This includes loans extended via digital portals, digital deposits, and automated credit facilities, where robust ECL models and digital transaction monitoring support accurate impairment measurement (European Banking Authority, 2023). IFRS 15, concerning revenue from contracts with customers, is applicable to revenues generated from platform or marketplace services, API access fees, and revenue-sharing arrangements with fintech partners, emphasizing careful identification of performance obligations and timing of revenue recognition.

IFRS 13 on fair value measurement provides guidance for the valuation of trading digital assets, tokenized instruments, and other financial instruments where market-based measurements are required. The fair value hierarchy and valuation methodologies must be applied

rigorously, with attention to the volatility and liquidity of digital instruments. Additionally, IAS 1 and IAS 8 govern presentation and disclosure requirements, emphasizing the need to transparently report accounting judgments and assumptions, including model inputs, automation logic, and digital system parameters that affect financial reporting outcomes.

## 2. Practical Implementation Issues in Digital Banking

The practical implementation of accounting in digital banking introduces several complex considerations that require careful mapping to established standards. One critical area is the timing and automation of recognition. Modern digital cores and event-driven architectures enable near-real-time posting of transactions. However, it is essential that automated posting logic aligns precisely with the economic recognition triggers required by accounting standards. For instance, under IFRS 15, revenue must be recognized when control over a promised good or service transfers, and under IFRS 9, impairments must reflect changes in expected credit losses. Automation can amplify errors if business rules diverge from accounting policies, making rigorous change management, testing, and version control vital to ensure accurate reporting (IFRS Foundation, 2023).

Classification of new digital products also poses challenges. Emerging instruments such as stored-value wallets, platform credits, loyalty tokens, or tokenized securities require careful assessment to determine whether they constitute financial instruments under IFRS 9 or intangible assets under IAS 38. For example, e-money or stored-value balances generally represent liabilities, reflecting an obligation to customers, unless the legal form alters the underlying economic substance. Proper classification directly impacts subsequent measurement and disclosure requirements.

Revenue recognition in platform-based models adds further complexity. Banks often collaborate with platform partners, splitting roles as principal or agent. IFRS 15 requires evaluation of whether the entity controls the service before it is transferred. If acting as a principal, revenue is recognized on a gross basis, including fees and interchange; if acting as an agent, only net commission is recognized. Layered digital fees, such as API access, merchant charges, and interchange, require

detailed contract analysis and robust documentation to ensure compliance with revenue recognition principles.

Expected Credit Loss (ECL) modeling under IFRS 9 benefits from the rich behavioral and transactional data available in digital banking. High-frequency data can enhance forward-looking models but introduces governance challenges. Data quality, lineage, model explainability, and validation—particularly for non-traditional inputs—are critical for auditability and regulatory review. The European Banking Authority (2023) highlights practical issues around comparability and model limitations.

Valuation of digital assets presents additional challenges. Many trade on fragmented platforms, requiring careful selection of market inputs and disclosure of the fair value hierarchy level. For tokenized instruments representing contractual rights, valuation must reflect the underlying economics rather than the digital wrapper, emphasizing transparency and sensitivity analyses under IFRS 13.

Finally, intercompany and platform revenue allocation adds complexity in multi-jurisdictional contexts. Transfer pricing, tax treatment, and coordinated recognition across entities require collaboration between accounting, tax, and compliance teams to maintain consistent, accurate reporting. Collectively, these practical issues underscore the need for robust governance, documentation, and control frameworks in digital banking environments.

### 3. Digital Reporting — Taxonomies, Machine-Readable Statements and Continuous Reporting

Digital reporting represents a transformative opportunity for banks, particularly in the context of machine-readable financial statements and continuous reporting. Central to this development is the IFRS Accounting Taxonomy, published and regularly updated by the IFRS Foundation, most recently in 2024. The taxonomy provides a structured framework for tagging financial statement elements, enabling both numeric and narrative disclosures to be captured in a machine-readable format. For digital banks, adopting this taxonomy facilitates automated data extraction, enhances comparability across institutions, and allows investors, supervisors, and other stakeholders to analyze financial information more quickly and accurately (IFRS Foundation, 2024).

The practical benefits of digital reporting for banking institutions are substantial. Machine-readable tagging reduces the reliance on manual re-keying of regulatory submissions, thereby minimizing operational errors and increasing efficiency. Additionally, integration with internal systems allows for seamless reconciliation between management accounts and statutory reporting, promoting consistency and accuracy in financial information. Perhaps most notably, digital reporting supports continuous or near-real-time supervisory reporting where permitted by regulators. This capability allows banking supervisors to monitor liquidity, capital adequacy, and risk exposures more dynamically, improving the resilience and transparency of the financial system (IFRS Foundation, 2024).

Despite these advantages, digital reporting also presents implementation challenges. The IFRS taxonomy may lag in coverage for emerging digital banking items such as tokenized assets, API-related fees, or platform-specific service revenues. Consequently, banks must maintain detailed mapping documents and provide narrative explanations until the taxonomy fully incorporates these elements. Robust governance over tagging processes, validation controls, and documentation is essential to ensure accuracy and auditability. Additionally, while jurisdictional extensions of the IFRS taxonomy are encouraged, the IFRS Foundation emphasizes technology neutrality, allowing banks to implement solutions compatible with diverse systems and software platforms (IFRS Foundation, 2024).

## 4. Governance, Controls and Auditability in Automated Environments

In automated banking environments, governance, controls, and auditability are critical to ensuring the integrity and reliability of financial reporting. As accounting policies become codified into executable business rules within accounting engines, cross-functional ownership between finance, IT, and functional units becomes essential. This integration requires robust version control, systematic testing, and well-documented change management procedures to prevent errors from propagating through automated processes. According to Deloitte (2023), ensuring that automated systems faithfully implement accounting policies is fundamental to maintaining compliance with IFRS and other regulatory standards.

Data governance and lineage form another cornerstone of control in automated environments. Traceability from source events to published financial figures allows auditors and supervisors to verify and reproduce reported numbers accurately. Banks are increasingly employing metadata registries, data lineage tools, and reconciliation frameworks to maintain transparency across complex digital accounting architectures. Such practices enhance internal controls and facilitate regulatory and supervisory reviews, particularly in high-volume, real-time transaction settings (COSO, 2023).

Model risk management is also a central concern. Many IFRS-based estimates, such as Expected Credit Loss (ECL) under IFRS 9 or fair value measurements under IFRS 13, rely on statistical or machine learning models. The European Banking Authority (EBA, 2023) emphasizes that effective governance of these models—including development, validation, monitoring, and oversight by governance committees—is essential to ensure both prudential and accounting compliance. Documenting assumptions, methodologies, and limitations is vital to support auditability, regulatory scrutiny, and internal decision-making.

Continuous assurance is an emerging feature of automated financial reporting. Real-time posting and digital audit trails enable internal and external auditors to adopt continuous auditing methodologies, moving away from traditional periodic sample testing. Access to tagged financial statements, system logs, and structured data extracts allows auditors to monitor transaction-level data and assess control effectiveness on an ongoing basis. This approach improves the timeliness and reliability of audit evidence while addressing risks associated with automation and complex digital processes (Vasarhelyi et al., 2015).

## B. Fair Value Measurement in Digital Assets and Liabilities

Fair value measurement has become increasingly significant in the digital banking environment, particularly as banks engage with digital assets, complex financial instruments, and technology-driven liabilities. Digital banking accelerates transaction speed, expands product innovation, and introduces new asset classes such as crypto-assets, tokenized instruments, and embedded digital derivatives that

often require fair value accounting rather than historical cost measurement. Under IFRS and PSAK, fair value aims to provide relevant and market-based information that reflects current economic conditions. However, applying fair value measurement to digital assets and liabilities presents conceptual, technical, and governance challenges. According to IFRS 13 (IFRS Foundation, 2023), fair value measurement must reflect an orderly transaction between market participants, a requirement that becomes complex in volatile, fragmented, and technology-driven digital markets.

## 1. Conceptual Basis of Fair Value under IFRS and PSAK

The conceptual basis of fair value under IFRS and PSAK provides a consistent framework for measuring assets and liabilities at market-based prices rather than entity-specific values. IFRS 13 defines fair value as the price that would be received to sell an asset or paid to transfer a liability in an orderly transaction between market participants at the measurement date (IFRS Foundation, 2023). PSAK adopts the same definition, reflecting Indonesia's commitment to international convergence and ensuring that financial statements provide comparable, relevant, and reliable information. The primary objective of fair value measurement is to capture an exit price that represents the perspective of market participants, rather than the internal or strategic intentions of the reporting entity. This approach supports transparency and decision-usefulness in financial reporting, particularly for users assessing liquidity, risk, and performance.

In the context of digital banking, fair value measurement extends beyond traditional financial instruments, such as trading securities, derivatives, and loans, to include digital-native assets and liabilities. Examples include tokenized financial instruments, digital payment obligations, and certain crypto-assets that may meet the criteria for financial instrument classification under IFRS 9 or intangible asset recognition under IAS 38. The conceptual framework requires that these measurements incorporate market-based assumptions, reflecting the price at which independent market participants would transact under normal market conditions. This ensures that valuations are neither inflated by internal expectations nor constrained by technological infrastructure.

Key elements of the fair value concept include the principal (or most advantageous) market, the valuation technique, and the use of observable inputs where available. IFRS 13 emphasizes a hierarchy of inputs, with Level 1 inputs being quoted prices in active markets, Level 2 inputs being observable market data for similar instruments, and Level 3 inputs requiring unobservable assumptions when market data is insufficient. In digital banking, the application of these principles may involve additional challenges due to fragmented markets, limited liquidity for tokenized assets, or the need to incorporate alternative data sources for valuation purposes.

## 2. Digital Assets Subject to Fair Value Measurement

Digital assets increasingly play a central role in modern banking, and many of these assets are subject to fair value measurement to ensure transparent and decision-useful financial reporting. Common digital assets that require fair value accounting include crypto-assets held for trading purposes, tokenized securities and deposits, digital derivatives embedded in fintech products, and investments in fintech platforms measured at fair value. These instruments often exhibit high volatility and are traded in fragmented or rapidly evolving markets, making traditional cost-based measurement less informative for stakeholders. For banks that actively trade or hold digital assets for liquidity management or market-making purposes, reporting at fair value through profit or loss provides a real-time reflection of economic conditions and enhances the comparability of financial statements across entities and periods (Deloitte, 2023).

Fair value measurement of these assets requires banks to apply market-based assumptions that reflect the price at which independent participants would transact. For crypto-assets, this may involve using observable exchange rates, quoted market prices, or, in cases where markets are illiquid, applying valuation models with unobservable inputs consistent with IFRS 13 and PSAK guidelines. Tokenized securities, which represent ownership or contractual rights on underlying assets, are measured similarly, with valuation focused on the underlying economic substance rather than the digital wrapper. Digital derivatives embedded in fintech products, such as options or structured notes, also require fair value accounting, incorporating both market inputs and contractual terms to capture risk exposure accurately.

Investments in fintech platforms, whether in the form of equity stakes or other digital holdings, are also frequently measured at fair value when the bank intends to hold them for trading, strategic purposes, or potential disposal. Fair value reporting for these assets provides timely insights into the bank's exposure to innovation-driven financial products and the associated market risks. According to Deloitte (2023), this approach strengthens transparency, aids risk management, and facilitates informed decision-making by investors, regulators, and management.

### 3. Fair Value Measurement of Digital Liabilities

In digital banking, certain liabilities are increasingly subject to fair value measurement, reflecting the evolving nature of financial products and contractual obligations. Examples include derivative liabilities linked to digital products, obligations arising from tokenized instruments, and structured digital deposits with embedded options. These liabilities often feature complex payoff structures, high interconnectivity with other digital assets, and execution through automated platforms or smart contracts, which can create additional challenges for accurate measurement. According to IFRS 13, fair value measurement of liabilities must consider the price that would be paid to transfer the obligation in an orderly transaction, incorporating both market conditions and the entity's own credit risk. This contrasts with assets, where market participant assumptions primarily focus on observable prices and market conditions (IFRS Foundation, 2023).

In practice, digital banking liabilities require sophisticated valuation techniques that integrate credit risk, liquidity, and market inputs. Derivative liabilities, such as options or swaps embedded in digital products, demand continuous monitoring of underlying digital asset prices, volatility, and counterparty creditworthiness. Tokenized instruments that represent contractual obligations, whether in the form of digital bonds or redeemable tokens, necessitate careful modeling to capture the fair value of redemption or settlement obligations. Structured digital deposits with embedded options, including early withdrawal rights or interest rate-linked features, further complicate the measurement process due to the need to assess potential future cash flows under varying market scenarios. PwC (2023) emphasizes that accurate valuation in these contexts requires incorporating realistic

assumptions about the entity's own credit risk, funding costs, and potential liquidity constraints.

Furthermore, the automated execution of these liabilities through smart contracts or digital platforms introduces operational considerations. For example, the timing of cash flows, automated triggers, and embedded contractual terms must be accurately reflected in the valuation model to ensure faithful representation. Banks must also maintain robust documentation and governance over the valuation process, ensuring transparency and auditability in accordance with regulatory expectations.

### 4. Fair Value Hierarchy and Digital Instruments

In digital banking and finance, fair value measurement of digital instruments must consider the IFRS 13 fair value hierarchy, which classifies assets and liabilities based on the observability and reliability of inputs used in valuation. Level 1 inputs consist of quoted prices in active markets for identical instruments and provide the most reliable measurement. Level 2 inputs involve observable data other than quoted prices, such as market-corroborated prices for similar instruments or interest rates, while Level 3 inputs are unobservable and rely heavily on management assumptions, internal models, or non-transparent market data (IFRS Foundation, 2023).

Digital assets, including cryptocurrencies, tokenized securities, and certain structured digital instruments, frequently fall into Level 2 or Level 3 due to the fragmented nature of digital markets, limited liquidity, and the absence of standardized trading venues. For example, a cryptocurrency that is traded on multiple exchanges with varying prices may require a Level 2 valuation using averaged or adjusted market inputs. In contrast, tokenized instruments representing rights to underlying assets without active trading markets typically require Level 3 measurement, necessitating model-based valuations that incorporate unobservable inputs such as expected cash flows, discount rates, and probability-weighted outcomes (KPMG, 2023).

The classification into these levels carries important disclosure implications. Level 2 measurements require an explanation of the observable inputs used and the rationale for adjustments made to reflect fair value. Level 3 measurements demand far more detailed disclosures, including the valuation techniques applied, key assumptions, and

sensitivity analyses illustrating how changes in inputs could impact the reported value. This transparency is crucial for users of financial statements to understand the estimation uncertainty inherent in digital instruments.

The increasing prevalence of Level 3 digital assets underscores the importance of professional judgment, governance, and robust documentation. Banks and financial institutions must implement strong controls over model development, validation, and monitoring to ensure that fair value estimates are reasonable and consistent with IFRS 13 requirements. Additionally, sensitivity analyses help users assess potential volatility in reported values and enhance confidence in financial reporting (KPMG, 2023).

## C. Automated Financial Reporting Systems

Automated financial reporting systems represent a critical advancement in the digital transformation of banking and financial institutions. As transaction volumes increase, reporting requirements become more complex, and stakeholders demand real-time, accurate financial information, manual reporting processes are no longer sufficient. Automated financial reporting systems integrate accounting standards, digital transaction data, and advanced technologies such as enterprise resource planning (ERP), artificial intelligence, and cloud computing to generate timely, consistent, and reliable financial reports. According to Vasarhelyi, Kogan, and Tuttle (2015) and reaffirmed by recent studies (Deloitte, 2023; IFRS Foundation, 2024), automation is reshaping financial reporting from a periodic compliance exercise into a continuous and value-creating process.

### 1. Concept and Evolution of Automated Financial Reporting

Automated financial reporting represents a significant evolution in the way financial information is collected, processed, and communicated, particularly in digital banking environments. Traditionally, financial reporting relied heavily on manual processes, including journal entries, spreadsheet-based consolidations, and periodic adjustments performed at the end of reporting periods. These methods were often time-consuming, prone to errors, and limited in their ability to provide timely insights for decision-making. In contrast,

automated financial reporting leverages integrated information systems that capture financial events in real time and automatically translate them into accounting records, minimizing the need for manual intervention. Modern systems are typically built on core banking platforms, enterprise resource planning (ERP) solutions, and centralized data warehouses, where predefined accounting rules aligned with IFRS and PSAK standards ensure consistency, accuracy, and compliance across the organization (SAP, 2023).

The evolution of automated reporting is closely linked to the increasing digitalization of banking operations. Transactions initiated through online channels, mobile applications, or digital payment platforms feed directly into accounting engines, enabling straight-through processing and continuous updates of account balances and financial positions. This real-time capture not only accelerates the preparation of financial statements but also supports continuous monitoring and internal control activities. Automated systems can apply complex accounting treatments, including revenue recognition, fair value measurement, and impairment calculations, without manual calculation, thereby reducing operational risk and enhancing auditability.

According to SAP (2023), the benefits of automated financial reporting extend beyond efficiency gains. Data consistency and standardization across business units are improved, as all transactions are processed according to uniform rules embedded in the system. Reporting cycles are accelerated, allowing management and stakeholders to access timely, accurate, and decision-useful information. Moreover, automation facilitates enhanced transparency and traceability, as digital audit trails provide comprehensive records of every transaction, supporting both internal and external audits.

## 2. Key Components of Automated Financial Reporting Systems

Automated financial reporting systems in digital banking are composed of several interconnected components that collectively ensure accurate, timely, and compliant financial reporting. At the foundation of these systems are transaction capture systems, which record financial events directly from digital channels such as mobile banking applications, payment gateways, and application programming interfaces (APIs). Each transaction is automatically tagged with

relevant accounting attributes, including account codes, valuation methods, and reporting classifications, enabling immediate recognition and integration into the accounting system. This real-time capture reduces manual intervention, minimizes errors, and ensures that all digital transactions are accurately reflected in financial records.

Central to the system's functionality is the accounting rules engine. This component encodes accounting standards and policies, including IFRS and PSAK principles, into executable rules that govern the recognition, measurement, and classification of transactions. By automating these processes, the rules engine ensures consistent application of accounting principles across all business units and transaction types, including complex digital products such as tokenized instruments, e-wallet balances, and platform fees. This consistency is critical for maintaining reliable financial statements and supporting auditability.

Complementing the rules engine is the data integration and consolidation layer, which aggregates financial information from multiple subsidiaries, digital platforms, and business units. Cloud-based consolidation tools enable real-time group reporting, allowing banks to monitor financial positions and performance across jurisdictions seamlessly. According to KPMG (2023), automated consolidation enhances efficiency, reduces reconciliation efforts, and supports faster financial close cycles, particularly in organizations with complex, multi-platform operations.

The final component consists of reporting and visualization tools, which generate financial statements, regulatory submissions, and management dashboards using predefined templates and analytics capabilities. These tools allow for customizable, near-real-time reporting, facilitating internal decision-making and compliance with regulatory requirements. Advanced analytics within these tools can also provide insights into trends, risks, and performance indicators, supporting strategic management and oversight.

### 3. Benefits of Automation in Financial Reporting

The adoption of automated financial reporting systems in digital banking and finance delivers significant strategic and operational benefits that enhance the overall quality and efficiency of accounting processes. One of the primary advantages is timeliness, as automation

enables near real-time financial reporting. Transactions captured through digital channels such as mobile banking, payment gateways, and APIs are immediately processed and recorded in the accounting system, significantly reducing the time lag between the occurrence of economic events and their financial disclosure. This rapid reporting capability allows banks and financial institutions to respond quickly to operational, liquidity, and regulatory requirements, supporting better decision-making and risk management.

Another key benefit is improved accuracy and consistency. Automated systems minimize human intervention in data entry, posting, and consolidation processes, thereby reducing the risk of errors, omissions, and inconsistencies that are often associated with manual accounting. By applying predefined accounting rules aligned with IFRS and PSAK standards, these systems ensure that transactions are consistently recognized, measured, and classified across all business units and product lines. This consistency not only strengthens the reliability of financial statements but also facilitates auditability and regulatory scrutiny. According to the IFRS Foundation (2024), embedding accounting standards directly into reporting engines ensures adherence to recognition, measurement, and disclosure principles, reinforcing trust in financial reporting outputs.

Automated financial reporting also supports regulatory compliance. By integrating supervisory reporting requirements into the system, banks can generate regulatory submissions in line with both local and international frameworks, reducing the risk of non-compliance and associated penalties. Systematized compliance checks and tagging of reports also support transparency, traceability, and continuous monitoring, meeting the growing expectations of regulators and auditors.

## 4. Automation Technologies Supporting Financial Reporting

Automation technologies have become foundational to modern financial reporting, enabling banks and financial institutions to enhance accuracy, efficiency, and timeliness in their accounting processes. Enterprise Resource Planning (ERP) systems serve as the backbone of these automated environments by integrating accounting, operational, and risk data into a unified platform. This centralization ensures that transactions from diverse business units, digital channels, and

subsidiaries are recorded consistently, supporting both internal reporting and regulatory compliance. ERP platforms also provide structured workflows and predefined accounting rules, aligning system processes with IFRS and PSAK standards, thereby reducing manual intervention and enhancing data integrity.

Robotic Process Automation (RPA) further complements ERP systems by automating repetitive, rule-based tasks such as reconciliations, data extraction, journal posting, and inter-system data transfers. By reducing human involvement in these high-volume processes, RPA minimizes errors, accelerates transaction processing, and frees accounting staff to focus on more analytical and strategic responsibilities. According to PwC (2023), RPA adoption in financial reporting leads to significant reductions in processing time and operational risk, particularly in environments with complex, high-frequency transactions such as digital banking and treasury operations.

Artificial Intelligence (AI) adds an advanced layer of analytical capability to automated financial reporting. AI algorithms can detect anomalies, predict potential adjustments, and validate accounting data intelligently, improving both the quality and reliability of financial information. Machine learning models can also identify patterns across historical transaction data, supporting more accurate accrual estimates, revenue recognition, and forecasting. Deloitte (2023) highlights that AI-driven validation enhances both internal control effectiveness and audit readiness, as system-generated alerts and insights can guide accountants in investigating unusual transactions promptly.

Cloud computing underpins these technologies by offering scalable infrastructure, high availability, and seamless integration across multiple entities and geographies. Cloud-based reporting platforms facilitate near-real-time consolidation, allowing banks to generate financial statements and regulatory reports quickly and consistently. They also support remote access and collaboration, which are increasingly important in globally distributed organizations and digital banking operations. McKinsey (2023) notes that banks leveraging the combination of ERP, AI, RPA, and cloud computing achieve faster financial close cycles, improved data reliability, and enhanced responsiveness to regulatory and supervisory requirements.

## D. Data-Driven Decision-Making and Predictive Analytics

Data-driven decision-making and predictive analytics have become central pillars of financial reporting and management in the digital banking era. As banks generate massive volumes of structured and unstructured data from digital transactions, customer interactions, and external market sources, traditional descriptive reporting is no longer sufficient. Modern financial reporting systems increasingly incorporate advanced analytics and predictive models to support forward-looking decisions, risk management, and strategic planning. According to Marr (2022) and BIS (2023), predictive analytics enables banks not only to understand past performance but also to anticipate future trends, risks, and opportunities with greater accuracy.

### 1. Concept of Data-Driven Decision-Making in Digital Banking

Data-driven decision-making in digital banking represents a paradigm shift from intuition-based or retrospective management approaches to a model grounded in empirical evidence and analytical rigor. This concept entails leveraging vast amounts of structured and unstructured data generated through banking operations, customer interactions, and market activities to inform strategic and operational choices. Rather than relying solely on historical financial statements or periodic reports, banks now integrate real-time transaction data, behavioral analytics, and predictive models into their decision-making processes. By doing so, management gains a more dynamic and granular understanding of performance, risk exposure, and customer needs, enabling more timely and effective responses to market fluctuations.

In practice, data-driven decision-making transforms financial reporting systems into active analytical platforms. Modern digital banking platforms capture data from multiple sources, including mobile applications, online banking transactions, payment gateways, and social or alternative data channels. These data streams are processed through advanced analytics, artificial intelligence, and machine learning algorithms to identify patterns, trends, and anomalies that would be difficult to detect through traditional reporting. For example, predictive models can assess a customer's creditworthiness based on transaction history, income patterns, and external economic indicators, thereby

improving the accuracy of lending decisions while mitigating default risk. Similarly, liquidity management and cash flow forecasting benefit from real-time aggregation of payment and settlement data, allowing banks to optimize reserve allocations and capital deployment more efficiently.

Davenport and Harris (2017) emphasize that organizations that systematically embed analytics into their decision-making processes consistently outperform those relying on intuition or static historical analysis. In digital banking, the application of data-driven insights extends beyond risk management and operational efficiency to strategic areas such as dynamic pricing, product personalization, and portfolio optimization. Banks can adjust interest rates, fees, or rewards programs based on predictive models that anticipate customer behavior, competitive positioning, and macroeconomic trends.

## 2. Sources of Data for Financial Analytics

In digital banking, financial analytics relies on a wide range of data sources that collectively provide a comprehensive view of operations, customer behavior, and market conditions. Transactional data forms the backbone of financial analytics, encompassing information from core banking systems, payment networks, and digital channels such as mobile and online banking platforms. This data includes account balances, transfers, deposits, withdrawals, loan disbursements, and payment histories, offering granular insights into cash flows, liquidity positions, and revenue streams. When captured in near real-time, transactional data enables dynamic monitoring of financial performance and risk exposure, supporting more timely and informed decision-making.

Customer data represents another critical source, derived from customer relationship management (CRM) systems, mobile applications, and other digital touchpoints. Information such as demographic profiles, transaction preferences, digital behavior patterns, and engagement metrics allows banks to segment clients, predict future needs, and personalize financial products. For instance, data-driven insights can inform targeted lending offers, cross-selling strategies, or dynamic pricing models, enhancing both revenue generation and customer satisfaction.

Risk and compliance data is equally essential, encompassing credit risk models, market risk positions, operational risk incidents, and regulatory reporting records. Integrating this data into financial analytics enables banks to identify potential vulnerabilities, assess exposure to adverse scenarios, and ensure adherence to regulatory requirements. Advanced analytics can detect anomalies or emerging trends, allowing proactive risk mitigation and enhanced internal controls.

External data sources complement internal information by providing context and predictive signals. Macroeconomic indicators, market prices, interest rate movements, and alternative data such as social media sentiment, geolocation trends, or industry-specific metrics enable banks to incorporate external environmental factors into their financial models. This enhances forecasting accuracy, supports scenario planning, and informs strategic decisions under varying market conditions.

## 3. Predictive Analytics Techniques in Financial Reporting

Predictive analytics has become a cornerstone of modern financial reporting in digital banking, enabling institutions to move beyond traditional backward-looking reports and incorporate forward-looking insights into decision-making processes. By leveraging historical and real-time data, predictive analytics employs statistical, machine learning, and artificial intelligence techniques to forecast future financial outcomes, assess risks, and optimize operational strategies. Regression and time-series models are widely used for forecasting revenue, operational costs, and liquidity positions, allowing banks to anticipate cash flow requirements, plan capital allocation, and manage funding needs proactively. These models rely on patterns in past financial data and can be continuously updated as new information becomes available, providing dynamic and granular insights into future performance trends.

Machine learning algorithms further expand the predictive capabilities of financial reporting by identifying complex, non-linear relationships that traditional models may overlook. For example, banks employ machine learning to predict credit default probabilities, detect fraudulent transactions, and segment customers based on behavioral patterns. These models can automatically learn from new data,

improving their accuracy over time and enabling financial institutions to respond more quickly to emerging risks or opportunities. Scenario analysis and stress testing models complement these techniques by simulating adverse economic conditions, regulatory changes, or operational disruptions, allowing banks to evaluate the resilience of capital positions and liquidity buffers. Such forward-looking assessments are critical for meeting regulatory expectations and enhancing strategic planning (Marr, 2022).

Natural language processing (NLP) represents another important predictive tool, particularly for analyzing unstructured data such as financial disclosures, analyst reports, and market news. By extracting sentiment, trends, and relevant quantitative information from textual sources, NLP supports more nuanced assessments of market dynamics, risk factors, and potential regulatory impacts. The integration of NLP into predictive analytics enables banks to incorporate qualitative information alongside quantitative data, enhancing the comprehensiveness and contextual relevance of financial reporting.

### 4. Integration of Predictive Analytics with Financial Reporting

The integration of predictive analytics into financial reporting represents a significant evolution in how banks and financial institutions manage, interpret, and communicate financial information. Traditional reporting focused primarily on historical data, summarizing past transactions and financial positions. However, in digital banking environments, the rapid flow of data from multiple channels core banking systems, digital payments, mobile apps, and external market sources creates opportunities to embed predictive models directly into financial reports and dashboards, providing forward-looking insights that enhance both decision-making and regulatory compliance. Key financial indicators, including expected credit loss (ECL), liquidity coverage ratios, profitability measures, and revenue forecasts, are increasingly informed by predictive analytics, allowing management to anticipate trends and respond proactively to potential risks.

Under IFRS 9, the calculation of ECL explicitly requires the use of forward-looking information to estimate potential credit losses over the life of a financial instrument. Predictive analytics facilitates this process by analyzing historical borrower behavior, macroeconomic

trends, and other relevant variables to generate probabilistic forecasts of defaults and credit impairments. By integrating these forecasts into financial reporting systems, banks can produce estimates that are not only compliant with international standards but also more dynamic and responsive to changes in economic conditions. The IFRS Foundation (2023) emphasizes that such integration strengthens the relevance and reliability of financial information, ensuring that financial statements reflect both current conditions and expected future events.

In the Indonesian context, PSAK adoption similarly underscores the importance of forward-looking, reasonable, and supportable information in measurement and disclosure. Digital banks operating in Indonesia must ensure that predictive models align with PSAK requirements, particularly for ECL, provisioning, and risk-sensitive metrics. Integration of predictive analytics enables continuous updates to these estimates, enhancing transparency and enabling real-time management reporting. Predictive models can be embedded within dashboards that present both historical performance and forecasted outcomes, allowing executives to monitor trends in credit quality, liquidity, and operational efficiency.

# CHAPTER VII
# DIGITAL RISK ACCOUNTING AND MANAGEMENT

Digital Risk Accounting and Management has become a critical discipline in modern banking as financial institutions increasingly rely on digital technologies, automated decision systems, and real-time transactions. The integration of accounting with digital risk management enables banks to identify, measure, and disclose financial risks more accurately while responding to the growing complexity of credit, market, liquidity, operational, and cyber risks. In a digital environment where risks materialize rapidly and are highly interconnected, accounting frameworks such as IFRS 9 and regulatory guidelines from the Basel Committee emphasize forward-looking measurement, transparency, and resilience. As highlighted by BIS (2023) and the IFRS Foundation (2023), effective digital risk accounting is essential to safeguarding financial stability, supporting regulatory compliance, and enhancing strategic decision-making in the digital banking era.

## A. Credit, Market, Liquidity and Operational Risks

Risk is inherent in all banking activities, and effective risk accounting is essential for ensuring financial stability, regulatory compliance, and informed decision-making. In the digital era, traditional banking risks credit, market, liquidity, and operational risks have not diminished; instead, they have become more complex, faster-moving, and highly interconnected due to digital platforms, automation, real-time transactions, and advanced analytics. According to the Basel Committee on Banking Supervision (2023), digitalization increases both the velocity and transmission channels of banking risks, requiring more dynamic measurement, recognition, and disclosure within financial reporting systems. This section discusses the four core

banking risks and their implications for accounting and risk management in digital banking environments.

### 1. Credit Risk

Credit risk represents the potential that a borrower or counterparty will fail to fulfill its contractual obligations, creating financial exposure for the lending institution. In traditional banking, credit risk primarily concerns loans, advances, and trade receivables, where the likelihood of default is assessed through historical repayment behavior and established credit evaluation processes. However, the rapid expansion of digital banking has transformed the nature and scope of credit risk. With the proliferation of digital lending platforms, instant credit approvals, and alternative credit scoring models, banks are now exposed to a broader and faster-moving set of credit exposures. Automated decision systems, artificial intelligence, and machine learning algorithms increasingly underpin credit assessment, leveraging not only traditional financial data but also alternative sources, such as transactional behavior, mobile application usage, and e-commerce activity. While these innovations enhance operational efficiency and broaden financial inclusion, they simultaneously introduce model risk, data quality challenges, and heightened dependency on algorithmic accuracy (BIS, 2023).

From an accounting perspective, credit risk critically influences loan classification, impairment recognition, and the measurement of expected credit losses (ECL) under IFRS 9. Loans are categorized into stages based on changes in credit risk, which in turn determines the calculation of impairments and the timing of loss recognition. In digital banking environments, where loan origination volumes are high and approvals occur in near real-time, financial institutions must implement automated monitoring and impairment calculation mechanisms to capture credit deterioration promptly. IFRS 9 requires that forward-looking information be incorporated into credit risk assessments, including both macroeconomic indicators and borrower-specific risk factors. For digital lenders, this means integrating real-time economic data, behavioral signals, and stress-testing outputs into the ECL models to ensure faithful representation of credit exposures (IFRS Foundation, 2023).

The use of alternative data sources and predictive analytics also affects provisioning and disclosure requirements. Digital banks must ensure that their automated models are validated regularly, data inputs are of high quality, and assumptions are transparent and justifiable to auditors and regulators. Effective credit risk management in digital banking thus demands a combination of advanced technology, rigorous accounting standards compliance, and robust governance frameworks. By integrating real-time monitoring, predictive modeling, and automated accounting processes, banks can maintain financial stability, ensure regulatory compliance, and provide timely recognition of potential losses, thereby enhancing both operational efficiency and stakeholder confidence in the integrity of reported financial information.

**2. Market Risk**

Market risk refers to the potential for financial loss resulting from adverse changes in market variables such as interest rates, foreign exchange rates, equity prices, and commodity prices. In the context of digital banking, market risk is increasingly significant due to the widespread adoption of real-time trading platforms, algorithmic pricing engines, and automated treasury operations. These technological advancements allow banks to execute high-frequency transactions and manage large portfolios of financial instruments, but they also amplify exposure to rapid market fluctuations. Institutions holding assets and liabilities at fair value including trading securities, derivatives, and emerging digital financial instruments face heightened sensitivity to price volatility. IFRS 13 mandates that financial instruments be measured using observable market inputs wherever possible, while valuation models are applied when markets are illiquid or data is limited, ensuring that reported fair values reflect an exit price consistent with market participant assumptions (IFRS Foundation, 2023).

Digitalization, while enhancing market transparency, can also increase short-term volatility. Automated trading systems and algorithmic strategies may create rapid price swings, sometimes disconnected from fundamental values, making timely recognition of gains and losses critical. From an accounting perspective, market risk has a direct impact on several reporting elements. Fair value measurement affects both profit or loss and other comprehensive

income (OCI), influencing reported earnings and equity. Profit or loss volatility must be monitored carefully, and risk disclosures in financial statements are increasingly required to provide stakeholders with insights into the nature, extent, and management of market risk exposures. This includes sensitivity analyses, valuation techniques, and assumptions used in pricing complex instruments.

To mitigate these risks, digital banks employ robust valuation models, automated control mechanisms, and independent price verification processes. Risk management frameworks often integrate real-time monitoring dashboards that track market movements and their impact on portfolio valuations, enabling prompt intervention where necessary. According to Jorion (2021), the combination of high-frequency trading and automated systems necessitates continuous updating of models and controls to ensure accuracy and reliability of financial reporting. Moreover, scenario analysis and stress testing complement traditional valuation techniques, providing forward-looking assessments of potential losses under extreme market conditions. By embedding these practices into digital accounting and reporting systems, banks enhance transparency, strengthen regulatory compliance, and maintain stakeholder confidence in financial statements despite the inherent volatility of digital financial markets.

### 3. Liquidity Risk

Liquidity risk represents the possibility that a bank will not be able to meet its financial obligations as they fall due, potentially forcing the institution to incur significant losses or distress costs. In the context of digital banking, liquidity risk dynamics have evolved considerably due to the proliferation of real-time payments, continuous 24/7 banking access, and instantaneous fund transfers via mobile and online channels. Unlike traditional banking, where withdrawals and transfers are constrained by branch hours or processing cycles, digital banking allows customers to move substantial sums at any moment, sometimes simultaneously, which can amplify sudden liquidity pressures. The Bank for International Settlements (BIS, 2023) emphasizes that high-speed digital payment systems can accelerate liquidity shocks, particularly during periods of market stress or operational disruptions, highlighting the need for proactive liquidity risk management.

From an accounting perspective, liquidity risk has several critical implications. Accurate and timely preparation of cash flow statements becomes essential, as these provide insights into expected inflows and outflows of funds, enabling management to anticipate potential shortfalls. The classification of assets and liabilities by liquidity and maturity is equally important, as it informs both internal decision-making and regulatory reporting. Banks must ensure that highly liquid assets are distinguishable from longer-term or illiquid investments, supporting the maintenance of adequate buffers to meet short-term obligations. Moreover, liquidity risk directly affects disclosure requirements, including maturity analyses and scenario-based projections, which are increasingly scrutinized by regulators and stakeholders to evaluate a bank's capacity to withstand liquidity stress.

Modern digital banking institutions leverage automated liquidity monitoring and management systems that are closely integrated with accounting and core banking platforms. These systems provide real-time visibility into cash positions, funding gaps, and potential liquidity stress points, allowing banks to react promptly to emerging risks. Such integration supports compliance with regulatory liquidity metrics, such as the Liquidity Coverage Ratio (LCR) and Net Stable Funding Ratio (NSFR), which require banks to maintain sufficient high-quality liquid assets to survive periods of financial stress. According to Deloitte (2023), embedding liquidity management tools within automated accounting systems not only enhances the accuracy of financial reporting but also strengthens operational resilience by enabling scenario modeling, stress testing, and predictive funding assessments.

### 4. Operational Risk

Operational risk refers to the potential for loss resulting from inadequate or failed internal processes, human error, system malfunctions, or external events. In the context of digital banking, operational risk has become increasingly technology-centric, as banks rely heavily on digital platforms, automated processes, and real-time transaction systems. Key sources of operational risk in digital banking include system failures or outages, cybersecurity breaches, data leaks, and errors arising from automated processes or algorithmic decision-making. As COSO (2023) emphasizes, the digital transformation of

banking operations shifts the focus of operational risk from traditional manual procedures to technological infrastructure, creating greater dependency on system reliability, resilience, and cybersecurity controls.

From an accounting perspective, operational risk can have several direct and indirect impacts on financial reporting. When loss events occur such as cyber-attacks, system failures, or regulatory fines banks must recognize the financial implications promptly, either through direct loss recognition or the establishment of provisions for contingent liabilities. This may include provisions for potential legal and regulatory penalties, costs associated with remediation efforts, or compensation to affected customers. Additionally, material incidents related to operational risk often require explicit disclosure in financial statements to maintain transparency and provide stakeholders with a comprehensive understanding of risk exposure. In cases where operational disruptions impair the functionality or value of digital assets or systems, banks may need to assess impairment losses in accordance with relevant accounting standards, such as IFRS 9 for financial instruments or IAS 36 for non-financial assets.

Automated systems and digital infrastructure enhance the reliability of operational risk accounting by enabling continuous monitoring, exception reporting, and detailed audit trails. Digital logging tools capture time-stamped records of system events, transactions, and user activities, which not only facilitate real-time detection of anomalies but also support post-incident analysis and regulatory review. According to PwC (2023), embedding operational risk controls into automated processes such as transaction validation engines, access management, and anomaly detection algorithms helps mitigate losses and ensures that operational risk events are accurately captured, measured, and reported in financial statements.

## B. Expected Credit Loss (ECL / CKPN) Under IFRS 9

The introduction of IFRS 9 Financial Instruments marked a fundamental shift in credit risk accounting by replacing the incurred loss model with the Expected Credit Loss (ECL) approach. This forward-looking model requires banks to recognize credit losses earlier and more comprehensively, reflecting not only historical defaults but

also current conditions and future economic expectations. In the context of digital banking, where credit decisions are increasingly automated and loan portfolios are highly granular and dynamic, the ECL framework becomes even more critical. According to the IFRS Foundation (2023) and Basel Committee on Banking Supervision (2023), robust ECL implementation is central to financial stability, transparency, and prudential risk management.

## 1. Conceptual Foundation of the ECL Model

The Expected Credit Loss (ECL) model represents a fundamental shift in accounting for credit risk, emphasizing forward-looking recognition of potential losses rather than waiting for evidence of incurred loss. Under IFRS 9, the ECL framework applies to a broad range of financial instruments, including loans and advances, debt securities measured at amortized cost or fair value through other comprehensive income (FVOCI), as well as loan commitments and financial guarantee contracts. The core concept of ECL is to estimate the present value of expected shortfalls over the life of a financial asset, integrating both the probability of default and potential exposure at the time of default. This approach aligns accounting practices with modern risk management methodologies, which inherently focus on anticipatory assessment of credit risk.

Unlike the previous incurred loss model, which only recognized impairment after objective evidence of a loss event, the ECL model requires institutions to recognize potential credit losses from the point of origination. This shift ensures that financial statements provide a more timely and realistic reflection of the credit risk embedded in a bank's portfolio. In practice, the ECL calculation involves a combination of historical data, borrower-specific information, and forward-looking macroeconomic indicators, enabling banks to estimate the likelihood and magnitude of future losses under varying economic scenarios. According to EY (2023), the integration of probabilistic modeling with forward-looking inputs ensures that ECL estimates are both statistically robust and aligned with supervisory expectations.

The ECL framework is structured around a three-stage approach reflecting changes in credit risk since initial recognition. Stage 1 includes assets with no significant increase in credit risk, where a 12-month ECL is recognized. Stage 2 encompasses assets exhibiting a

significant increase in credit risk, requiring recognition of lifetime ECL. Stage 3 pertains to credit-impaired assets, also measured at lifetime ECL, with interest revenue calculated on the net carrying amount. This staging mechanism links accounting recognition directly with the underlying risk profile of each asset, providing a dynamic and granular approach to impairment measurement.

## 2. The Three-Stage Impairment Approach

IFRS 9 establishes a structured three-stage approach to credit impairment that links the recognition of expected credit losses (ECL) directly to changes in the credit risk profile of financial assets. Stage 1 includes performing assets, where there has been no significant increase in credit risk since initial recognition. For these assets, the 12-month ECL is recognized, representing the expected losses arising from default events that may occur within the next twelve months. Interest income continues to be recognized on the gross carrying amount of the asset, reflecting the full contractual cash flows. This stage ensures that even high-quality assets carry a prudent level of anticipated loss, promoting early recognition of potential credit risk.

Stage 2 applies to assets that have experienced a significant increase in credit risk (SICR) since initial recognition. At this stage, the lifetime ECL is recognized, reflecting the expected credit losses over the entire remaining life of the asset. Despite the increased risk, interest income continues to be calculated on the gross carrying amount, maintaining consistency in revenue recognition while the asset is still considered performing. The identification of SICR has become particularly sophisticated in digital banking environments, where automated monitoring systems, machine learning models, and real-time behavioral indicators allow for dynamic, data-driven assessment of credit deterioration. These technologies enhance the timeliness and accuracy of stage migration decisions, supporting both regulatory compliance and sound risk management.

Stage 3 encompasses credit-impaired assets, which are classified as non-performing or in default. In this stage, lifetime ECL continues to be recognized, but interest income is calculated on the net carrying amount after deducting the loss allowance, reflecting the reduced recoverable value of the asset. This approach aligns accounting recognition with the underlying economic substance of the credit-

impaired asset, ensuring that financial statements provide a realistic view of expected recoveries.

### 3. Components of Expected Credit Loss

Expected Credit Loss (ECL) measurement under IFRS 9 relies on three fundamental components: Probability of Default (PD), Loss Given Default (LGD), and Exposure at Default (EAD). Each component plays a critical role in quantifying the expected credit losses over the life of a financial instrument and ensuring that impairment recognition reflects forward-looking risk considerations.

The Probability of Default (PD) represents the likelihood that a borrower will fail to meet its contractual obligations within a specified time horizon, typically twelve months for Stage 1 assets or over the remaining life for Stage 2 and Stage 3 assets. In digital banking environments, PD estimation has become increasingly sophisticated due to the availability of high-frequency transactional data, behavioral signals, and alternative data sources such as e-commerce activity, mobile usage, and social data. Machine learning models and advanced statistical techniques allow banks to dynamically assess PD, producing more granular and timely estimates compared to traditional credit scoring methods (BIS, 2023).

Loss Given Default (LGD) measures the proportion of exposure that is expected to be unrecoverable if a default occurs. LGD takes into account collateral values, potential recovery rates, legal costs, and the operational effectiveness of collection processes. Digital banking platforms can enhance LGD estimation by providing real-time insights into collateral liquidity, automated monitoring of asset values, and historical recovery data across portfolios. Accurate LGD estimation is crucial for reflecting the economic reality of potential losses and for regulatory compliance under IFRS 9 and related prudential guidelines.

Exposure at Default (EAD) captures the expected outstanding exposure at the time of default, including both drawn amounts and any anticipated future drawdowns under committed facilities. In digital lending platforms, EAD can vary rapidly due to automated credit line utilization, instant loan disbursements, or dynamic credit limits. Real-time monitoring and predictive analytics enable banks to estimate EAD more accurately, ensuring that the credit risk profile is aligned with the institution's actual exposure.

### 4. Forward-Looking Information and Macroeconomic Scenarios

A central feature of the Expected Credit Loss (ECL) model under IFRS 9 is the integration of forward-looking information, which ensures that impairment recognition is anticipatory rather than reactive. Forward-looking information encompasses forecasts of key macroeconomic variables such as GDP growth, unemployment rates, interest rates, inflation, and sector-specific indicators that are likely to influence the creditworthiness of borrowers. By incorporating these projections, banks can estimate potential credit losses before objective evidence of default arises, aligning accounting practices more closely with risk management frameworks.

In the context of digital banking, the generation and utilization of forward-looking information are increasingly automated. Advanced analytics, machine learning models, and real-time data feeds allow digital banks to dynamically update macroeconomic assumptions and simulate multiple economic scenarios. For instance, a digital lending platform can adjust expected credit losses based on shifts in unemployment trends or interest rate changes within hours, rather than waiting for traditional monthly or quarterly updates. This continuous integration of macroeconomic data enhances the relevance and accuracy of ECL estimates, allowing financial institutions to respond proactively to emerging risks.

Scenario analysis is a key technique in this process. Banks typically develop baseline, optimistic, and adverse scenarios to capture a range of possible future economic conditions. Each scenario is assigned a probability weight, which is used to calculate a probability-weighted ECL estimate. According to the Basel Committee on Banking Supervision (2023), employing multiple macroeconomic scenarios improves the robustness of ECL models and provides a more realistic representation of potential credit losses under varying economic circumstances. Scenario analysis also facilitates stress testing and regulatory reporting, helping banks demonstrate resilience to supervisors and investors.

## C. Cyber Risk Accounting and Digital Fraud Detection

As banking operations increasingly rely on digital platforms, cloud infrastructure, and interconnected information systems, cyber

risk has emerged as one of the most significant sources of operational and financial risk in modern banking. Cyberattacks, data breaches, and digital fraud incidents not only disrupt operations but can also result in substantial financial losses, legal liabilities, and reputational damage. Consequently, cyber risk is no longer viewed solely as a technical or IT issue; it has become a critical concern for accounting, financial reporting, and risk management. According to the Basel Committee on Banking Supervision (2023) and BIS (2023), effective cyber risk accounting and advanced digital fraud detection mechanisms are essential to ensure financial resilience and transparency in the digital banking era.

## 1. Concept of Cyber Risk in Digital Banking

Cyber risk in digital banking refers to the potential for financial loss, operational disruption, or reputational damage arising from breaches or failures in information systems, digital infrastructure, or data security. Unlike traditional operational risks, cyber risk is unique due to its intangible nature and the speed at which incidents can propagate across interconnected systems. The digital banking ecosystem encompassing mobile banking applications, open APIs, cloud computing platforms, and fintech partnerships has significantly expanded the attack surface, making institutions more vulnerable to a wide range of threats. Common cyber risks include malware and ransomware attacks that can encrypt critical systems, phishing and social engineering tactics targeting employees or customers, unauthorized access to banking systems, theft of sensitive customer or institutional data, and distributed denial-of-service (DDoS) attacks that disrupt digital operations (KPMG, 2023).

From an operational standpoint, cyber incidents can halt payment processing, compromise transaction integrity, and impede access to customer accounts, potentially triggering liquidity strains if funds cannot be mobilized effectively. The financial implications of cyber risk extend beyond direct remediation costs, including legal liabilities, regulatory fines, and potential loss of customer confidence, which can indirectly increase credit and market risks. For example, a major data breach may lead to sudden customer withdrawals or reduced lending capacity, thereby impacting both liquidity and credit exposure. In this sense, cyber risk is interrelated with broader banking risk

management frameworks, necessitating an integrated approach to monitoring and mitigation.

From an accounting perspective, cyber risk is generally treated as part of operational risk. Financial reporting standards require institutions to recognize losses when they are probable and reliably measurable. Accordingly, banks must account for expected losses from cyber incidents through provisions for contingent liabilities, impairment of affected digital assets, or accruals for anticipated regulatory penalties. Effective risk governance in digital banking includes implementing robust cyber risk management frameworks, continuous monitoring systems, automated logging, and comprehensive audit trails to capture and quantify incidents in real time. According to Deloitte (2023), embedding cyber risk considerations into financial reporting enhances transparency, strengthens internal controls, and improves preparedness for both internal and external audit reviews.

## 2. Accounting Implications of Cyber Risk

Cyber risk has increasingly become a critical consideration for accounting and financial reporting in digital banking, given the potential for significant operational, financial, and reputational consequences. From an accounting perspective, cyber incidents can generate both direct financial losses and indirect effects that require careful measurement, recognition, and disclosure. Direct losses may include stolen funds, expenses for system restoration and recovery, penalties imposed by regulators, and costs associated with customer notification and remediation. According to Deloitte (2023), such losses must be recognized in the profit or loss statement when they are incurred and reliably measurable, reflecting the economic impact of the incident on the bank's financial position.

In addition to recognizing immediate losses, cyber risk may create obligations that require the recognition of provisions under IAS 37. For instance, if a cyber event results in probable legal claims, class-action lawsuits, or anticipated regulatory penalties, banks are required to record a provision that reflects the best estimate of the expected outflow of resources to settle the obligation. Where the potential liability is possible but not probable, these are disclosed as contingent liabilities in the financial statements, providing transparency while reflecting the uncertainty surrounding the event (IASB, 2023). This

distinction ensures that users of financial statements understand the nature and scope of potential financial exposures without overstating obligations.

Significant cyber events can also lead to impairment of intangible assets. Digital banking relies heavily on internally developed software, digital platforms, and customer-facing applications, all of which are recorded as intangible assets. When cyber incidents compromise system functionality, reduce asset usability, or damage associated future cash flows, impairment testing under IAS 36 is necessary. The carrying amount of these assets must be written down to their recoverable amount if evidence indicates that the assets no longer generate expected economic benefits (PwC, 2023).

### 3. Regulatory Expectations and Cyber Risk Disclosure

In the digital banking environment, regulators have placed increasing emphasis on cyber resilience and transparent reporting of cyber risk exposures. Cyber risk is no longer treated solely as an operational concern; it has become a critical component of enterprise risk management (ERM), governance, and financial disclosure. According to the Basel Committee on Banking Supervision (2023), effective cyber risk management requires clear governance structures, including board-level oversight, defined responsibilities for risk monitoring, and integration of cyber risk into the broader ERM framework. Banks are expected to maintain proactive strategies for detecting, preventing, and mitigating cyber incidents, and these strategies must be demonstrably linked to risk appetite and capital planning processes.

Regulatory expectations also extend to the disclosure of material cyber events in financial statements. Regulators encourage banks to report significant cyber incidents promptly, both to supervisory authorities and, where appropriate, to the public. This requirement affects the timing and measurement of recognized losses, as accounting judgments must align with regulatory definitions of materiality and expected outflows. For instance, IFRS-compliant financial reporting mandates recognition of losses when they are probable and reliably measurable, while disclosures must provide sufficient detail to inform stakeholders about potential financial impacts and the nature of cyber threats (IFRS Foundation, 2023). In practice,

this means that banks must integrate internal incident reporting systems with accounting and reporting functions to ensure timely recognition of liabilities, provisions, or contingent exposures arising from cyber events.

Cyber risk disclosure also entails describing governance arrangements, policies, and the effectiveness of controls. Transparent reporting enhances stakeholder confidence by demonstrating that the institution actively manages and mitigates cyber threats. Furthermore, consistent and structured disclosures support comparability across institutions, enabling regulators, investors, and analysts to assess cyber risk exposure systematically. As noted by KPMG (2023), comprehensive cyber risk reporting should cover the type of incidents, potential financial impacts, accounting treatments, and mitigation measures, emphasizing both quantitative and qualitative aspects.

## 4. Digital Fraud in Banking

Digital fraud in banking represents a critical and evolving threat in the era of online and mobile financial services. It encompasses deliberate actions aimed at deceiving banks or their customers for financial gain, leveraging the speed, accessibility, and complexity of digital channels. Common manifestations of digital fraud include payment fraud and account takeovers, where criminals gain unauthorized access to customer accounts to execute transactions. Identity theft and synthetic identity fraud have also increased, with perpetrators creating fake profiles or using stolen personal information to obtain credit or execute fraudulent transfers. Transaction manipulation, such as altering transaction details or initiating unauthorized transfers, and insider fraud where employees misuse privileged system access add further dimensions to the risk landscape (ACFE, 2022).

The rapid proliferation of digital banking platforms has amplified both the scale and velocity of fraudulent activity. Real-time payment systems, while improving customer convenience, also provide minimal time for detection and intervention, increasing the potential for financial loss. According to the Association of Certified Fraud Examiners (2022), highly digitized banking environments tend to experience a higher frequency of fraud incidents; however, the average financial loss per incident may be lower due to improved monitoring

and preventive controls. This pattern emphasizes the need for continuous surveillance and proactive fraud detection strategies.

From an accounting and financial reporting perspective, digital fraud has immediate implications for the recognition of losses, provisions, and contingent liabilities. Institutions must accurately identify and quantify losses resulting from fraudulent transactions, which may include direct monetary losses, system restoration costs, legal expenses, and potential regulatory penalties. IFRS standards, particularly IAS 37 on provisions and contingencies, require that probable obligations arising from fraud be recognized, while possible but not probable exposures should be disclosed as contingent liabilities (IFRS Foundation, 2023). Additionally, accounting systems must ensure proper segregation of fraudulent transactions from normal operations to maintain the integrity of financial statements.

## D. Scenario Planning and Stress Testing With AI Models

Scenario planning and stress testing are essential tools in banking risk management, enabling institutions to assess their resilience under adverse economic, financial, and operational conditions. In the digital era, the growing complexity of financial products, interconnected markets, and technology-driven risks has significantly increased the limitations of traditional stress testing approaches. Artificial intelligence (AI) and advanced analytics now play a critical role in enhancing scenario planning and stress testing by enabling more granular, dynamic, and forward-looking risk assessments. According to the Basel Committee on Banking Supervision (2023) and BIS (2023), AI-driven stress testing strengthens banks' ability to anticipate vulnerabilities, support regulatory compliance, and improve risk-informed financial reporting.

### 1. Concept and Objectives of Scenario Planning

Scenario planning is a strategic tool used by banks to anticipate and prepare for a range of plausible future developments that may affect their financial performance and stability. Unlike traditional forecasting, which seeks to predict the most likely outcome based on historical trends, scenario planning emphasizes the exploration of uncertainty, including extreme or tail-risk events, and their potential consequences.

In the context of digital banking, scenario planning has become increasingly important due to the rapid evolution of financial technologies, real-time transaction processing, and the integration of digital channels, all of which can amplify both opportunities and risks. By constructing multiple hypothetical scenarios, banks can evaluate how variations in economic conditions, market volatility, regulatory changes, or cyber threats might impact capital adequacy, liquidity positions, and overall operational resilience.

One key objective of scenario planning is to assess the robustness of a bank's capital and liquidity. By simulating stressed conditions such as sharp interest rate movements, sudden deposit outflows, or credit market shocks, banks can determine whether their balance sheets can withstand adverse developments without breaching regulatory thresholds. This analysis informs capital planning, contingency funding strategies, and stress-testing exercises mandated by prudential regulators. Scenario planning also plays a critical role in credit risk management by evaluating the vulnerability of loan portfolios under different macroeconomic conditions. For example, simulations may incorporate scenarios of rising unemployment, declining property prices, or sector-specific downturns, providing insights into potential loan defaults and the associated expected credit losses under IFRS 9 (IFRS Foundation, 2023).

Beyond credit and liquidity considerations, scenario planning supports operational and cyber risk preparedness. Digital banking systems, while efficient, are susceptible to cyberattacks, system outages, and transaction anomalies. Scenario planning enables banks to model the financial and operational impacts of such events, guiding investments in cybersecurity, backup systems, and automated monitoring tools. From an accounting perspective, scenario planning informs forward-looking estimates, including fair value measurements of volatile assets, impairment assessments for digital and intangible assets, and going concern evaluations, ensuring that financial statements provide a realistic representation of potential risks.

## 2. Stress Testing in Banking Regulation and Accounting

Stress testing in banking represents a critical tool for evaluating the resilience of financial institutions under adverse economic and financial conditions. Unlike routine forecasting, stress testing applies

extreme but plausible scenarios to assess how shocks such as sharp interest rate changes, market volatility, credit defaults, or liquidity disruptions affect a bank's financial position and performance. Regulatory authorities increasingly mandate stress testing as part of prudential supervision, ensuring that banks maintain sufficient capital and liquidity buffers to withstand periods of systemic stress and protect depositors and market stability. According to the Basel Committee (2023), effective stress testing should be forward-looking, comprehensive, and closely integrated with internal risk management frameworks and accounting systems.

From a regulatory perspective, stress testing informs capital planning and provisioning decisions. By modeling the potential losses arising from hypothetical adverse events, banks can evaluate whether their existing capital base is adequate to absorb shocks or whether additional capital buffers are required. This process complements the Expected Credit Loss (ECL) framework under IFRS 9, where forward-looking credit risk estimates incorporate scenario-based adjustments. Stress test results also guide liquidity management, enabling banks to determine appropriate liquidity coverage ratios, contingency funding strategies, and the sufficiency of high-quality liquid assets under stressed conditions. In digital banking environments, where customer fund movements can be rapid and unpredictable, real-time liquidity monitoring integrated with stress testing models is essential for timely risk mitigation.

In addition to regulatory compliance, stress testing has significant accounting and financial reporting implications. The outputs from stress scenarios support management judgments in impairment testing, fair value measurement, and provision recognition. For instance, anticipated losses under extreme scenarios may affect the staging of loans, the calculation of lifetime expected credit losses, and the valuation of financial instruments measured at fair value. Transparent disclosure of stress testing methodologies, assumptions, and outcomes enhances stakeholder confidence and aligns with IFRS and PSAK reporting requirements, as stakeholders increasingly demand insights into how banks manage systemic and idiosyncratic risks.

## 3. Limitations of Traditional Stress Testing Models

Traditional stress testing models have long been a cornerstone of banking risk management, providing structured scenarios to evaluate potential losses under adverse conditions. These models typically rely on linear assumptions, historical correlations, and static input variables to simulate shocks to credit, market, and liquidity risk exposures. While effective in relatively stable and predictable financial environments, the rise of digital banking has exposed significant limitations in these conventional approaches. Digital banking introduces complexities such as high-frequency transaction flows, real-time fund movements, and innovative financial products that traditional models may not adequately capture. For instance, the velocity and scale of digital payment systems can trigger liquidity stress in a manner that historical models, based on slower transaction patterns, fail to predict.

Additionally, emerging risk types pose challenges to conventional stress testing. Cyber risk, digital fraud, and operational disruptions stemming from cloud or API failures introduce non-linear and often systemic impacts on banking operations. Traditional models, which assume relatively independent risk factors and linear propagation of shocks, may underestimate the cascading effects of such events. For example, a cyberattack compromising transaction systems could simultaneously impact liquidity positions, customer confidence, and market risk exposures, a scenario that simple historical correlations cannot fully capture (Deloitte, 2023). Similarly, fintech innovations, such as instant credit approval platforms or tokenized assets, create exposures that lack sufficient historical data for conventional model calibration, reducing predictive reliability.

Another limitation of traditional stress testing is its reliance on static assumptions about market behavior and borrower performance. In rapidly evolving digital environments, customer behaviors, market liquidity, and macroeconomic responses can change abruptly, rendering static models obsolete. Furthermore, traditional approaches often focus on a limited number of scenarios, whereas digital banking requires consideration of a broader range of plausible adverse events, including tail-risk and low-probability, high-impact occurrences. The lack of flexibility in scenario design constrains the ability of banks to evaluate resilience comprehensively.

## 4. Role of Artificial Intelligence in Scenario Planning

Artificial intelligence (AI) has become a transformative tool in enhancing scenario planning within digital banking, enabling institutions to navigate complex and rapidly evolving risk environments. Traditional scenario planning often relied on limited historical data and expert judgment, which constrained the number and sophistication of scenarios that could be considered. In contrast, AI leverages vast volumes of structured and unstructured data, including transaction records, market feeds, social media sentiment, regulatory updates, and macroeconomic indicators, to generate more comprehensive and nuanced scenarios. Machine learning algorithms, for instance, can analyze historical correlations and emerging trends to construct macroeconomic scenarios that reflect a wider spectrum of potential outcomes, including low-probability but high-impact events. These models dynamically adjust as new data becomes available, allowing banks to maintain up-to-date and forward-looking scenario analyses (Marr, 2022).

Neural networks, another AI application, are particularly valuable for modeling non-linear interactions among risk factors. In digital banking, risks such as cyber threats, liquidity shocks, and market volatility do not operate in isolation; they often interact in complex ways that linear models cannot capture. Neural networks can learn these non-linear relationships from historical and simulated data, enabling scenario planners to better anticipate cascading effects and systemic vulnerabilities. For example, a sudden cyberattack might trigger simultaneous liquidity withdrawals, market volatility, and credit deterioration a chain of events that AI models can simulate more realistically than conventional approaches.

Natural language processing (NLP) further expands the scope of scenario planning by incorporating qualitative risk signals. Regulatory reports, news articles, earnings calls, and social media posts can be analyzed to detect emerging threats or shifts in market sentiment, which may not yet be visible in numerical data. By integrating NLP insights, banks can enrich their scenarios with forward-looking intelligence, improving the accuracy and relevance of risk assessments.

The application of AI in scenario planning also facilitates the generation of extreme tail-risk scenarios that, while unlikely, have significant potential impact. These scenarios support stress testing,

capital planning, and strategic decision-making, ensuring that banks remain resilient under adverse conditions. AI-driven scenario planning enhances both the efficiency and depth of analysis, allowing risk managers and executives to explore a wider array of plausible futures, evaluate potential vulnerabilities, and develop proactive mitigation strategies. This shift from static, retrospective models to dynamic, data-driven simulations represents a significant evolution in digital banking risk management and strategic planning (Marr, 2022).

# CHAPTER VIII
# REGULATORY COMPLIANCE AND ETHICAL ACCOUNTING

Regulatory compliance and ethical accounting form the backbone of trust, transparency, and accountability in modern banking, particularly in the digital era where financial transactions and reporting are increasingly automated and data-driven. Banks must adhere not only to legal and regulatory frameworks, such as AML-CFT, KYC, ESG reporting, and IFRS/PSAK standards, but also to high ethical standards in the use of technology, artificial intelligence, and digital financial platforms. Integrating regulatory compliance with ethical accounting ensures accurate financial reporting, mitigates risks of fraud and misconduct, strengthens corporate governance, and enhances stakeholder confidence, ultimately supporting sustainable and responsible banking practices in a complex, digitalized financial ecosystem.

## A. AML-CFT, KYC and Digital Identity Validation

Anti-Money Laundering and Counter-Terrorist Financing (AML-CFT) and Know-Your-Customer (KYC) controls are foundational to financial system integrity. In the digital era these controls must operate at scale, in real time, and across complex platform and API ecosystems. Digital identity validation (e-KYC) using biometric verification, trusted government databases, device signals and cryptographic attestations has therefore become central to enabling secure onboarding, ongoing customer due diligence (CDD), and effective transaction monitoring while supporting financial inclusion goals. Authoritative guidance (FATF), development partners (World Bank) and national supervisors (e.g., OJK, central banks) now expect institutions to adopt risk-based, technology-enabled approaches and to govern associated model, privacy and third-party risks. (FATF)

## 1. Regulatory and Guidance Landscape

The regulatory and guidance landscape for digital identity and anti-money laundering (AML) in banking is shaped by a combination of global standards, national regulations, and evolving supervisory expectations. At the international level, the Financial Action Task Force (FATF) provides a global baseline for managing digital identity risks within AML and counter-terrorism financing (CFT) frameworks. FATF guidance emphasizes that reliable digital ID systems can be used to fulfill customer due diligence (CDD) requirements, provided that risk-based approaches are applied. Key expectations include the strength and resilience of authentication mechanisms, robust privacy safeguards, and clear governance structures to ensure that the adoption of digital identity tools does not weaken AML/CFT controls (FATF, 2023). This guidance underlines the importance of balancing technological innovation with regulatory compliance, ensuring that digital identities maintain integrity and traceability while supporting secure financial transactions.

National regulations and supervisory guidance translate these principles into jurisdiction-specific requirements. In Indonesia, for example, the Financial Services Authority (Otoritas Jasa Keuangan, OJK) has issued comprehensive norms governing e-KYC and digital banking operations under regulations such as the POJK on Digital Banking. These rules require financial institutions to implement secure customer identification processes, manage risks associated with third-party service providers, and promptly report suspicious activities. In addition, OJK engages in public-private dialogues to promote interoperability within identity ecosystems and to advance financial inclusion objectives, ensuring that digital identification frameworks are both secure and accessible to a wide population (OJK Portal, 2023).

Supervisory bodies also focus on the integration of RegTech solutions to enhance transaction monitoring, KYC refresh processes, and sanctions screening. Central banks such as the Hong Kong Monetary Authority (HKMA) have conducted thematic reviews on the use of AI and RegTech in AML automation, highlighting opportunities to improve efficiency and effectiveness while identifying potential weaknesses such as false positives, model drift, and outsourcing risks. Industry surveys and barometers, for instance from NICE Actimize, further document operational priorities and emerging best practices in

transaction monitoring, politically exposed persons (PEP) and sanctions screening, and data quality management (Hong Kong Monetary Authority, 2023).

## 2. Core Components of Digital AML/CFT & KYC

The core components of digital Anti-Money Laundering (AML), Counter-Terrorism Financing (CFT), and Know Your Customer (KYC) frameworks are designed to ensure that financial institutions can efficiently verify identities, assess risk, and monitor transactions in a secure, scalable, and compliant manner. A key starting point is onboarding through electronic KYC (e-KYC), which enables remote identity verification using technologies such as Optical Character Recognition (OCR) for identity documents, biometric liveness checks, and validation against trusted government registries where available. FATF (2023) emphasizes that e-KYC processes should be risk-based: lower-risk customers may undergo simplified verification, while higher-risk clients require enhanced validation to mitigate exposure to financial crime.

Customer Due Diligence (CDD) and Enhanced Due Diligence (EDD) form the next critical layer. Automated systems can gather information on beneficial ownership, politically exposed person (PEP) status, sanctions lists, and adverse media coverage. For high-risk relationships, EDD combines algorithmic enrichment, such as natural language processing for adverse news and network analysis, with human expert review to ensure thorough evaluation of potential risks (info.niceactimize.com, 2023). This integration of automation and expert oversight enhances both efficiency and reliability in risk assessment.

Transaction monitoring is another essential component, leveraging rules-based systems and machine learning to continuously score transactions and customer relationships. Alerts are generated for potentially suspicious activity, feeding into case management workflows for investigation. Continuous calibration, feedback loops, and expert review are necessary to minimize false positives and prevent model drift, maintaining the integrity of monitoring processes (Hong Kong Monetary Authority, 2023).

Ongoing monitoring and KYC refresh mechanisms ensure that customer risk profiles remain up to date. This involves periodic and

event-driven updates based on transactional behavior, external adverse information, or automated triggers such as sudden increases in transaction volumes (info.niceactimize.com, 2023). These processes allow banks to react proactively to changing risk dynamics and regulatory expectations.

### 3. Accounting and Financial Reporting Implications

The accounting and financial reporting implications of implementing digital identity, AML/CFT, and RegTech solutions in banking are significant, encompassing capitalization, expense recognition, provisions, and auditability. One critical area is the treatment of implementation costs. Banks invest in digital identity platforms, AML analytics, and regulatory technology to enhance compliance and operational efficiency. According to IFRS and PSAK guidance, certain costs related to software development and system integration may meet the criteria for capitalization, while ongoing operating costs, such as subscription fees, data feeds, and maintenance, are expensed as incurred. Accounting teams must carefully evaluate which costs qualify for capitalization and ensure transparent disclosure of material investments, amortization policies, and useful life assumptions to provide stakeholders with clear insight into the bank's technology investments (nevisfsrc.com, 2023).

Provisions and contingencies form another important aspect. Failures or deficiencies in AML/CFT controls that result in regulatory fines, litigation, or remediation costs must be recognized or disclosed under IAS 37. Provisions are recorded when outflows are probable and can be reliably estimated, while contingent liabilities are disclosed for reasonably possible obligations. Maintaining robust documentation of internal controls, risk assessments, and monitoring outcomes is essential to support professional judgments regarding the timing and amount of provisions (FATF, 2023).

Operational losses linked to identity fraud or other compliance breaches are also relevant for financial reporting. Fraudulent transactions, customer reimbursements, and remediation costs must be recognized as expenses in the period they occur, while recoveries, such as insurance claims or restitution, are recorded only when realization is virtually certain. This ensures prudence in financial reporting and aligns

with IAS 37 and IAS 1 requirements for consistent recognition of losses and recoveries (info.niceactimize.com, 2023).

## 4. Implementation Challenges and Risks

The implementation of digital identity, AML/CFT, and RegTech solutions in banking presents several practical challenges and risks that require careful management. One of the primary concerns is data quality and provenance. Machine learning (ML) and artificial intelligence (AI) models, as well as automated scoring systems, rely heavily on accurate, complete, and traceable data. Poor-quality data, inconsistent lineage, or gaps in transaction records can lead to misclassification of customers, false alerts, and ultimately regulatory exposure. To mitigate these risks, banks must implement regular data quality assessments, reconciliation processes, and data lineage documentation, ensuring that all inputs to ML or automated decision systems are verifiable and auditable (info.niceactimize.com, 2023).

Model risk and explainability represent another critical area of concern. Supervisory authorities have highlighted the dangers of "black-box" AI and ML models used for transaction monitoring or risk scoring. Such models may generate large numbers of irrelevant alerts, obscure the underlying decision logic, and hinder effective risk management. To address this, banks are required to establish robust model governance frameworks, including model validation, periodic revalidation, performance monitoring, and clear documentation of assumptions and algorithms. Explainable AI is increasingly seen as essential not only for regulatory compliance but also for operational reliability and auditability (European Banking Authority, 2023).

Third-party and outsourcing risks also pose significant challenges. Banks often rely on external vendors for identity verification, e-KYC services, and AML analytics. While these partnerships can enhance efficiency, they transfer operational, compliance, and reputational risks to the bank. Contracts with vendors must include explicit provisions for supervisory access, service-level agreements, data protection, and audit rights. Supervisory reviews have frequently identified inadequate oversight of outsourced AML tools, underscoring the importance of strong vendor management, continuous monitoring, and risk assessment frameworks (European Banking Authority, 2023).

## B. ESG and Sustainable Banking Reporting

Environmental, Social, and Governance (ESG) and sustainable banking reporting have become central components of regulatory compliance, ethical accounting, and strategic management in the digital banking era. Banks are no longer assessed solely on financial performance but also on how responsibly they manage environmental risks, social impacts, and governance practices. Regulators, investors, and stakeholders increasingly demand transparent, standardized, and data-driven ESG disclosures that are integrated with financial reporting. According to the IFRS Foundation (2023) and the Bank for International Settlements (BIS, 2023), ESG reporting in banking plays a critical role in promoting financial stability, sustainable economic growth, and long-term value creation.

### 1. Concept of ESG and Sustainable Banking

The concept of Environmental, Social, and Governance (ESG) has emerged as a critical framework for assessing the non-financial performance of organizations, particularly in the banking sector. ESG evaluation encompasses three interrelated dimensions. The Environmental aspect focuses on how an organization manages its impact on natural resources and climate, including carbon emissions, energy efficiency, pollution, and exposure to environmental risks. Banks are increasingly expected to monitor and mitigate their financed emissions and support clients in transitioning to low-carbon practices. The Social dimension addresses the institution's role in promoting financial inclusion, protecting consumer rights, ensuring employee welfare, safeguarding data privacy, and contributing to broader community development. Social performance also involves diversity, equity, and inclusion within the organization and responsible engagement with stakeholders. Governance pertains to the effectiveness of the board, quality of risk oversight, robustness of internal controls, adherence to ethical standards, and transparency in reporting. Strong governance is essential for embedding ESG principles into corporate strategy and ensuring accountability (OECD, 2022).

In the context of banking, ESG is closely aligned with sustainable finance, which integrates environmental and social considerations into core financial activities such as lending, investment,

and risk management. Sustainable banking seeks to balance profitability with long-term societal and environmental objectives. For instance, banks may prioritize financing for renewable energy projects, offer green bonds, or implement ESG-linked lending criteria. By doing so, they manage both traditional financial risks and emerging sustainability-related risks, such as those arising from climate change or social inequalities. The integration of ESG factors also enhances risk assessment, investor confidence, and reputation management, as stakeholders increasingly demand transparency on sustainability practices (UNEP FI, 2023).

Moreover, ESG reporting and disclosure frameworks have evolved to support banks in demonstrating accountability and comparability. Standards such as the Task Force on Climate-related Financial Disclosures (TCFD) and the Global Reporting Initiative (GRI) provide guidance on metrics, governance structures, and scenario analysis to ensure robust reporting. ESG considerations are not merely regulatory obligations; they are strategic tools that influence lending policies, capital allocation, and product development. Banks adopting ESG principles systematically are better positioned to mitigate long-term environmental and social risks, attract responsible investors, and align with global sustainability agendas (OECD, 2022; UNEP FI, 2023).

## 2. Regulatory and Standard-Setting Landscape

The regulatory and standard-setting landscape for Environmental, Social, and Governance (ESG) reporting has undergone significant evolution in recent years, driven by the growing recognition of sustainability risks and opportunities in financial decision-making. At the global level, the IFRS Foundation, through the International Sustainability Standards Board (ISSB), has issued the IFRS Sustainability Disclosure Standards (S1 and S2) in 2023. IFRS S1 requires entities to provide disclosures on sustainability-related risks and opportunities that could affect enterprise value, while IFRS S2 specifically focuses on climate-related financial information, including governance, strategy, risk management, and metrics. These standards aim to enhance consistency and comparability of sustainability reporting across jurisdictions, facilitating investors' ability to assess

climate and sustainability impacts alongside traditional financial information (IFRS Foundation, 2023).

The Basel Committee on Banking Supervision (BCBS) complements these global standards by emphasizing climate-related financial risk management and disclosure in banks. The BCBS guidance encourages financial institutions to integrate climate risks into risk assessment, capital planning, and disclosure processes, recognizing the systemic importance of climate resilience in the banking sector (BCBS, 2023). Such guidance underscores the need for banks to adopt forward-looking approaches, scenario analysis, and robust internal controls to manage environmental and social risks effectively.

At the national level, regulatory authorities have also developed ESG frameworks tailored to local market conditions. In Indonesia, the Financial Services Authority (OJK) mandates banks to publish Sustainability Reports and implement Sustainable Finance Action Plans, as outlined in POJK No. 51/2017. These regulations require financial institutions to disclose sustainability strategies, risk management practices, and performance metrics, reinforcing accountability and aligning banking operations with national sustainable development objectives (OJK Portal, 2023).

### 3. ESG Accounting and Measurement in Banking

ESG accounting and measurement in banking focus on the systematic identification, quantification, and disclosure of environmental, social, and governance-related factors that have a material impact on a bank's financial performance and position. From an accounting perspective, the integration of ESG considerations requires linking sustainability metrics to traditional financial reporting frameworks, ensuring transparency, comparability, and relevance for stakeholders. One key area is climate-related credit risk, where banks assess borrowers' exposure to both physical risks such as extreme weather events and transition risks arising from shifts toward a low-carbon economy. These assessments can influence credit ratings, loan classification, and provisioning decisions under IFRS 9, as expected credit losses (ECL) may be affected by climate-related scenarios (IFRS Foundation, 2023).

Green asset classification is another critical aspect of ESG accounting. Banks are required to identify and track sustainable loans

and investments, distinguishing them from conventional exposures. This involves defining eligibility criteria, verifying alignment with recognized sustainability standards, and ensuring proper documentation to support regulatory reporting and investor disclosures. Accurate classification supports both internal risk management and external reporting obligations, while also facilitating the allocation of capital toward sustainable economic activities (OECD, 2022).

Provisioning and valuation impacts are also increasingly influenced by ESG factors. For instance, climate stress testing may affect ECL calculations or the fair value of certain financial instruments, particularly those exposed to transition or physical risks. Similarly, investments in green technologies or digital infrastructure may influence impairment assessments under IAS 36, as well as amortization or depreciation of capitalized assets. Accounting professionals must apply judgment in estimating these impacts, considering both quantitative models and qualitative information about environmental and social risks (PwC, 2023).

Operational sustainability costs constitute an additional dimension of ESG accounting. Banks increasingly invest in green IT, energy-efficient systems, and sustainable digital platforms, which can be capitalized or expensed depending on IFRS and PSAK guidance. Accurate recognition and disclosure of these expenditures are essential to provide stakeholders with a holistic view of how ESG initiatives influence operational efficiency, cost structures, and long-term financial resilience.

### 4. Integration of ESG into Financial Reporting

The integration of ESG factors into financial reporting represents a paradigm shift in sustainable banking, moving beyond traditional, standalone sustainability reports to a more holistic approach where environmental, social, and governance information is embedded directly into financial statements and management commentary. This approach ensures that sustainability considerations are treated as a core element of financial performance and risk assessment rather than as supplementary disclosures. A key aspect of this integration involves linking climate-related risks to credit loss assumptions, enabling banks to reflect potential financial impacts of physical and transition risks in expected credit loss calculations under IFRS 9. By incorporating

forward-looking climate scenarios into credit risk models, banks can provide more accurate, risk-sensitive valuations and disclosures (IFRS Foundation, 2023).

Furthermore, ESG integration requires transparent reporting on how sustainability strategies influence capital allocation and investment decisions. Banks are increasingly disclosing the proportion of assets directed toward green or socially responsible projects, illustrating the alignment between strategic objectives, risk appetite, and sustainable finance goals. Governance disclosures are another critical component, detailing board-level oversight, sustainability committees, and risk management structures that ensure ESG considerations are systematically incorporated into decision-making and operational controls (OECD, 2022).

Scenario-based climate risk analysis forms an additional layer of integrated reporting. Banks are expected to simulate adverse environmental events, policy transitions, and macroeconomic shifts to assess potential impacts on liquidity, capital adequacy, and asset valuations. This scenario analysis not only informs internal risk management but also enhances transparency for external stakeholders, including investors, regulators, and rating agencies (TCFD, 2022). By providing both qualitative explanations and quantitative metrics, integrated reporting improves the decision-usefulness of ESG disclosures and supports comparability across institutions.

The IFRS Sustainability Disclosure Standards (S1 and S2) and the TCFD recommendations provide widely accepted guidance for integrating ESG into financial reporting, emphasizing consistency, materiality, and linkage between sustainability and financial information. Adopting these frameworks ensures that ESG factors are embedded into mainstream accounting processes, such as impairment testing, fair value measurement, and capital planning, creating a unified reporting ecosystem.

## C. Ethical Digital Accounting Practices

Ethical digital accounting practices are essential in ensuring trust, transparency, and accountability within modern banking institutions operating in highly digitalized environments. As accounting processes increasingly rely on automated systems, artificial intelligence

(AI), big data analytics, and cloud-based platforms, ethical considerations extend beyond traditional professional conduct to include data integrity, algorithmic transparency, cybersecurity, and responsible use of technology. According to the International Ethics Standards Board for Accountants (IESBA, 2023) and the IFRS Foundation (2023), ethical digital accounting is a critical pillar for safeguarding public trust and maintaining the credibility of financial reporting in the digital banking era.

## 1. Foundations of Ethics in Digital Accounting

The foundations of ethics in digital accounting build upon the long-established principles of integrity, objectivity, professional competence, confidentiality, and professional behavior, but their application has evolved in the context of rapidly advancing technology. Integrity in digital accounting requires ensuring that financial information generated by automated systems, AI algorithms, and cloud-based platforms is complete, accurate, and free from manipulation. Accountants must remain vigilant in validating digital outputs and maintaining transparency in all reporting processes, recognizing that errors or biases in automated systems can have material consequences for stakeholders (IESBA, 2023).

Objectivity, another cornerstone, involves preventing bias in automated decision-making processes, algorithmic judgments, and predictive models. In digital accounting, machine learning models may produce outcomes influenced by historical data patterns, which could inadvertently perpetuate discrimination or misrepresent financial performance. Accountants must apply critical oversight, test assumptions, and validate algorithms to ensure that decisions and reports remain unbiased and aligned with professional standards. This requires not only technical understanding but also ethical discernment to challenge outputs that may be misleading or incomplete (IFAC, 2023).

Professional competence in the digital era extends beyond traditional accounting skills to include digital literacy, data analytics, and understanding of AI-driven systems. Accountants must acquire the knowledge and skills necessary to supervise automated processes, interpret system outputs, and assess the appropriateness of model-based valuations or predictive forecasts. Continuous professional

development is essential to maintain relevance and uphold ethical responsibilities in an environment where technology increasingly mediates financial reporting and decision-making.

Confidentiality takes on heightened importance in digital accounting due to the volume and sensitivity of data processed electronically. Financial institutions handle vast amounts of personal and transactional data, and accountants must implement safeguards against unauthorized access, cyber threats, and data breaches. Ethical practice demands adherence to data protection regulations, secure handling of digital records, and careful consideration of privacy implications in automated reporting (IESBA, 2023).

## 2. Ethical Challenges in Digital Accounting Systems

The rise of digital accounting systems has transformed the financial reporting landscape but has also introduced complex ethical challenges that require careful management by banks and accounting professionals. One of the foremost concerns is algorithmic bias and the use of "black-box" models. AI-driven accounting and risk assessment tools rely on large datasets and complex algorithms to produce outputs such as predictive forecasts, credit scoring, or fraud detection alerts. When these models are trained on incomplete, skewed, or unrepresentative data, they may generate biased or unjust outcomes, potentially affecting decision-making and stakeholder trust. Ethical practice in this context demands model explainability, rigorous validation, and human oversight to ensure fairness, transparency, and accountability (BIS, 2023).

Data manipulation and integrity risks present another ethical challenge. Automated systems can process massive volumes of transactions in real time, which, while improving efficiency, also amplifies the consequences of errors or deliberate tampering. Accountants must implement robust internal controls, maintain comprehensive audit trails, and enforce segregation of duties to safeguard data accuracy and uphold ethical standards. Failure to do so could result in material misstatements, regulatory breaches, and erosion of stakeholder confidence (Vasarhelyi et al., 2015).

Overreliance on automation constitutes a further ethical concern. The efficiency and sophistication of digital systems may encourage accountants to accept system-generated results uncritically.

Such a mindset can diminish professional skepticism, a cornerstone of ethical accounting. Ethical responsibility in digital accounting requires practitioners to actively interpret, challenge, and corroborate automated outputs, ensuring that decisions are well-founded and aligned with professional standards.

Cybersecurity and privacy risks add an additional layer of ethical complexity. Breaches of digital accounting systems can expose sensitive financial data and personal information, potentially harming customers, investors, and other stakeholders. Accountants have an ethical obligation to support proactive cybersecurity governance, implement strong access controls, and comply with applicable data protection regulations. Protecting confidentiality and maintaining system integrity are essential for ethical stewardship in a digital environment (BIS, 2023).

### 3. Ethical Use of Artificial Intelligence in Accounting

The ethical use of artificial intelligence (AI) in accounting has become a critical consideration as banks increasingly integrate AI-driven systems into financial reporting, risk assessment, and compliance processes. Central to this ethical framework are principles of transparency, accountability, and proportionality, which ensure that AI systems support reliable and responsible decision-making without undermining professional judgment. Transparency requires that AI-generated outputs be interpretable and explainable; stakeholders, including auditors, regulators, and management, must understand how the system arrives at specific conclusions or recommendations. This is particularly important in areas such as credit risk modeling, expected credit loss calculations, and fraud detection, where AI outputs can materially influence financial statements (OECD, 2022).

Accountability in AI-driven accounting emphasizes the need for clearly defined responsibility for decisions informed by AI outputs. Even when automated systems generate recommendations or risk assessments, human professionals must review, validate, and, if necessary, override outputs to ensure decisions align with regulatory standards and ethical principles. Establishing accountability structures, such as assigning ownership of model governance, validation, and oversight, helps prevent inappropriate reliance on “black-box” algorithms and ensures that any errors or biases are promptly addressed.

Proportionality is another ethical principle guiding AI adoption in accounting. AI systems should be used appropriately relative to the significance and complexity of the accounting task. For instance, highly automated predictive models for financial forecasting or impairment testing must be complemented by human judgment, scenario analysis, and professional skepticism. Banks are expected to implement robust controls, including continuous monitoring, model revalidation, and periodic recalibration, to prevent model drift or degradation of predictive accuracy over time. This ensures that AI outputs remain reliable and that potential risks from evolving market conditions, data anomalies, or algorithmic bias are mitigated (OECD, 2022).

**4. Professional Judgment and Accountability**

In the era of digital accounting, professional judgment and accountability remain fundamental principles, even as automation and artificial intelligence increasingly support financial reporting processes. While technology can streamline data processing, perform complex calculations, and generate predictive insights, it cannot replace the nuanced assessment and ethical responsibility that accountants bring to financial decision-making. Accountants retain ultimate responsibility for approving accounting policies embedded within digital systems, ensuring that automated workflows align with IFRS, PSAK, and other regulatory requirements. This includes verifying that recognition, measurement, and classification rules are correctly applied to transactions and financial instruments, particularly when systems handle complex scenarios such as fair value measurement, expected credit loss, or ESG-related adjustments (IFRS Foundation, 2023).

Automated models and AI outputs provide valuable estimates and scenario analyses, yet these projections require careful human review. Professional judgment is essential to assess the reasonableness of assumptions, validate model outputs, and identify potential anomalies or biases. For example, algorithmic predictions in credit risk, liquidity management, or impairment calculations must be scrutinized for sensitivity to changing economic conditions, market volatility, or data quality issues. Accountants must ensure that model outputs do not obscure uncertainty or inadvertently misrepresent the financial position of the organization, maintaining both accuracy and transparency.

Accountability also extends to communication with stakeholders. In digital accounting environments, assumptions, limitations, and uncertainties inherent in automated processes must be clearly disclosed in financial statements and accompanying notes. Stakeholders, including regulators, investors, and auditors, rely on these disclosures to understand the reliability and integrity of reported figures. Transparent reporting of system-driven judgments and management overrides supports trust in automated accounting solutions while demonstrating that ethical and professional standards remain paramount.

The IFRS Foundation (2023) emphasizes that technology should enhance professional judgment, not supplant it. Automated systems serve as decision-support tools that improve efficiency, consistency, and analytical capability, but the ultimate responsibility for financial reporting decisions rests with human professionals. Maintaining rigorous oversight, ethical scrutiny, and informed judgment ensures that digital accounting innovations deliver accurate, reliable, and compliant financial information while upholding the professional and ethical standards that form the foundation of accounting practice.

## D. Governance and Internal Control 4.0

Governance and Internal Control 4.0 represent the evolution of traditional corporate governance and internal control systems in response to digital transformation, automation, and data-driven decision-making in the banking industry. As banks adopt artificial intelligence (AI), cloud computing, blockchain, and real-time transaction processing, governance and internal control frameworks must evolve to address new technological, operational, and ethical risks. Internal Control 4.0 emphasizes continuous monitoring, automation, and integration with digital risk management and accounting systems. According to the Basel Committee on Banking Supervision (2023) and COSO (2022), modern governance and internal control structures are critical to maintaining financial integrity, regulatory compliance, and organizational resilience in the digital banking era.

## 1. Evolution from Traditional Internal Control to Internal Control 4.0

The evolution of internal control systems in the digital era reflects a fundamental shift from traditional, manual processes to what is now referred to as Internal Control 4.0. Historically, internal controls were designed around paper-based or spreadsheet-driven workflows, emphasizing preventive and detective mechanisms, segregation of duties, and periodic post-transaction reviews. These traditional systems provided essential oversight but were often reactive, with risk detection occurring after transactions had been processed, limiting the organization's ability to respond promptly to emerging threats (COSO, 2022).

Internal Control 4.0 represents a transformative approach, leveraging digital technologies to embed controls directly into business processes. Continuous and automated controls are now implemented within ERP systems, financial platforms, and operational workflows, enabling real-time monitoring and instant alerts when anomalies or deviations are detected. This integration allows organizations to move from a periodic assurance model to a continuous control environment, enhancing responsiveness to potential errors, fraud, or compliance breaches.

A key feature of Internal Control 4.0 is the convergence of financial, operational, and IT controls into a unified framework. By combining data from multiple sources transactional records, system logs, and user activity organizations can gain a holistic view of risk exposure. Advanced analytics and artificial intelligence tools facilitate anomaly detection, trend analysis, and predictive risk assessment, allowing organizations to proactively address potential issues before they materialize. For instance, AI algorithms can identify unusual patterns in payment transactions, deviations in system access, or irregularities in procurement processes, supporting more effective decision-making and risk mitigation.

Moreover, digital internal controls are designed to be adaptive and scalable, accommodating the dynamic nature of modern enterprises. COSO (2022) emphasizes that these systems should be closely aligned with enterprise risk management frameworks to ensure that controls remain relevant as business models evolve, technologies advance, and regulatory requirements change. Internal Control 4.0 also

supports audit readiness by maintaining immutable digital records, automated documentation, and continuous reporting capabilities, enhancing transparency and accountability.

## 2. Governance Structure in Digital Banking

Governance in digital banking has become increasingly critical as technological innovation, digital platforms, and cyber risks transform the financial landscape. Effective governance requires clearly defined accountability across all organizational layers to ensure that digital strategy, risk management, and ethical standards are properly aligned with the bank's objectives. At the highest level, the board of directors bears ultimate responsibility for overseeing the bank's digital strategy, establishing risk appetite, and setting ethical and compliance standards. Boards are expected to possess sufficient understanding of digital and cyber risks to exercise informed judgment and provide strategic guidance (Basel Committee, 2023).

Senior management plays a pivotal role in translating board policies into operational practices. This includes implementing governance frameworks, embedding internal controls within digital processes, and ensuring that the bank's technology investments support both strategic goals and regulatory compliance. Effective management must maintain a balance between innovation and risk mitigation, coordinating across multiple departments to integrate risk management into day-to-day digital operations.

Risk and audit committees serve as specialized oversight bodies, focusing on the identification, monitoring, and mitigation of technology, cybersecurity, operational, and compliance risks. They review digital risk assessments, audit reports, and control effectiveness, providing recommendations to the board and senior management for continuous improvement. Their role is especially important in digital banking, where the rapid pace of technological change can introduce emerging risks that require proactive attention.

The three lines of defense model remains a cornerstone of governance in digital banking. Business units, as the first line, are responsible for operational risk management and compliance within their processes, including adherence to digital controls and cybersecurity protocols. The second line, consisting of risk management and compliance functions, provides independent

oversight, develops policies, and monitors adherence to regulatory requirements. The internal audit function forms the third line, offering independent assurance on the effectiveness of risk management, control systems, and governance practices. Together, these three lines ensure that risks are managed consistently and transparently, supporting accountability and informed decision-making.

## 3. Digital Internal Control Components

Digital Internal Control, often referred to as Internal Control 4.0, integrates multiple control layers to ensure reliability, accuracy, and security in financial and operational processes within digital banking. At its core, automated preventive controls play a crucial role by embedding system-based validations, access restrictions, and authorization workflows directly into digital platforms. These controls aim to prevent errors, unauthorized activities, and fraudulent transactions before they occur, reducing reliance on manual oversight and minimizing the risk of financial misstatement (COSO, 2022).

Complementing preventive measures, detective and continuous controls provide real-time monitoring of transactions and system activities. Using advanced analytics and artificial intelligence, these controls can detect anomalies, suspicious patterns, or breaches of internal policies as they happen. Continuous monitoring enhances responsiveness and supports early intervention, which is essential in digital banking environments characterized by high transaction volumes and rapid data flows. Such controls are critical for maintaining operational integrity and ensuring timely reporting to management and regulators (PwC, 2023).

IT General Controls (ITGC) form the foundational layer of digital internal control. They encompass system development governance, change management, access management, and data integrity assurance. By ensuring that IT systems function as intended, ITGC provides a reliable environment for automated accounting processes, predictive analytics, and financial reporting. Without strong ITGC, the effectiveness of other internal control layers may be compromised, potentially leading to operational failures or financial misstatements (KPMG, 2023).

Data governance and integrity controls further reinforce the reliability of digital systems by ensuring that financial and operational

data are accurate, complete, consistent, and traceable across the organization. Policies for data lineage, quality checks, and reconciliation are essential to support auditability and regulatory compliance. Effective data governance ensures that automated reporting, risk models, and decision-making processes are based on trustworthy information, reducing errors and enhancing stakeholder confidence.

## 4. Role of Technology in Internal Control 4.0

In the era of Internal Control 4.0, technology plays a pivotal role in transforming traditional control frameworks into dynamic, real-time systems that enhance both governance and risk management within digital banking. Artificial Intelligence (AI) is at the forefront, enabling automated anomaly detection, predictive risk alerts, and continuous monitoring of high-volume transactional data. By analyzing patterns and flagging unusual behaviors in real time, AI allows banks to proactively address potential operational, financial, or compliance risks before they escalate, thus strengthening the overall control environment (Deloitte, 2023).

Robotic Process Automation (RPA) complements AI by executing repetitive control activities with consistency, speed, and accuracy. Tasks such as reconciliations, approvals, and transaction verifications can be standardized through RPA, reducing human error and ensuring that preventive and detective controls operate seamlessly across multiple systems. This not only improves operational efficiency but also frees staff to focus on higher-value activities, including judgment-based oversight and exception management (KPMG, 2023).

Blockchain technology further enhances the integrity and transparency of internal control processes. Its immutable ledger provides tamper-proof records of transactions, supporting auditability and facilitating traceable workflows. By creating transparent audit trails, blockchain reduces the risk of data manipulation and strengthens confidence in the reliability of financial and operational reporting. In particular, smart contract functionalities can automate compliance-related checks, ensuring that predefined control conditions are enforced consistently (PwC, 2023).

Cloud platforms also play a central role in Internal Control 4.0 by enabling centralized monitoring and scalable infrastructure. Cloud-

based control dashboards integrate data from disparate systems, allowing management and internal auditors to access real-time insights into control effectiveness, exceptions, and risk exposures. The flexibility of cloud computing supports rapid adaptation to changing regulatory requirements, operational processes, and business growth, enhancing both resilience and responsiveness of internal control systems.

The convergence of these technologies AI, RPA, blockchain, and cloud computing creates a synergistic environment in which internal controls are no longer static or periodic but continuous, adaptive, and data-driven. Banks implementing technology-enabled controls report improved detection of operational and compliance risks, reduced error rates, and enhanced governance oversight. This integration allows organizations to not only meet regulatory expectations but also to foster a culture of proactive risk management, operational transparency, and audit readiness in a rapidly digitizing financial landscape (Deloitte, 2023; KPMG, 2023; PwC, 2023).

# CHAPTER IX
# STRATEGIC FINANCIAL MANAGEMENT IN DIGITAL BANKING

Strategic Financial Management in Digital Banking focuses on how banks design, allocate, and control financial resources to achieve sustainable value creation in an increasingly digital and data-driven environment. As digital technologies transform business models, revenue structures, and risk profiles, financial management must evolve beyond traditional budgeting and performance measurement toward integrated, analytics-based, and strategy-oriented approaches. In digital banking, strategic financial management aligns capital allocation, profitability analysis, valuation, and transformation planning with technological innovation and regulatory requirements, enabling banks to enhance competitiveness, resilience, and long-term financial performance in a rapidly changing financial ecosystem.

## A. Performance Metrics and Digital Profitability Analysis

The transformation of banking into a digitally driven industry has fundamentally reshaped how financial performance is measured and evaluated. Traditional banking performance metrics such as Return on Assets (ROA), Return on Equity (ROE), Cost-to-Income Ratio (CIR), and Net Interest Margin (NIM) remain relevant, but they are no longer sufficient on their own to capture the economic realities of digital banking. Digital banks operate on platform-based business models, rely heavily on data analytics, and prioritize scalability, customer experience, and technological efficiency. As a result, performance measurement frameworks have evolved to incorporate digital-specific metrics that assess profitability, efficiency, customer value, and innovation capability (Bunea, Kogan, & Vasarhelyi, 2023).

## 1. Evolution of Performance Measurement in Digital Banking

The evolution of performance measurement in digital banking reflects a fundamental shift from traditional balance-sheet-focused assessments to a more dynamic, multi-dimensional approach that captures both financial and non-financial drivers of value. Conventional banking metrics primarily emphasized interest income, cost-to-income ratios, and branch-level profitability, providing a periodic snapshot of performance. However, the rise of digital banking has introduced diversified revenue streams, including transaction fees, subscription services, embedded finance products, and data monetization models. These non-interest income sources, coupled with lower marginal costs per transaction and higher operational scalability, require banks to adopt a platform-level perspective that evaluates the economic efficiency and strategic value of digital ecosystems rather than isolated branch operations (McKinsey, 2022).

Digital banking performance measurement also benefits from the capability of real-time monitoring. Integrated core banking systems, coupled with automated data capture from digital channels such as mobile apps, payment platforms, and online marketplaces, allow banks to continuously track key performance indicators (KPIs) including transaction volumes, customer engagement, revenue contribution per product, and operational efficiency metrics. This continuous insight enables management to identify trends, detect anomalies, and implement corrective measures promptly, thereby improving responsiveness in highly dynamic market conditions (Deloitte, 2023).

In addition, digital banking increasingly incorporates customer-centric and ecosystem-oriented performance indicators. Metrics such as customer acquisition cost, lifetime value, churn rate, and engagement frequency provide insights into the effectiveness of product offerings and service delivery. Advanced analytics, including predictive and prescriptive models, enhance the ability to anticipate customer behavior and optimize portfolio management, supporting data-driven strategic decisions. Furthermore, sustainability and regulatory compliance metrics are integrated into performance evaluation to align financial outcomes with broader environmental, social, and governance (ESG) objectives, reflecting the growing expectation for responsible banking practices (OECD, 2022).

## 2. Traditional Financial Metrics in a Digital Context

In the era of digital banking, traditional financial metrics such as Return on Assets (ROA), Return on Equity (ROE), Cost-to-Income Ratio (CIR), and Net Interest Margin (NIM) continue to play a critical role in evaluating bank performance, though their interpretation requires adjustment to reflect digital transformation dynamics. ROA remains a measure of how efficiently a bank employs its total assets to generate profit. In digital banks, asset efficiency is influenced not only by tangible assets but also by technology investments, cloud infrastructure, and intangible assets such as proprietary software, customer data, and digital platforms, which form a significant part of the operational base (Deloitte, 2023).

ROE continues to serve as an indicator of shareholder value creation. However, digital banking often entails substantial upfront investments in technology, cybersecurity, and platform development, which can temporarily suppress ROE during early growth phases. As digital banks scale and leverage automation and network effects, ROE can improve substantially, reflecting the high operational leverage inherent in platform-based business models (BIS, 2023). This underscores the importance of interpreting ROE in a forward-looking context, considering the long-term return potential from digital transformation initiatives.

The Cost-to-Income Ratio is particularly relevant in digital banking environments, where automation, straight-through processing, and the reduction of physical branch infrastructure allow for considerable cost savings. Digital banks typically achieve lower CIR than their traditional counterparts, highlighting efficiency gains from technology adoption. However, CIR must be analyzed in conjunction with investment cycles and platform expansion costs to accurately gauge sustainable operational efficiency (McKinsey, 2022).

Net Interest Margin, while still a core metric, is increasingly affected by diversification strategies in digital banking. As banks shift toward fee-based services, subscription models, and embedded financial products, NIM may decline relative to traditional lending-focused institutions. Nevertheless, NIM remains a useful measure for assessing the profitability of interest-earning assets and the effectiveness of risk-adjusted pricing strategies, particularly in hybrid banking models combining traditional lending and digital services.

### 3. Digital-Specific Performance Metrics

In the context of digital banking, performance measurement extends beyond traditional financial metrics to include digital-specific indicators that capture customer behavior, platform efficiency, and technology effectiveness. One critical metric is Customer Acquisition Cost (CAC), which measures the expense incurred to acquire a new digital customer through online channels, including social media marketing, search engine campaigns, and referral programs. Lower CAC indicates more efficient digital marketing strategies and a strong brand ecosystem capable of attracting users at minimal cost. Complementing CAC, Customer Lifetime Value (CLV) estimates the total net profit a bank expects to earn from a customer over the entire relationship. Leveraging advanced analytics and predictive modeling, digital banks can calculate CLV more accurately by incorporating behavioral data, transaction frequency, product usage, and cross-selling potential (Marr, 2022). This allows management to prioritize resources toward high-value customer segments and optimize retention strategies.

Another important KPI is the Active User Ratio, which measures the proportion of users actively engaging with digital banking services relative to total registered customers. High engagement levels signal customer satisfaction, successful onboarding, and effective product offerings. Monitoring this metric enables banks to identify dormant accounts and deploy targeted reactivation initiatives. Transaction Cost per Unit is a metric that assesses operational efficiency in digital payment and transaction processing systems. Lower transaction costs indicate streamlined processing, automation effectiveness, and cost savings, which can directly enhance profitability.

Additionally, Platform Scalability Metrics evaluate the technological backbone of digital banking operations, including system capacity, uptime, and processing speed. High system reliability ensures uninterrupted customer service, supports high transaction volumes, and mitigates operational risk, while slow or unstable platforms can lead to customer dissatisfaction and revenue leakage. These digital-specific metrics not only provide a more granular understanding of operational and customer-centric performance but also directly align financial outcomes with strategic objectives such as innovation, customer satisfaction, and digital growth. By integrating these indicators with

traditional financial measures, banks can achieve a holistic view of organizational performance that reflects both economic efficiency and the effectiveness of digital transformation initiatives. In rapidly evolving digital markets, continuous monitoring of these KPIs allows institutions to adapt strategies proactively, optimize resource allocation, and maintain competitive advantage in the digital financial ecosystem.

## 4. Digital Profitability Analysis Models

Digital profitability analysis in modern banking transcends traditional product-centric accounting by focusing on customer-level and ecosystem-level performance. In digital environments, banks manage a multitude of channels, services, and revenue streams, making conventional cost allocation methods insufficient for capturing the true profitability of operations. Activity-Based Costing (ABC), particularly in its time-driven form, offers a robust solution by linking costs directly to digital activities and customer interactions. By leveraging automated transaction and operational data, banks can attribute expenses accurately to mobile banking, online payments, API usage, or embedded finance services. Kaplan and Anderson (2021) highlight that time-driven ABC models are especially effective in digital banking because they utilize real-time data to allocate costs dynamically, reflecting the complexity and scalability of digital operations.

Beyond cost attribution, digital banks increasingly employ integrated profitability dashboards that combine financial and non-financial metrics. These dashboards provide a comprehensive view of profitability across multiple dimensions, including customer segments, service channels, product lines, and even entire ecosystems of partners and fintech collaborators. For instance, profitability can be assessed not only by revenue minus cost per transaction but also by evaluating customer engagement, retention rates, cross-sell opportunities, and digital adoption metrics. This holistic approach enables management to identify high-value customers and underperforming segments, guiding resource allocation and strategic interventions effectively.

Advanced analytics further enhances profitability analysis by incorporating predictive elements. Using behavioral data, transaction patterns, macroeconomic indicators, and market trends, banks can forecast future revenue and cost trajectories with greater precision. Predictive models allow institutions to simulate the impact of strategic

decisions, such as pricing changes, new product launches, or digital expansion initiatives, on overall profitability. Moreover, these models can support scenario analysis, helping management understand how shifts in customer behavior or external conditions might influence financial outcomes (PwC, 2023).

## B. Digital Banking Valuation and Strategy

The rapid digitalization of banking has fundamentally altered how banks are valued and how financial strategy is formulated. Unlike traditional banks, whose valuation is largely driven by balance-sheet strength, interest income stability, and branch-based market dominance, digital banks derive value from platform scalability, data assets, technological capabilities, and ecosystem integration. As a result, digital banking valuation requires a strategic framework that incorporates both conventional financial metrics and forward-looking digital value drivers (Damodaran, 2023).

### 1. Conceptual Shift in Bank Valuation

The conceptual approach to bank valuation has undergone a significant transformation in the digital era. Traditional valuation models primarily focused on tangible assets, net interest margins, and regulatory capital, emphasizing the stability and historical performance of banks with extensive branch networks and physical infrastructure. However, digital banking fundamentally alters these dynamics by operating with minimal physical presence, leveraging high technology intensity, and prioritizing customer engagement and digital platform ecosystems. The Bank for International Settlements (BIS, 2023) notes that a substantial and increasing portion of bank value now resides in intangible assets, including proprietary software, customer data, advanced algorithms, and brand reputation. These elements are critical drivers of competitive advantage, customer retention, and scalable revenue models, yet they are often underrepresented in traditional accounting metrics.

This conceptual shift necessitates valuation approaches that account for the strategic importance of digital capabilities and future growth potential. Unlike conventional banks, digital banks derive value not only from current earnings but also from their ability to innovate,

rapidly launch new products, and integrate with fintech ecosystems. Such flexibility represents real options, which provide management with the opportunity to exploit favorable market conditions, invest in technology enhancements, or enter new digital service segments. These options create additional value that static, historical-based accounting models typically fail to capture. Incorporating these elements into valuation frameworks requires a forward-looking perspective that blends financial, operational, and technological considerations.

Moreover, investor and regulatory expectations are increasingly aligned with non-financial indicators. Metrics such as customer acquisition and retention rates, platform scalability, and engagement levels are now critical inputs for understanding a bank's sustainable value. Brand trust and data analytics capabilities directly influence future revenue streams, risk management efficiency, and the resilience of digital banking models under volatile market conditions. Traditional net asset approaches or earnings multiples may undervalue these intangible assets, leading to a misrepresentation of the bank's true economic worth.

In practice, contemporary valuation methodologies for digital banks often integrate discounted cash flow (DCF) models with adjustments for intangible asset contributions, scenario-based forecasts, and optionality in digital growth strategies. Analysts increasingly supplement these quantitative methods with qualitative assessments of technological maturity, digital adoption rates, and ecosystem partnerships. This comprehensive approach ensures that valuation reflects both current performance and strategic potential, providing investors, regulators, and management with a more accurate understanding of value creation in digital banking environments.

## 2. Valuation Approaches in Digital Banking

Valuation in digital banking requires a nuanced approach that accounts for the unique characteristics of technology-driven financial institutions. Traditional valuation methods remain relevant but must be adapted to capture the strategic value of digital capabilities, scalability, and intangible assets. Among the most commonly applied approaches, the Discounted Cash Flow (DCF) model continues to serve as a foundational tool. In the context of digital banks, DCF projections must integrate assumptions about rapid digital growth, economies of scale,

and investment cycles in technology infrastructure. Unlike conventional banks, digital banks often exhibit an initial period of limited profitability followed by accelerated cash flows as platform adoption scales and operational efficiencies are realized. Damodaran (2023) emphasizes that accurately modeling these dynamics is crucial to reflecting the true economic potential of digital banking ventures.

Comparable company analysis is another widely used method, but traditional multiples such as Price-to-Book (P/B) or Price-to-Earnings (P/E) are supplemented with digital-specific metrics. Metrics like Price-to-Customer, Revenue per User, and Cost-to-Income efficiency ratios are increasingly applied to neo-banks and digital platforms, capturing growth potential and cost structure advantages. McKinsey (2022) notes that these institutions often command higher valuation multiples compared to traditional banks, reflecting expected scalability and lower marginal costs once digital operations reach maturity. Such metrics provide investors with a clearer understanding of the operational leverage and market traction inherent in digital business models.

Economic Value Added (EVA) is also gaining prominence in evaluating digital banking investments. EVA measures whether initiatives, particularly long-term platform and ecosystem investments, generate returns exceeding the cost of capital. This approach supports management in assessing the value creation from strategic digital initiatives, guiding resource allocation and performance incentives.

## 3. Strategic Value Drivers in Digital Banking

In digital banking, valuation is increasingly determined by strategic value drivers that extend beyond immediate financial performance, reflecting the institution's long-term growth potential and digital maturity. One of the most significant drivers is scalability. Digital platforms allow banks to expand their customer base rapidly with relatively low incremental costs, enabling high operating leverage and stronger long-term profitability. As customer adoption grows, fixed technology and infrastructure investments are spread over a larger revenue base, amplifying the impact on overall valuation. Scalability is particularly critical for neo-banks and fintech-integrated platforms, where rapid market penetration can significantly increase investor perception of value (Accenture, 2023).

Another key driver is the capability to leverage customer data through advanced analytics. Digital banks collect vast amounts of transactional, behavioral, and demographic data, which can be used for personalized offerings, cross-selling, and predictive customer engagement. By enhancing customer lifetime value and stabilizing revenue streams, sophisticated data and analytics capabilities become central to valuation assessments. Institutions that effectively monetize data while maintaining privacy and ethical standards demonstrate stronger resilience and strategic positioning in competitive markets.

Technology architecture also plays a pivotal role in shaping strategic value. Cloud-native core banking systems, modular microservices, and API-based architectures improve operational agility, enable faster product development, and reduce the risk of system downtime or operational failures. Such technological sophistication not only lowers operational costs but also supports regulatory compliance and seamless integration with third-party service providers, enhancing both efficiency and market credibility.

Ecosystem integration represents an additional strategic value driver. Digital banks increasingly form partnerships with fintechs, payment processors, and embedded finance providers, creating new revenue streams and strategic optionality. By participating in broader digital ecosystems, banks can access innovative services, diversify income, and enhance customer engagement, which collectively strengthen the institution's competitive edge and long-term valuation potential (Accenture, 2023).

Incorporating these strategic value drivers into planning and valuation ensures that digital banking assessments capture the full spectrum of competitive advantages. Unlike traditional banks, whose value is primarily derived from interest margins and tangible assets, digital banks derive a substantial portion of their worth from intangible factors such as platform scalability, data monetization, technology robustness, and ecosystem connectivity. Investors and management alike must consider these drivers to make informed decisions regarding growth, capital allocation, and strategic positioning in an increasingly technology-driven financial landscape.

## 4. Digital Banking Strategy and Value Creation

In digital banking, strategy and value creation are tightly interwoven, as strategic decisions regarding platform development, product innovation, and market expansion directly shape the institution's valuation. Unlike traditional banking models that emphasize interest margins and physical branch networks, digital banking competition increasingly revolves around ecosystems, where the ability to orchestrate platforms, integrate services, and harness data determines long-term value (Porter & Heppelmann, 2022). Strategic orientation thus becomes a key determinant of both financial performance and intangible asset accumulation, such as customer relationships, technology infrastructure, and brand equity.

A platform strategy is one of the most prominent approaches, positioning the bank as a digital marketplace that connects customers, fintech partners, and third-party service providers. By facilitating multi-sided interactions, digital banks can generate diversified revenue streams from transaction fees, embedded finance services, and partner integrations. This ecosystem-based strategy enhances scalability and network effects, increasing the strategic optionality and market valuation of the institution.

Customer-centric strategies focus on leveraging analytics, artificial intelligence (AI), and machine learning to deliver personalized financial solutions. By optimizing customer engagement and lifetime value, banks can deepen relationships, reduce churn, and improve cross-selling opportunities. The ability to transform data into actionable insights strengthens competitive differentiation and supports higher valuation multiples, reflecting the bank's capacity for sustainable revenue generation and customer retention.

Cost leadership through automation is another strategic dimension, wherein banks utilize Robotic Process Automation (RPA), AI-driven workflows, and cloud-based infrastructures to minimize operational costs and improve efficiency ratios. Lower cost-to-income ratios enhance profitability while freeing capital for innovation or growth initiatives. From a valuation perspective, cost-efficient digital operations reduce risk and enhance return on invested capital, providing a strong foundation for sustainable value creation.

## C. Capital Allocation and Digital Investment Assessment

Capital allocation is a core function of strategic financial management in digital banking, as banks must balance regulatory capital requirements with significant investments in technology, innovation, and digital infrastructure. In the digital era, capital allocation decisions extend beyond traditional lending and asset growth considerations to include investments in core banking systems, cloud platforms, artificial intelligence, cybersecurity, and fintech partnerships. Effective digital investment assessment ensures that limited financial resources are deployed in projects that generate sustainable value, enhance competitiveness, and maintain financial stability (Brealey, Myers, & Allen, 2023).

### 1. Changing Nature of Capital Allocation in Digital Banking

The nature of capital allocation in digital banking has undergone a profound transformation, reflecting the shift from traditional, asset-heavy banking models toward technology-driven, platform-based operations. Historically, banks concentrated capital on credit portfolios, physical branch networks, and ATMs, emphasizing tangible assets and incremental expansions. These investments were relatively straightforward to plan, measure, and control, as cash flows were predictable and returns could be directly linked to interest income or transaction volumes. However, the digital era has redefined strategic priorities, compelling banks to redirect significant portions of capital toward intangible assets such as software development, advanced data analytics, cloud-based platforms, cybersecurity infrastructure, and customer experience enhancements. According to the Bank for International Settlements (BIS, 2023), technology expenditures are now considered strategic investments that underpin growth, competitiveness, and resilience, rather than discretionary operational costs.

This paradigm shift introduces several challenges for conventional capital budgeting frameworks. Digital banking investments often involve high upfront costs, with financial benefits realized only over an extended horizon. Unlike traditional loans or physical expansions, returns from digital platforms may be indirect, encompassing operational efficiency gains, increased customer lifetime

value, ecosystem monetization, and enhanced scalability. Moreover, these investments are subject to higher uncertainty, as technological adoption, customer engagement, regulatory compliance, and cybersecurity risks influence the ultimate success and financial payoff. Traditional accounting measures, which primarily focus on tangible assets and short-term profitability, may undervalue these strategic initiatives, necessitating new approaches that capture both financial and strategic benefits.

To address these complexities, digital banks increasingly integrate scenario-based forecasting, real options valuation, and performance metrics linked to platform usage, active customer engagement, and data monetization. This enables management to assess the potential upside of technology investments under multiple market conditions, align capital allocation with long-term strategic objectives, and prioritize initiatives that enhance digital agility. Furthermore, the integration of risk-adjusted metrics ensures that capital is deployed efficiently while maintaining resilience against operational, credit, and market uncertainties inherent in digital banking ecosystems.

## 2. Principles of Capital Allocation in Digital Banking

Capital allocation in digital banking is increasingly guided by a set of principles designed to balance strategic growth, risk management, and regulatory compliance. At the core is value creation, which requires that every investment whether in technology platforms, data analytics, or customer experience initiatives generates returns that exceed the bank's cost of capital. These returns may be realized directly through revenue growth from digital products and services, or indirectly through efficiency gains, improved risk management, and enhanced operational resilience. According to the Bank for International Settlements (BIS, 2023), prioritizing value creation ensures that scarce capital is deployed to initiatives that contribute substantively to long-term financial performance rather than short-term operational convenience.

Closely linked to value creation is strategic alignment. Digital banking investments must support the institution's overarching strategic objectives, such as scaling digital platforms, achieving customer-centric service delivery, or integrating with broader fintech ecosystems. Strategic alignment ensures that capital allocation decisions reinforce the bank's competitive positioning and long-term

growth trajectory, rather than being reactive or ad hoc expenditures. For example, investments in cloud-native core banking systems or AI-driven customer analytics are not just operational expenses they underpin scalability, personalization, and ecosystem monetization, which are central to digital banking strategy (McKinsey, 2022).

Another critical principle is risk-adjusted assessment. Digital investments are exposed to multiple risk dimensions, including operational failures, cybersecurity threats, regulatory changes, and execution uncertainties. Effective capital allocation involves evaluating expected returns against these risks, often using scenario analysis, sensitivity testing, and risk-adjusted performance metrics. By incorporating risk considerations, banks can prioritize initiatives that offer the best trade-off between potential value and exposure to adverse outcomes (Deloitte, 2023).

Finally, regulatory compliance remains essential. Capital allocation decisions must respect regulatory frameworks such as Basel III/IV, which set minimum capital adequacy requirements and risk-weighted asset considerations, as well as local supervisory guidelines. Ensuring compliance safeguards financial stability and maintains stakeholder confidence, particularly when investments involve novel digital products or partnerships.

### 3. Digital Investment Assessment Techniques

Assessment of digital investments in banking relies on a combination of traditional financial metrics and advanced techniques adapted to the unique characteristics of digital transformation. Net Present Value (NPV) remains a foundational tool, providing an estimate of the present value of expected cash flows from digital initiatives. In the context of digital banking, NPV calculations must integrate assumptions about adoption rates, scalability effects, and potential cost synergies arising from automation, cloud infrastructure, or AI-driven platforms. By capturing these dynamic factors, NPV helps quantify the financial contribution of digital projects to the bank's overall value (BIS, 2023).

Internal Rate of Return (IRR) is widely used to compare alternative digital projects, offering insight into the profitability of competing initiatives. However, IRR may underestimate strategic flexibility in highly uncertain environments where digital investments

are phased or linked to growth options. Banks often complement IRR with scenario analysis to account for variability in user uptake, transaction volumes, and regulatory changes (McKinsey, 2022).

The payback period provides a simpler perspective, particularly useful for investments focused on risk mitigation, such as cybersecurity upgrades or compliance systems. While it does not fully capture long-term strategic value, the payback period highlights the speed at which initial capital outlays are recovered, which is critical when operational resilience and regulatory adherence are prioritized.

Economic Value Added (EVA) offers a value-based lens, assessing whether a digital investment generates returns exceeding the bank's cost of capital. By focusing on value creation rather than accounting profits alone, EVA aligns investment decisions with shareholder value enhancement and long-term strategic goals (Stewart, 2021).

Given the inherent uncertainty and optionality of digital projects, real options analysis has become particularly relevant. Many digital investments create optionality, such as the ability to scale platforms, launch new services, or defer additional spending depending on market response. Real options valuation captures the economic value of this flexibility, providing a more realistic and forward-looking assessment of investment potential (PwC, 2023).

## 4. Technology Investments and Capital Efficiency

Investments in technology play a pivotal role in enhancing capital efficiency within digital banking, as they enable banks to optimize resource utilization, lower operational expenses, and improve risk management outcomes. Automation of routine processes, such as transaction processing, reconciliations, and regulatory reporting, reduces manual labor requirements and minimizes error rates, directly contributing to cost savings. Simultaneously, advanced data analytics and AI-driven models facilitate more accurate credit assessments, dynamic portfolio management, and predictive risk monitoring, which improve risk-adjusted returns and strengthen asset quality. These capabilities allow banks to deploy capital more effectively, ensuring that resources are allocated to high-performing and strategically aligned activities rather than being absorbed by inefficiencies or unproductive operations (McKinsey, 2022).

Moreover, digital investments can generate economies of scale. As platforms and digital services grow, incremental costs per transaction or per customer decrease, enabling banks to serve larger customer bases without proportionally increasing capital outlays. Cloud infrastructure and modular system architectures further enhance scalability, allowing banks to expand operations rapidly while maintaining cost discipline. This structural efficiency enhances the overall return on invested capital and supports sustainable growth (BIS, 2023).

However, the realization of capital efficiency gains depends heavily on governance, project management, and alignment with strategic objectives. Poorly executed digital projects such as fragmented system upgrades, inadequate integration across platforms, or underutilized analytics tools can result in cost overruns, implementation delays, and operational disruptions. Such outcomes not only erode anticipated efficiency benefits but may also negatively impact shareholder value and regulatory compliance. Therefore, rigorous project evaluation, risk-adjusted capital allocation, and continuous performance monitoring are essential to ensure that technology investments deliver their intended value (PwC, 2023).

## D. Strategic Financial Transformation Planning

Strategic financial transformation planning represents the culmination of digital banking strategy, integrating financial management, technology adoption, organizational change, and long-term value creation. In the digital era, financial transformation is not limited to incremental process improvements but involves a fundamental redesign of financial structures, performance management systems, and decision-making models. According to the World Economic Forum (2023), banks that approach digital transformation strategically rather than tactically are more likely to achieve sustainable competitive advantage and financial resilience.

### 1. Concept and Scope of Financial Transformation

Financial transformation in digital banking represents a fundamental rethinking of how financial resources are managed, controlled, and optimized to support rapidly evolving digital business

models. Unlike traditional transformation efforts that primarily target cost reduction or process streamlining, digital financial transformation emphasizes agility, scalability, and the integration of advanced analytics into financial decision-making. This shift entails a holistic redesign of the financial architecture, including real-time reporting systems, predictive planning tools, and automated workflows that enable timely insights for strategic and operational decisions. Governance frameworks are also adapted to ensure that financial policies, risk management practices, and compliance mechanisms align with the dynamic requirements of digital operations, bridging the gap between finance, technology, and business strategy (Deloitte, 2023).

The scope of financial transformation extends beyond technology adoption to encompass changes in performance measurement and capital deployment. Traditional metrics, such as Return on Assets (ROA) or Cost-to-Income Ratio (CIR), are complemented by digital-specific indicators like customer acquisition cost, lifetime value, and platform scalability. These metrics enable banks to evaluate profitability and efficiency at a granular, customer- or transaction-level, providing actionable insights that support strategic prioritization of resources. Additionally, capital allocation mechanisms are increasingly guided by principles of value creation, strategic alignment, and risk-adjusted assessment, reflecting the higher reliance on intangible assets such as software, data, and digital platforms, which are central to digital banking models (BIS, 2023).

Another critical aspect of financial transformation is the incorporation of forward-looking, scenario-based planning. Digital banks leverage predictive analytics and AI-driven simulations to assess the impact of various market, operational, and technological scenarios on financial performance. This forward-looking approach enhances resilience, supports informed decision-making under uncertainty, and aligns financial planning with long-term strategic objectives, including ecosystem integration, customer-centric innovation, and operational scalability (PwC, 2023).

## 2. Drivers of Strategic Financial Transformation

Strategic financial transformation in digital banking is driven by a convergence of technological, regulatory, competitive, and business model shifts that compel banks to rethink traditional financial

management approaches. One of the foremost drivers is technological disruption. Rapid advances in artificial intelligence, cloud computing, and platform-based architectures have redefined how financial processes are executed, monitored, and analyzed. These technologies enable real-time data capture, predictive analytics, and automated workflows, necessitating new mechanisms for financial planning, control, and reporting that are agile, scalable, and closely integrated with operational systems (Deloitte, 2023).

Changing revenue models represent another critical driver. Unlike conventional banks that rely primarily on net interest income, digital banks increasingly generate revenue through fee-based services, subscription models, and embedded financial offerings within broader digital ecosystems. This shift demands a reorientation of budgeting, performance measurement, and capital allocation practices to account for new income streams, recurring revenue cycles, and customer-level profitability. Financial systems must be capable of tracking and attributing revenues and costs at a granular level to support informed strategic decisions and long-term value creation (McKinsey, 2022).

Regulatory complexity further propels the need for transformation. Digital banking operates under heightened scrutiny regarding data security, anti-money laundering (AML), cyber risk management, and capital adequacy. Banks must implement sophisticated financial reporting systems that capture real-time risk exposures, ensure compliance with Basel III/IV and local supervisory requirements, and provide transparent disclosure to regulators. Failure to adapt can lead to regulatory penalties, reputational damage, and inefficiencies in capital deployment (BIS, 2023).

## 3. Strategic Planning Framework for Financial Transformation

Strategic planning for financial transformation in digital banking involves a systematic framework designed to ensure that financial functions evolve in alignment with digital strategy and long-term organizational objectives. The process begins with defining a clear vision and ensuring strategic alignment. This step establishes the overarching financial goals that support the bank's digital ambitions, such as enhancing data-driven decision-making, improving capital efficiency, or enabling scalable platform operations. A well-articulated

vision ensures that all transformation initiatives contribute to sustainable value creation and competitive advantage (PwC, 2023).

The next stage involves a comprehensive current-state assessment, which evaluates existing financial systems, processes, organizational capabilities, and performance gaps. This diagnostic step identifies inefficiencies, manual dependencies, outdated technology, and skill shortages that could hinder digital transformation. By understanding these baseline conditions, banks can prioritize areas requiring urgent attention, allocate resources more effectively, and set realistic expectations for transformation outcomes (Deloitte, 2023).

Building on the assessment, a target operating model is developed to define the future-state financial function. This model incorporates automation, advanced analytics, cloud-based platforms, and integrated digital tools to streamline processes, enhance accuracy, and enable real-time insights. It also addresses the organizational structure, roles, and governance required to support a digitally enabled financial function. By clearly specifying how technology, processes, and people will interact, the target operating model provides a blueprint for transformation that balances efficiency, control, and innovation (McKinsey, 2022).

The transformation roadmap translates strategic objectives into actionable initiatives. It includes phased implementation plans with defined milestones, resource allocation, risk management provisions, and governance structures to ensure accountability. The roadmap helps coordinate cross-functional activities, sequence interdependent projects, and manage the pace of change to minimize disruption to ongoing banking operations. Regular progress reviews and updates ensure that the transformation remains adaptive to evolving business conditions and technological advancements (PwC, 2023).

## 4. Role of Technology in Financial Transformation

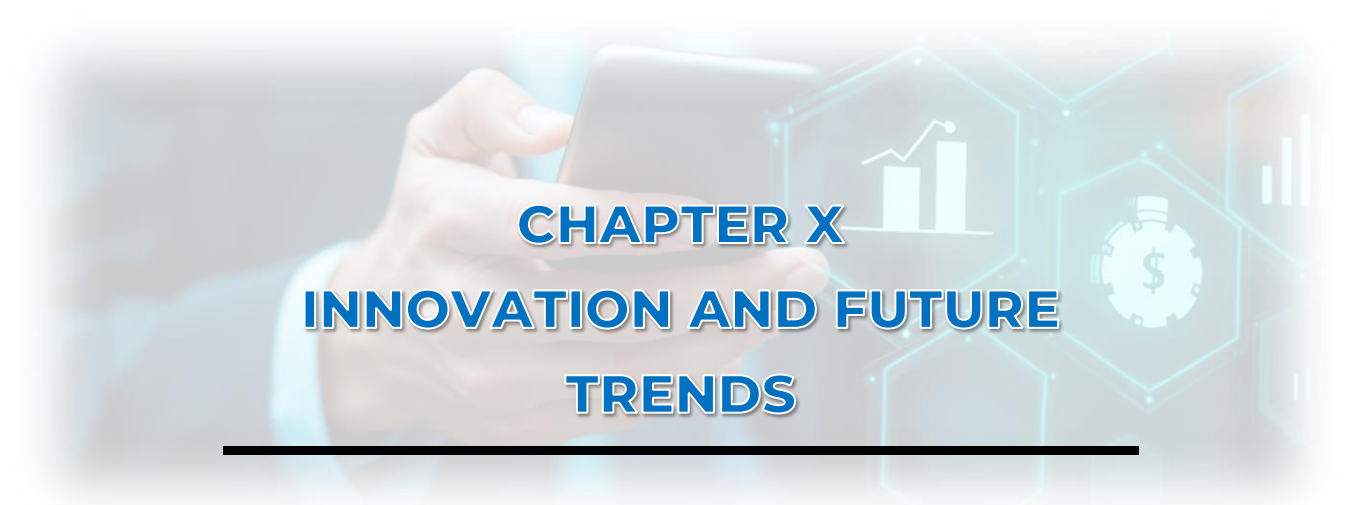
Technology serves as a cornerstone in driving financial transformation within digital banking, fundamentally reshaping how financial resources are managed, analyzed, and reported. Cloud-based financial systems provide scalable infrastructure that supports real-time reporting, centralized data management, and seamless integration with other digital platforms. This enables banks to consolidate financial information across diverse business units and geographies, enhancing

decision-making agility and operational efficiency (IBM, 2023). Furthermore, cloud solutions reduce dependency on legacy systems, lower IT maintenance costs, and allow rapid deployment of new financial functionalities, aligning technology investments with strategic objectives.

Artificial Intelligence (AI) plays a critical role in augmenting traditional finance functions by enabling predictive analytics, scenario modeling, and automated risk assessments. AI-driven forecasting allows banks to anticipate cash flow needs, optimize capital allocation, and simulate the financial impact of various market and operational scenarios. These capabilities enhance strategic planning and provide management with actionable insights that support both short-term operational decisions and long-term investment strategies (Deloitte, 2023). In addition, AI facilitates anomaly detection, fraud prevention, and early warning systems for credit and liquidity risks, strengthening the reliability and resilience of financial operations.

Robotic Process Automation (RPA) further complements digital transformation by automating repetitive, rules-based tasks such as accounts reconciliation, transaction posting, and compliance reporting. By minimizing manual intervention, RPA not only reduces processing errors and operational costs but also frees finance professionals to focus on higher-value activities, including financial analysis, performance monitoring, and strategic business partnering. This shift enhances the role of the finance function as a proactive contributor to organizational strategy rather than a purely transactional unit (McKinsey, 2022).

However, successful technological adoption in financial transformation requires robust data governance and cybersecurity frameworks. As financial operations become increasingly digital, ensuring the accuracy, integrity, and security of financial data is paramount. Proper governance includes standardized data lineage, audit trails, and regulatory compliance checks, while cybersecurity measures protect sensitive financial information from breaches, manipulation, or operational disruption. The integration of strong controls with advanced technology ensures that transformation efforts deliver both efficiency and trustworthiness, enabling banks to achieve sustainable performance improvements while meeting regulatory expectations (PwC, 2023).



# CHAPTER X
# INNOVATION AND FUTURE TRENDS

Innovation and Future Trends in banking accounting highlight how emerging technologies and new organizational paradigms are reshaping the way financial information is generated, analyzed, and governed. Rapid advances in digital simulation, artificial intelligence, quantum computing, and autonomous systems are transforming accounting from a historically retrospective function into a forward-looking, predictive, and continuously adaptive discipline. In this context, innovation is not only a driver of operational efficiency but also a strategic enabler that influences decision-making quality, risk management, ethical governance, and professional competencies, positioning banking accounting at the center of future digital financial ecosystems.

## A. Digital Twin Technology in Banking Simulations

A digital twin is a dynamic, virtual replica of a real-world system that ingests live and historical data to simulate behaviour, run what-if scenarios, and produce actionable insights. In banking, digital twins can model discrete components (a payment engine, customer journey, or a loan portfolio) or complex, interconnected systems (entire balance-sheet dynamics, enterprise risk architecture, or end-to-end customer experience). By enabling controlled experimentation in a safe, sandboxed environment, digital twins let banks anticipate failures, optimise design choices, and improve decision quality without disrupting production systems (Altair, 2023; IADB, 2024).

### 1. Key Use Cases

In digital banking, the application of advanced simulation and digital twin technologies has become central to enhancing operational

resilience, customer experience, risk management, and regulatory compliance. One of the key use cases is operational resilience and capacity planning, where digital twins allow banks to simulate traffic spikes, such as those occurring on payroll days or during major retail events like Black Friday. These simulations help financial institutions to appropriately size cloud capacity, test failover strategies, and rehearse incident response procedures. By revealing potential choke points and stress areas, banks can verify recovery time objectives and ensure continuity under realistic load conditions (Altair, 2023).

Another significant application lies in customer journey and product experimentation. Digital twins enable banks to model customer behavior across the entire lifecycle, from onboarding to product adoption and servicing. By simulating potential changes in user interface, product features, or pricing, banks can estimate impacts on revenue, churn, and customer effort before implementing changes in production environments. This proactive approach reduces operational risk and enhances decision-making for customer-centric strategies.

Portfolio stress-testing and credit dynamics are also enhanced by digital twin methodologies. By combining granular customer-level behavioral models, including probability of default (PD) and propensity to draw, with macroeconomic scenarios, banks can generate more accurate estimates of expected credit loss (ECL) trajectories, concentration risks, and capital requirements. The ability to run thousands of scenario permutations rapidly provides deeper insights than traditional stress-testing tools and enables more agile capital and risk management.

Liquidity and payments network simulation represent another core application. Digital twins recreate intra-day payment flows and counterparty exposures to assess settlement risk, potential funding gaps, and the consequences of system outages on liquidity positions. This capability allows banks to proactively identify vulnerabilities in their operational and funding frameworks.

Fraud and anti-money laundering (AML) scenario simulation benefits from digital twin technology as well. Banks can test detection rules against synthetic adversary patterns, evaluating detection rates, false positives, and investigator capacity requirements without exposing actual customer data, thus improving compliance and security while safeguarding privacy.

## 2. Architecture and Data Requirements

A robust digital twin architecture for banking integrates multiple layers to enable comprehensive simulation, analytics, and decision support. At the foundation is the data ingestion layer, which aggregates real-time feeds from core banking systems, payment networks, customer relationship management platforms, market data providers, and third-party services. This layer ensures that the twin operates on up-to-date and comprehensive information, capturing both internal operations and external market dynamics. Above this, a centralized data platform or single source of truth typically a governed data lake or warehouse maintains data lineage, metadata management, and quality controls, forming the backbone for reliable modeling and analytics (Altair, 2023).

The model layer is composed of modular submodels that represent key aspects of banking operations, including customer behavior, credit and market shocks, operational failure modes, IT capacity constraints, and liquidity dynamics. These submodels can be composed into composite scenarios, enabling the simulation of complex interactions across financial, operational, and technological dimensions. The simulation engine and orchestration layer then executes these scenarios, manages stochastic and parallel runs, and ensures efficient workload distribution, allowing banks to stress-test multiple conditions rapidly.

For decision-making, the analytics and visualization layer provides dashboards, sensitivity analyses, and scenario comparators that translate raw simulation outputs into actionable insights. This enables managers to assess the impact of strategic choices, operational disruptions, or regulatory changes in a comprehensible format. To ensure reliability and regulatory compliance, a governance and audit layer underpins the system, incorporating version control, model registry, approval workflows, and immutable logs to facilitate traceability, validation, and auditability.

Data requirements for digital twins are extensive and exacting. High-quality, time-stamped transactional data, detailed product definitions, instrument valuations, operational telemetry such as latency and error rates, workforce schedules, and external macroeconomic or market feeds are all critical inputs. Lineage, completeness, and consistency checks are mandatory because the accuracy and usefulness

of the digital twin are highly sensitive to input data quality. Inaccurate or incomplete data can materially distort outputs, leading to flawed stress-testing, capacity planning, or risk assessment results (Altair, 2023).

## 3. Modeling Approaches

Modeling approaches in banking digital twins leverage diverse methodologies to capture the complexity of financial, operational, and customer dynamics. Agent-based models are particularly useful for simulating the behavior of thousands or even millions of individual customer agents, each governed by specific behavioral rules. These models enable banks to analyze customer journeys, adoption patterns, and contagion effects, such as how a change in pricing or service experience might propagate across the customer base. By representing heterogeneous agent behaviors, agent-based modeling provides insights into emergent system-level outcomes that traditional aggregate models may overlook (Macal & North, 2019).

System dynamics models complement this approach by focusing on flows, stocks, and feedback loops within the banking system. These models are ideal for capturing the interactions between balance-sheet items, liquidity positions, and operational constraints over time. By representing feedback mechanisms, such as the effect of liquidity shortages on lending capacity or the interplay between credit defaults and capital adequacy, system dynamics models provide a macroscopic view of systemic risk and resource allocation (Sterman, 2022).

Hybrid stochastic models further enhance predictive capability by combining statistical and machine learning techniques for short-term dynamics with scenario-driven stress inputs to assess tail-risk events. These models allow banks to capture both the probabilistic behavior of day-to-day operations and extreme, low-probability shocks, such as cyberattacks, sudden liquidity drains, or market shocks. By integrating stochastic elements with stress-testing frameworks, hybrid models support forward-looking risk assessment and regulatory compliance, particularly under Basel III/IV requirements (BIS, 2023).

Digital twin ensembles extend these modeling approaches by running multiple model variants in parallel, enabling the quantification of model risk and structural uncertainty. By comparing outputs from

different modeling assumptions, banks can assess the robustness of predictions and identify potential vulnerabilities. Ensemble modeling is particularly valuable in high-uncertainty environments, where reliance on a single model could lead to biased or incomplete insights (Altair, 2023).

Collectively, these modeling approaches allow digital twins to provide a multi-dimensional, dynamic, and probabilistic view of banking operations. They enable banks to simulate complex interactions among customers, markets, and internal processes, thereby supporting strategic decision-making, stress-testing, and operational resilience in an increasingly digital financial ecosystem. By combining agent-based, system dynamics, hybrid stochastic, and ensemble methodologies, financial institutions can achieve both granularity and systemic insight, ensuring that digital twins are both predictive and actionable.

## 4. Accounting & Reporting Implications

The adoption of banking digital twins carries significant accounting and reporting implications, particularly as financial institutions increasingly rely on simulated outputs for forward-looking decision-making. Digital twin outputs can inform expected credit loss (ECL) calculations under IFRS 9 by generating probabilistic credit scenarios, helping banks to anticipate potential credit deterioration across portfolios. Similarly, twins support fair-value sensitivity analyses in accordance with IFRS 13, allowing finance teams to model the impact of market shocks or liquidity constraints on instrument valuations. These forward-looking estimates must, however, be fully auditable and meticulously documented, with auditors expecting comprehensive model governance artifacts, input data snapshots, and sensitivity disclosures to ensure reliability and transparency (IFRS Foundation, 2023).

In cases where twins are used to derive valuations for illiquid or complex instruments, the outputs may shift more measurements into Level 3 fair value inputs. This classification demands rigorous disclosure of underlying assumptions, modeling methodologies, and sensitivity ranges, as Level 3 valuations are inherently subjective and carry greater uncertainty. Transparent communication of these

assumptions is essential for stakeholders to understand the potential variability and risk embedded in financial statements (KPMG, 2023).

Digital twin simulations also play a critical role in regulatory filings and stress-testing exercises. For example, banks can leverage twin-based scenario analysis to support ICAAP (Internal Capital Adequacy Assessment Process) and ILAAP (Internal Liquidity Adequacy Assessment Process) submissions, demonstrating capital and liquidity resilience under adverse conditions. Regulators expect traceability from the assumptions and parameters used in the twin models to the reported capital and liquidity metrics, ensuring that the simulations are not only theoretically robust but also operationally connected to regulatory reporting (Basel Committee, 2023).

## B. Quantum Computing and Future of Accounting

Quantum computing represents a paradigm shift in computation by exploiting quantum-mechanical phenomena such as superposition, entanglement, and quantum interference to process information in fundamentally new ways. Unlike classical computers that operate on binary bits, quantum computers use qubits, enabling them to solve certain classes of problems exponentially faster. For accounting and financial reporting domains characterized by massive datasets, complex optimization, probabilistic estimation, and high-dimensional risk quantum computing holds the potential to transform how data are processed, analyzed, and assured. Although practical, fault-tolerant quantum systems are still emerging, their implications for accounting theory, practice, and regulation are already shaping strategic planning in the financial sector (Preskill, 2018; Arute et al., 2019; McKinsey, 2023).

### 1. Conceptual Foundations Relevant to Accounting

The conceptual foundations of quantum computing offer intriguing implications for accounting, particularly in areas requiring complex computation, simulation, and optimization. One of the most distinctive features is superposition and parallelism, where qubits can exist in multiple states simultaneously. This allows quantum algorithms to explore a vast number of solution paths in parallel, a capability that is especially valuable for accounting tasks such as portfolio valuation,

multi-period budgeting, and scenario analysis. In these domains, classical computing often struggles with combinatorial explosions as the number of variables or potential outcomes increases exponentially, whereas quantum computation can potentially evaluate multiple scenarios concurrently, enhancing speed and depth of analysis (Arute et al., 2019; IBM Quantum, 2023).

Another foundational concept is entanglement, which creates correlations between qubits that cannot be explained using classical logic. This property resonates with financial and accounting systems, where asset prices, cash flows, and risk exposures are highly interdependent. Entanglement enables quantum algorithms to capture these complex relationships more naturally, allowing for improved modeling of systemic risks, inter-account correlations, and dependencies across financial instruments. For instance, in multi-entity consolidation, intercompany balances, or derivative risk aggregation, quantum approaches could provide more accurate and computationally efficient solutions than traditional methods (Biamonte et al., 2021).

Quantum interference and probability amplification further contribute to the potential utility of quantum computing in accounting. Interference allows quantum algorithms to amplify the probability of correct outcomes while suppressing incorrect ones. In practical accounting applications, this mechanism could accelerate convergence in complex estimations such as fair value measurement, Expected Credit Loss (ECL) simulations, and stochastic financial forecasting. By directing computational resources toward the most relevant solutions, quantum interference enhances the precision and efficiency of calculations that underpin decision-making, reporting, and regulatory compliance (Cerezo et al., 2021).

## 2. Key Applications in Accounting and Finance

Quantum computing presents transformative potential for accounting and finance by addressing computationally intensive tasks that are challenging for classical systems. One prominent application is high-dimensional valuation and fair value measurement, which is critical under accounting standards such as IFRS 13. Valuing complex financial instruments, derivatives, and structured products often requires sophisticated models and simulations, particularly when markets are illiquid or observable inputs are limited. Quantum

algorithms, notably quantum Monte Carlo methods, can drastically reduce computation times, offering quadratic speedups compared to classical simulations. This enhancement improves both the efficiency and accuracy of fair value estimations, enabling more timely and precise reporting (Montanaro, 2015; Woerner & Egger, 2019).

Another significant application is in risk modeling and scenario analysis. Accounting and regulatory frameworks, including IFRS 9, require banks and financial institutions to assess credit risk, market risk, and liquidity risk under numerous stress scenarios. Quantum computing enables exploration of vastly larger scenario spaces, supporting stress-testing, provisioning, and capital planning with higher robustness. By leveraging quantum-enhanced optimization, accountants and risk managers can model complex interactions between risk factors and macroeconomic variables more effectively, leading to improved forecasting and resilience in financial planning (Bova et al., 2021).

Optimization of accounting processes and internal controls also benefits from quantum approaches. Core tasks such as cost allocation, transfer pricing, inventory management, and capital budgeting often involve combinatorial optimization problems, where classical heuristics may be slow or suboptimal. Quantum annealing and variational quantum algorithms provide more efficient pathways to optimal or near-optimal solutions, allowing organizations to achieve precise resource allocation, enhance internal control structures, and improve operational efficiency (D-Wave Systems, 2022).

## 3. Implications for Accounting Standards and Regulation

The adoption of quantum computing in accounting and finance introduces profound implications for standards and regulatory oversight, challenging traditional assumptions about measurement, transparency, and model governance. One key concern is measurement reliability and verifiability. Quantum algorithms can produce valuation outputs that are computationally infeasible to replicate on classical systems, raising questions about how auditors and regulators can assess the credibility and accuracy of financial statements. This necessitates the development of new verification approaches, including audit procedures that combine quantum simulations with classical cross-checks, documentation of algorithmic assumptions, and independent validation of input data (IASB, 2023).

Another significant implication relates to transparency and explainability. Quantum models are inherently complex, often relying on superposition, entanglement, and probabilistic interference to achieve computational speedups. While these properties enhance efficiency and scalability in tasks such as fair value measurement or risk simulation, they also challenge the accounting principle of understandability. Regulators and standard-setters may require enhanced disclosures that explain the nature of quantum models, their decision logic, and the extent to which outputs are interpretable by users of financial statements, balancing innovation with stakeholder comprehension (PwC, 2023).

Model risk and governance also become critical considerations. The use of quantum-enhanced valuation or risk models introduces new sources of operational and estimation risk, including sensitivity to qubit errors, algorithmic assumptions, and calibration limitations. Accounting standards may need to prescribe explicit governance frameworks for quantum model deployment, including documentation of assumptions, version control, sensitivity testing, and segregation of duties between model developers, finance teams, and auditors. Enhanced disclosure requirements around quantum-based models could become necessary to ensure that users understand the limitations, uncertainties, and potential impacts on reported figures (Montanaro, 2015; Woerner & Egger, 2019).

International standard-setters, including the IASB, along with global regulators, have begun to explore the implications of emerging computational technologies on financial reporting and assurance. While quantum computing adoption is still nascent, these bodies recognize that proactive guidance will be essential to maintain consistency, reliability, and comparability in financial statements. Future standards may incorporate guidance on when and how quantum-generated data can be used, the necessary audit evidence, and the disclosure of model assumptions and limitations. These initiatives reflect a broader trend toward integrating technological innovation into the regulatory framework without compromising the foundational principles of transparency, prudence, and accountability in financial reporting (IASB, 2023; PwC, 2023).

## 4. Cybersecurity and Cryptography Considerations

The advent of quantum computing introduces significant cybersecurity and cryptography considerations that directly impact accounting systems and financial reporting. Traditional cryptographic mechanisms, such as RSA and ECC (Elliptic Curve Cryptography), underpin the security of digital accounting records, online transaction authentication, and blockchain-based ledgers. However, sufficiently powerful quantum computers are theoretically capable of executing Shor's algorithm, which can efficiently factor large integers and solve discrete logarithms, effectively breaking these widely used public-key encryption schemes. This poses a systemic threat to the confidentiality, integrity, and authenticity of financial data, potentially exposing sensitive accounting information, digital signatures, and audit trails to malicious actors (NIST, 2022).

In response to this looming risk, the accounting and finance sectors must proactively adopt post-quantum cryptography (PQC). PQC encompasses encryption algorithms and digital signature schemes designed to resist quantum attacks, ensuring that financial records, regulatory filings, and blockchain transactions remain secure even in a post-quantum environment. The migration to PQC requires careful planning, as it involves updating software libraries, auditing cryptographic implementations, and ensuring interoperability with existing financial systems. For accounting professionals, this means not only understanding the technical implications of quantum-resistant cryptography but also integrating these measures into broader internal control and risk management frameworks.

Moreover, quantum-induced cybersecurity risks have implications for audit and compliance processes. Auditors will need to verify that post-quantum encryption standards are properly implemented and that accounting systems continue to maintain reliable data integrity. Organizations must document cryptographic transitions and maintain traceable audit trails to satisfy regulators and standard-setters, particularly in areas like digital reporting, XBRL filings, and electronic signature compliance. Cybersecurity governance in accounting systems will therefore become closely aligned with strategic technology planning, requiring collaboration between finance, IT, and risk management teams.

## C. Rise of Autonomous Banking and Self-Generating Reports

The rise of autonomous banking represents a transformative stage in the evolution of the financial industry, where banking operations, decision-making, and reporting processes are increasingly executed by intelligent systems with minimal human intervention. Driven by advances in artificial intelligence (AI), machine learning, robotic process automation (RPA), big data analytics, and cloud computing, autonomous banking shifts financial institutions from reactive, manual operations toward predictive, self-learning, and self-optimizing systems. Within this context, self-generating financial reports emerge as a natural extension enabling real-time, continuous, and standardized financial reporting that fundamentally reshapes accounting practice and governance (BIS, 2022; McKinsey, 2023).

### 1. Concept and Maturity Levels of Autonomous Banking

Autonomous banking represents a progressive evolution in financial services, encompassing a spectrum of maturity levels rather than a single, uniform state. At its foundational stage, assisted banking, automation primarily supports human decision-making by handling repetitive, rule-based tasks such as transaction processing, payment reconciliations, or routine reporting. These systems reduce operational errors, increase efficiency, and free staff to focus on higher-value tasks, yet human oversight remains central. As banks adopt more sophisticated technologies, they move into the augmented banking phase, where artificial intelligence (AI) and advanced analytics provide predictive insights and decision support. In this stage, AI can offer recommendations for credit approval, liquidity management, and risk assessment, enabling finance and accounting teams to make more informed and timely decisions. Although humans retain ultimate authority, decision-making becomes data-driven, anticipatory, and increasingly proactive.

The pinnacle of this evolution is fully autonomous banking, in which systems independently execute financial and operational decisions within predefined governance frameworks. At this level, autonomous platforms continuously monitor market conditions, customer behavior, and operational metrics, adjusting parameters and triggering actions in real time. For example, an autonomous credit

management system may adjust lending limits dynamically based on evolving credit risk profiles, while liquidity management modules automatically optimize cash positions across accounts and subsidiaries. Accounting systems are no longer passive record-keeping tools but are fully integrated with operational platforms, facilitating seamless data flow from transaction initiation to financial statement preparation. This integration reduces latency, enhances accuracy, and ensures that financial reporting reflects real-time economic activity (Accenture, 2022).

Maturity in autonomous banking also entails robust governance and control mechanisms. Even as systems act independently, accountability frameworks, risk thresholds, and audit trails are embedded to ensure compliance with regulatory standards and internal policies. Continuous monitoring, model validation, and exception management are critical to maintain trust and reliability in autonomous operations. Furthermore, autonomous banking leverages scalable cloud infrastructure, AI-driven analytics, and interconnected digital platforms to support rapid adaptation to market shifts, technological innovations, and evolving customer expectations.

## 2. Enabling Technologies Behind Autonomous Banking

The foundation of autonomous banking rests on several enabling technologies that collectively transform operational, risk, and accounting functions. Artificial intelligence (AI) and machine learning (ML) are central to this transformation, continuously learning from transactional, behavioral, and market data to optimize processes across banking operations. In the accounting domain, ML algorithms facilitate automated transaction classification, anomaly detection, and predictive provisioning in line with IFRS 9 standards, significantly reducing manual intervention and accelerating the preparation of financial statements. AI-driven models also enhance credit approval, fraud detection, and revenue recognition, enabling real-time decision-making and adaptive responses to emerging risks (Deloitte, 2023).

Complementing AI, Robotic Process Automation (RPA) and intelligent workflows automate repetitive, rule-based accounting tasks such as journal entries, reconciliations, and regulatory reporting. When integrated with AI forming Intelligent Process Automation RPA systems gain adaptive capabilities, allowing them to interpret

unstructured data, manage exceptions, and trigger self-correcting actions. This combination supports self-generating, near-real-time financial reports and operational dashboards, which are essential for the autonomous execution of banking functions while maintaining compliance and auditability. These intelligent workflows reduce errors, enhance processing speed, and free finance professionals to focus on strategic analysis and oversight.

Underlying these capabilities are real-time data architectures and cloud-native platforms, which provide the scalability, flexibility, and continuous processing required for autonomous banking. Data is ingested in real time from core banking systems, digital channels, and external APIs, creating a comprehensive and up-to-date view of financial and operational metrics. Cloud platforms enable high availability and elastic scalability, ensuring that the bank can dynamically handle transaction spikes, integrate new data sources, and generate timely financial reports as activities occur. This infrastructure allows both operational and accounting systems to interact seamlessly, supporting automated reconciliations, liquidity management, and regulatory reporting while preserving data integrity and audit trails (AWS, 2022).

## 3. Self-Generating Financial Reports: Mechanisms and Features

Self-generating financial reports represent a transformative shift in accounting practices, where integrated digital systems produce financial statements and related disclosures automatically, without requiring manual compilation. At the core of these systems is continuous accounting, which ensures that transactions are recorded, validated, and classified in real time. This real-time processing eliminates the traditional end-of-period bottlenecks, enabling finance teams to access up-to-date financial positions, performance metrics, and risk exposures at any moment. By maintaining an always-current view of the general ledger and subsidiary ledgers, banks and financial institutions can respond more quickly to operational and strategic challenges, while also improving the timeliness of regulatory reporting.

Another fundamental feature of self-generating reports is embedded rule-based and standards-compliant logic. Accounting rules aligned with IFRS, PSAK, and local regulatory frameworks are encoded directly into the system, ensuring consistent treatment of

transactions and uniform application of accounting principles across the organization. This approach reduces errors arising from manual journal entries, accelerates reconciliations, and facilitates auditability, as all system logic is documented and traceable. Moreover, these systems can accommodate updates to accounting standards automatically, supporting continuous compliance in dynamic regulatory environments.

In addition to numeric outputs, automated disclosures and narrative generation are increasingly incorporated through Natural Language Generation (NLG) tools. These tools translate financial data into explanatory notes, management commentary, variance analyses, and other textual disclosures. As a result, stakeholders—including management, regulators, and investors—receive comprehensive insights into financial performance, risk exposures, and operational trends without manual reporting effort. NLG-generated commentary can be tailored for different audiences, combining quantitative precision with qualitative explanations, enhancing clarity and decision-usefulness (PwC, 2023).

Collectively, self-generating financial reports transform accounting from a static, periodic function into a living, dynamic process. Financial statements are no longer end-of-month artifacts but continuously updated representations of an institution's financial health. This paradigm supports real-time performance monitoring, proactive risk management, and faster, data-driven decision-making. By integrating continuous accounting, embedded compliance logic, and automated narrative generation, self-generating reports exemplify the future of accounting in autonomous and digitally mature banking environments, improving efficiency, accuracy, and transparency.

## 4. Implications for Accounting Quality and Assurance

Autonomous reporting in digital and autonomous banking environments significantly impacts accounting quality and assurance, enhancing the reliability, relevance, and decision-usefulness of financial information. One of the primary benefits is timeliness: financial reports can be generated on demand, reflecting transactions and events as they occur rather than waiting for period-end closings. This capability allows management, investors, and regulators to make faster, more informed decisions, and supports proactive risk

management. In an environment where market conditions and operational dynamics change rapidly, the ability to access real-time financial insights is a major qualitative advantage (IAASB, 2023).

Another critical improvement is in accuracy and consistency. Automated validation rules, embedded accounting standards, and system-enforced transaction classifications reduce human errors, manual adjustments, and inconsistencies across reporting periods. Continuous accounting processes ensure that all entries are immediately reconciled against business rules, contracts, and regulatory requirements, thereby strengthening data integrity and reducing the likelihood of misstatements. These features collectively enhance the reliability of financial statements, a core qualitative characteristic emphasized in accounting frameworks such as the IASB Conceptual Framework.

Auditability also improves under autonomous reporting. Digital systems maintain immutable logs and comprehensive audit trails, allowing auditors to trace each reported figure back to its originating transaction or data source. Such transparency supports both internal and external assurance, enabling more efficient audits and greater confidence in reported outcomes. Auditors can leverage system extracts, automated reconciliations, and embedded validation workflows to perform risk-focused, near-real-time assessments of financial data (IAASB, 2023).

However, while autonomous reporting enhances quality, it introduces new risks and assurance challenges. Dependence on complex algorithms, machine learning models, and automated decision-making raises concerns about model risk, algorithmic bias, and the potential for system errors that could propagate through financial statements. Overreliance on automated judgments may diminish professional skepticism if human oversight is insufficient. Addressing these risks requires robust governance frameworks, including model validation, independent review, continuous monitoring, and clear accountability for outputs generated by digital systems. Effective control environments ensure that automation complements, rather than replaces, professional judgment in financial reporting.

## D. Future Skills Required for Banking Accountants

The rapid digital transformation of the banking industry fundamentally reshapes the competency profile of banking accountants. As banks adopt advanced technologies such as artificial intelligence, big data analytics, blockchain, cloud computing, and autonomous reporting systems, the role of accountants evolves from traditional record-keepers into strategic partners, technology stewards, and ethical guardians of financial information. Consequently, future banking accountants must develop a hybrid skill set that integrates accounting expertise, digital literacy, analytical capability, and professional judgment. International professional bodies and industry studies consistently emphasize that the sustainability of the accounting profession depends on its ability to adapt to these technological and organizational shifts (ACCA, 2023; IFAC, 2022; World Economic Forum, 2023).

### 1. Advanced Digital and Technological Literacy

In the evolving landscape of digital banking, accountants are increasingly required to demonstrate advanced digital and technological literacy to manage and oversee complex, technology-driven financial systems. Unlike traditional roles that focused primarily on manual bookkeeping and financial statement preparation, future banking accountants must be digitally fluent, enabling them to understand, evaluate, and supervise modern accounting infrastructures effectively. A fundamental competency is familiarity with core banking systems and cloud-based accounting platforms, which underpin real-time data architectures. This knowledge allows accountants to ensure that transaction data is accurately captured, classified, and integrated into financial reports without delay, supporting continuous accounting and timely decision-making (Deloitte, 2023).

Another critical area is artificial intelligence (AI) and machine learning (ML). Accountants must understand how these models operate, their underlying logic, and their limitations. For example, AI-driven credit provisioning, fraud detection, and financial forecasting rely on complex algorithms that may be subject to bias or produce unexplained outcomes. Professionals are expected to assess model outputs critically, perform validation checks, and identify anomalies,

thereby maintaining objectivity and accuracy in financial reporting. This extends beyond mere technical familiarity; accountants must bridge the gap between technology and financial standards, ensuring that AI outputs comply with IFRS/PSAK requirements.

Furthermore, basic knowledge of blockchain and distributed ledger technologies (DLT) is increasingly important. Blockchain systems provide immutable audit trails and facilitate the accounting of crypto-assets and tokenized instruments, which are becoming more prevalent in financial markets. Understanding how DLT affects transaction verification, record-keeping, and regulatory compliance allows accountants to oversee innovative asset classes while maintaining transparency and accountability.

**2. Data Analytics and Quantitative Skills**

In the context of digital banking, data analytics and quantitative skills have become indispensable for accountants, transforming the profession from traditional bookkeeping to a more strategic, insight-driven role. As financial institutions increasingly operate on vast volumes of transactional, behavioral, and market data, accountants must be capable of interpreting these datasets to support decision-making, risk management, and regulatory compliance. Key competencies include the ability to conduct descriptive, diagnostic, and predictive analytics, enabling professionals to summarize historical performance, identify the underlying causes of financial deviations, and forecast future outcomes with greater accuracy. For example, predictive analytics can inform credit risk modeling under IFRS 9, projecting expected credit losses by analyzing borrower behavior and macroeconomic indicators (McKinney et al., 2021).

Statistical reasoning is another core requirement. Accountants must apply statistical techniques to detect trends, anomalies, and risk patterns across large and complex datasets. This involves not only identifying outliers or unusual transactions that may indicate fraud or misstatements, but also evaluating correlations between operational metrics, market conditions, and financial results. Such analytical rigor strengthens internal controls, enhances provisioning accuracy, and supports robust scenario analysis for stress testing and capital planning. Quantitative skills also underpin valuation exercises under IFRS 13,

where fair value assessments of illiquid or complex instruments demand probabilistic modeling and sensitivity analysis (Marr, 2022).

Furthermore, data visualization and communication skills are critical for translating complex analytical results into actionable insights. Accountants must present financial information effectively to management, auditors, and regulators using dashboards, charts, and other visual tools. Clear visualization enhances transparency, supports strategic decision-making, and facilitates compliance with reporting obligations, particularly in environments that rely on real-time or near-real-time reporting.

### 3. Strategic and Business-Oriented Thinking

In the evolving landscape of digital banking, accountants are increasingly expected to adopt strategic and business-oriented thinking, moving beyond traditional compliance and bookkeeping functions toward roles that directly influence enterprise value creation. With automation and artificial intelligence handling routine transactional and reporting tasks, accountants can focus on providing insights that support strategic decision-making, guiding banks through complex digital transformations. This requires a deep understanding of modern banking business models, including fintech partnerships, embedded finance solutions, and Banking-as-a-Service (BaaS) platforms. By evaluating these models, accountants can assess not only their financial viability but also their potential to enhance customer engagement, operational efficiency, and long-term profitability (Kaplan & Norton, 2020).

A core aspect of strategic thinking involves investment appraisal and value creation analysis. Digital banking initiatives often require substantial upfront capital in technology platforms, cloud infrastructure, and data analytics capabilities. Accountants must be able to critically evaluate the expected return on these investments, incorporating both quantitative financial metrics and qualitative strategic considerations, such as scalability, ecosystem integration, and customer experience enhancements. Techniques such as Net Present Value (NPV), Internal Rate of Return (IRR), and real options analysis are increasingly applied in combination with scenario-based modeling to capture the flexibility and uncertainties inherent in digital projects (PwC, 2023).

Moreover, accountants must link financial performance metrics with broader strategic objectives. Traditional measures like Return on Assets (ROA) or Cost-to-Income Ratio (CIR) remain relevant, but they need to be contextualized alongside customer-centric KPIs such as Customer Lifetime Value (CLV), engagement ratios, and digital adoption rates. This integrated approach ensures that financial insights are not isolated from the bank's strategic goals, enabling management to make informed decisions about product development, channel optimization, and platform investments (Accenture, 2022).

**4. Risk Management and Regulatory Competence**

In the rapidly evolving domain of digital banking, accountants are increasingly required to develop advanced risk management and regulatory competence to navigate the complex landscape of financial, operational, and technological risks. Unlike traditional banking, where risks were largely centered on credit, liquidity, and interest rate exposures, digital banking introduces additional dimensions such as cybersecurity threats, operational disruptions in automated processes, AI-driven model risk, and reputational risks arising from customer data misuse. Accountants must therefore possess a comprehensive understanding of these multifaceted risks, enabling them to quantify potential impacts on financial statements, capital adequacy, and liquidity positions (BIS, 2022).

A key aspect of this competence involves the application of regulatory frameworks. Digital bankers must ensure adherence to accounting standards such as IFRS for provisioning, fair value measurement, and financial disclosures, while also integrating Basel III/IV capital and liquidity requirements into risk assessments and reporting processes. Furthermore, compliance extends to anti-money laundering (AML) and counter-terrorist financing (CFT) regulations, data privacy rules, and ESG reporting standards, which increasingly influence banking operations and strategic decisions. Proficiency in these frameworks allows accountants to align internal control systems and automated reporting mechanisms with evolving legal obligations, ensuring both regulatory compliance and stakeholder confidence (IASB, 2023).

In addition, digital banking relies heavily on AI and machine learning for risk assessment, credit scoring, and predictive analytics,

creating the need for accountants to monitor model risk and maintain explainability. Since algorithmic outputs can influence provisioning, loan-loss estimates, and capital planning, accountants must verify assumptions, validate results, and provide clear documentation for audit and regulatory purposes. This emphasizes the dynamic role of accountants as both risk controllers and strategic advisors, translating regulatory requirements into system design, automated workflows, and governance structures that mitigate operational and financial exposures.

# CHAPTER XI
# CASE STUDIES AND BEST PRACTICES

Case Studies and Best Practices provide practical insights into how banking accounting concepts and digital technologies are implemented in real-world settings. By examining leading banks' experiences with AI-based accounting, comparing conventional and neo bank financial systems, and analyzing FinTech collaboration models, this chapter bridges theory and practice in digital banking accounting. These case studies highlight success factors, common challenges, and strategic lessons, demonstrating how effective governance, technology integration, and human capital development can transform accounting into a value-creating and strategic function within the modern banking ecosystem.

## A. Implementation of AI-Based Accounting at Leading Banks

The implementation of artificial intelligence (AI) in accounting has become a defining feature of leading banks as they respond to increasing transaction volumes, complex regulatory requirements, and the demand for faster, more accurate financial information. AI-based accounting systems integrate machine learning (ML), natural language processing (NLP), robotic process automation (RPA), and advanced analytics to transform traditional accounting processes that were historically manual, periodic, and retrospective. Rather than replacing professional accountants, AI reshapes their role by automating routine tasks, enhancing analytical depth, and supporting forward-looking decision making. According to Deloitte (2023) and McKinsey (2023), banks that successfully implement AI in finance and accounting functions achieve measurable improvements in efficiency, accuracy, and strategic insight.

## 1. Key Drivers of AI Adoption in Banking Accounting

The adoption of artificial intelligence (AI) in banking accounting is driven by several structural and strategic factors that make it an attractive solution for modern financial management. One of the primary drivers is the high transaction intensity inherent in contemporary banking operations. Banks process millions of transactions daily across payments, lending, trading, and treasury activities. Traditional manual accounting processes and controls struggle to scale effectively under such volumes, often resulting in delays, errors, and operational bottlenecks. AI technologies, through automation and intelligent data processing, enable banks to handle large-scale transactional data efficiently, ensuring accuracy and timeliness in financial reporting.

Another key driver is regulatory and compliance pressure. Banks must comply with complex standards, including IFRS 9 for expected credit losses, Basel III capital adequacy rules, and enhanced supervisory reporting requirements. These frameworks demand sophisticated estimation methods, detailed documentation, and comprehensive audit trails. AI systems facilitate regulatory compliance by automating calculations, generating consistent records, and providing continuous monitoring of accounting processes, thereby reducing the risk of human error and enhancing audit readiness (Basel Committee, 2023).

The demand for real-time financial insight also motivates AI adoption. Digital banking models rely on dynamic performance metrics and operational dashboards to make rapid strategic and operational decisions. Monthly or quarterly reporting cycles are insufficient for this environment. AI-driven accounting systems can process, analyze, and present financial data in near real-time, supporting decision-makers with timely insights into liquidity, risk exposure, and profitability across business lines (PwC, 2023). This capability enables banks to respond proactively to market shifts, customer behavior changes, and emerging risks.

## 2. Core AI Use Cases in Accounting Functions

Artificial intelligence (AI) has increasingly become integral to modern banking accounting, enabling automation, precision, and enhanced risk management across core accounting functions. One of

the most prevalent use cases is transaction processing and classification. Machine learning algorithms are trained on historical transaction data to automatically classify payments, receipts, and other financial events into appropriate general ledger accounts. In addition, natural language processing (NLP) techniques allow AI systems to interpret unstructured transaction descriptions, such as invoice texts or payment notes, facilitating accurate categorization of expenses, revenues, and fees. This ensures consistency in accounting treatment and reduces manual intervention, enhancing overall efficiency (Kokina & Davenport, 2017).

Another key application is reconciliation and close automation. Traditional reconciliation processes are time-consuming and prone to errors, particularly when data is incomplete or inconsistent. AI-driven matching algorithms can automatically reconcile bank statements, intercompany balances, and suspense accounts, even in the presence of irregularities. By significantly reducing unmatched items and discrepancies, AI supports faster and more reliable month-end closing cycles, paving the way for continuous accounting practices where financial positions are updated in near real-time (Vasarhelyi et al., 2015).

AI also contributes through journal entry recommendations. Systems analyze historical posting trends, real-time transactional data, and recurring accounting patterns to propose routine entries such as accruals, amortizations, and allocations. While human accountants retain final approval responsibility, these AI-generated recommendations streamline preparation, reduce errors, and improve consistency across accounting periods.

A critical function enhanced by AI is anomaly detection and fraud prevention. Unsupervised learning models identify irregular patterns in financial data, such as duplicate payments, unusual transaction timing, or deviations from standard behavior. By flagging these anomalies, AI strengthens internal controls, ensuring the integrity of accounting records and mitigating the risk of fraud (Deloitte, 2023).

## 3. Implementation Architecture and Operating Model

The implementation of AI-based accounting in leading banks relies on a carefully structured architecture that integrates technology, data governance, and human oversight. At the foundation is the data

layer, which comprises centralized data lakes and governed data warehouses. These platforms consolidate transactional, customer, and operational data from multiple sources, ensuring accuracy, completeness, and consistency. High-quality data is essential for reliable AI outputs, as errors or inconsistencies at this level can propagate through automated processes and compromise financial reporting (PwC, 2023).

Built atop this foundation is the automation layer, primarily leveraging Robotic Process Automation (RPA) to execute deterministic, repetitive tasks. Activities such as data extraction, journal posting, reconciliations, and report generation are handled by RPA bots, significantly reducing manual workload and minimizing human error. By automating these routine functions, banks can accelerate the accounting cycle and focus human resources on higher-value tasks requiring judgment and oversight.

The next tier is the AI analytics layer, where machine learning (ML) and natural language processing (NLP) models perform sophisticated analyses. ML algorithms classify transactions, predict accounting estimates such as provisions or credit losses, and identify anomalies that may indicate errors or fraud. NLP enables the automated interpretation of unstructured data, including invoice descriptions or customer communications, to support consistent accounting treatments. This layer enhances the timeliness and precision of accounting outputs, while also providing predictive insights that inform financial decision-making (PwC, 2023).

## 4. Governance, Auditability, and Ethical Considerations

Governance, auditability, and ethical considerations form the cornerstone of AI-based accounting in modern banking. Given that accounting outputs directly impact financial statements, shareholder reporting, and regulatory disclosures, banks prioritize the establishment of robust governance frameworks. These frameworks typically include comprehensive model risk management processes, encompassing model validation, thorough documentation, and ongoing performance monitoring to ensure that AI systems operate reliably and produce accurate results. Explainability is a central concern: banks must be able to demonstrate that AI-driven judgments, such as transaction classification, provisioning estimates, or anomaly detection, can be

clearly understood and justified to auditors and regulators. This transparency is critical for maintaining trust in automated accounting outputs and satisfying supervisory expectations regarding model governance and accountability (European Central Bank, 2023).

Auditability is equally vital. AI-based systems generate complex outputs that, if left unchecked, could undermine the traceability and verifiability of financial data. Leading banks implement end-to-end audit trails, logging all automated and human-in-the-loop interventions. These immutable records allow auditors to trace every figure back to its source transaction, supporting the reliability and integrity of financial statements. Workflow controls, exception management, and human oversight further enhance audit readiness, ensuring that any discrepancies or unusual outputs are promptly identified and resolved. This approach transforms AI from a black-box tool into a transparent, controlled element of the accounting function.

Ethical considerations also underpin AI adoption. Banks must proactively mitigate bias, ensuring that machine learning models do not produce skewed outcomes that could affect provisioning, revenue recognition, or risk assessments. Data privacy is another critical concern; sensitive customer and transaction information must be protected from unauthorized access or misuse. Ethical governance requires clear accountability, with explicit ownership of decisions, robust review processes, and adherence to established professional accounting standards and codes of conduct. This ensures that technology supports, rather than replaces, responsible human judgment in financial reporting (IFAC, 2022).

## B. Comparison: Conventional vs Neo Bank Financial Systems

The rapid growth of digital technology has fundamentally reshaped the banking landscape, giving rise to neo banks (also known as digital-only or challenger banks) that operate without physical branches and rely entirely on technology-driven financial systems. In contrast, conventional banks evolved from branch-based, paper-intensive operations and later incorporated digital layers on top of legacy infrastructures. This section compares conventional and neo bank financial systems from an accounting, operational, technological, and regulatory perspective, highlighting how differences in system

architecture and business models influence financial reporting, cost structures, risk management, and strategic decision making.

### 1. System Architecture and Core Platforms

The system architecture and core platforms of banks fundamentally shape their accounting capabilities and operational efficiency. Conventional banks typically operate on legacy core banking systems developed decades ago, which were primarily designed for batch processing, periodic reconciliation, and product-centric accounting. These traditional back-end systems often remain fragmented and inflexible, despite modernization efforts at the front-end channels, such as mobile and online banking. As a result, conventional banks face challenges in achieving real-time financial reporting, integrated ledgers, and seamless data flows, which can slow decision-making, limit automation, and complicate regulatory compliance (Accenture, 2023). These limitations necessitate extensive manual intervention, workarounds, and reconciliation procedures, which in turn increase operational risk and cost.

In contrast, neo banks and other digital-native financial institutions are built on cloud-native, modular architectures that prioritize flexibility, scalability, and real-time data integration. These platforms are designed from the ground up to unify transaction processing, accounting, and reporting. Accounting processes are embedded directly into transaction flows, enabling continuous posting, instant reconciliation, and dynamic financial statements. By leveraging API-based connectivity, these systems can seamlessly integrate with third-party services, fintech partners, and internal operational platforms, facilitating a fully interconnected digital ecosystem. This architecture not only enhances operational efficiency but also supports innovative business models, such as Banking-as-a-Service (BaaS), embedded finance, and platform-based revenue streams (Bunea et al., 2020).

Moreover, the modular design of neo bank platforms allows rapid deployment of new products, flexible configuration of accounting rules, and easier updates to comply with evolving standards like IFRS or local regulatory requirements. Real-time data architectures, combined with cloud scalability, ensure high availability, robust performance under peak transaction volumes, and improved disaster

recovery capabilities. These capabilities enable finance teams to focus on strategic analysis and decision-making rather than manual reconciliations or legacy system maintenance.

**2. Accounting Processes and Financial Reporting**

Accounting processes and financial reporting in banking differ significantly between conventional banks and neo banks, reflecting the evolution from batch-oriented operations to real-time, technology-driven models. In conventional banks, accounting is typically periodic and labor-intensive, relying on end-of-day or end-of-month closing cycles. Transactions recorded throughout the period are accumulated in multiple sub-ledgers, requiring extensive reconciliations and manual adjustments before finalizing financial statements. This approach often delays insight into the institution's financial position, limits agility in decision-making, and increases operational risk due to human error or inconsistencies across ledgers (PwC, 2023). Compliance and regulatory reporting, while accurate, may be time-consuming and reactive rather than proactive, with auditors dependent on snapshot data rather than continuous transaction flows.

Neo banks, by contrast, have reimagined accounting as a continuous, integrated process embedded directly within transaction systems. In these institutions, each transaction is recorded, validated, and reflected in the general ledger in near real time, enabling financial statements that dynamically represent the bank's current position. Automated controls, such as AI-driven transaction classification and anomaly detection, reduce the need for manual interventions, shorten closing cycles, and enhance the accuracy and consistency of financial records. Integrated audit trails and immutable logs allow auditors and regulators to trace every posting from source transactions to final reports, strengthening governance and transparency (Deloitte, 2023).

Furthermore, neo banks leverage advanced analytics and AI tools to enhance financial reporting. Natural Language Generation (NLG) technologies can automatically produce management commentary, variance analysis, and regulatory disclosures, converting raw data into actionable insights. This automation supports faster decision-making for management and timely communication with stakeholders, transforming financial reporting from a static, periodic activity into a continuous, value-added function. Continuous

accounting also enables scenario analysis, real-time performance monitoring, and proactive risk assessment, aligning financial operations with strategic objectives and customer-centric business models.

### 3. Cost Structure and Operational Efficiency

Cost structure and operational efficiency represent key differentiators between conventional banks and neo banks, particularly in the context of accounting and financial operations. Conventional banks typically operate under high fixed-cost models driven by extensive branch networks, legacy IT systems, and large operational workforces. Maintaining multiple physical locations requires significant expenditures on rent, utilities, security, and staffing, while aging core banking and accounting systems demand continuous maintenance, upgrades, and integration efforts. These structural costs contribute to higher cost-to-income ratios, limiting the bank's ability to reallocate resources toward strategic initiatives or technology investments. Additionally, manual or semi-automated accounting processes increase reliance on human labor for reconciliations, journal entries, and reporting, which not only adds costs but also introduces potential for errors and delays (McKinsey, 2023).

Neo banks, in contrast, benefit from a digital-native cost advantage. Operating without physical branches dramatically reduces overhead, while cloud-based core banking and accounting platforms eliminate the need for extensive on-premise IT infrastructure. Automation and AI-driven accounting processes such as real-time transaction classification, anomaly detection, and continuous reconciliation allow neo banks to maintain lean finance functions with minimal staff, achieving higher accuracy and speed in reporting. Robotic Process Automation (RPA) and intelligent workflow tools further optimize routine tasks, freeing human accountants to focus on strategic decision support, risk assessment, and regulatory compliance (BIS, 2022).

The combination of digital distribution, scalable IT infrastructure, and automation enables neo banks to achieve operational efficiency at scale. Cost structures become variable rather than fixed, allowing banks to expand transaction volumes, onboard new customers, or introduce new products without proportionally increasing accounting or operational resources. This scalability not only improves profitability

but also provides strategic flexibility in a rapidly evolving financial market. Moreover, reduced process complexity and integrated systems enhance transparency and auditability, lowering operational risk while supporting faster regulatory reporting.

### 4. Risk Management and Internal Controls

Risk management and internal controls are fundamental aspects distinguishing conventional banks from neo banks, particularly in the context of accounting and financial operations. Conventional banks typically rely on ex post control mechanisms, where reconciliations, audits, and variance analyses are conducted after transactions have been executed. While these approaches provide oversight and verification, they inherently create lagged risk identification, meaning exposures or errors may only be detected after they have already impacted financial statements or operational processes. This reactive nature can delay corrective actions, increase operational risk, and necessitate extensive manual intervention to ensure compliance and accuracy (PwC, 2023). Traditional controls often depend on multiple sub-ledgers, batch processing, and periodic review cycles, which can limit transparency and slow down the detection of unusual transactions or compliance breaches.

In contrast, neo banks adopt a proactive and embedded risk control model, leveraging technology to integrate risk management directly into daily accounting and transaction processes. Real-time transaction validation, automated limit checks, and AI-driven anomaly detection are implemented at the point of transaction execution. These mechanisms allow banks to identify irregularities, policy violations, or potential fraud immediately, rather than retrospectively. For example, machine learning models can flag abnormal payment patterns, unusual customer behavior, or discrepancies in journal entries, enabling finance teams to respond swiftly. Continuous monitoring ensures that both operational and financial risks are assessed on an ongoing basis, supporting continuous assurance and more reliable financial reporting (Vasarhelyi et al., 2015).

Moreover, neo banks integrate internal control functions with IT systems and operational workflows, creating a unified control environment that enhances transparency and accountability. Automated workflows enforce segregation of duties, approval hierarchies, and

audit trails, reducing the reliance on human intervention while strengthening compliance with regulatory standards. Cloud-based platforms and real-time data architectures further support risk oversight by providing comprehensive visibility across transactions, customer accounts, and operational activities. This architecture also enables scenario simulations and stress testing, allowing management to anticipate potential exposures and adjust controls dynamically.

## C. FinTech Collaboration Models in Accounting Processes

The increasing complexity of digital banking and financial reporting has encouraged banks to collaborate closely with FinTech firms to enhance the efficiency, accuracy, and strategic value of accounting processes. Rather than developing all technological capabilities internally, banks leverage FinTech innovation to modernize accounting systems, automate compliance, and integrate advanced analytics. These collaborations reshape traditional accounting functions into technology-enabled ecosystems, where data, platforms, and expertise are shared across institutional boundaries (Arner, Barberis, & Buckley, 2017).

### 1. Rationale for Bank–FinTech Collaboration in Accounting

Collaboration between banks and FinTech firms in accounting is increasingly driven by both structural imperatives and strategic opportunities. One of the primary rationales is the growing **regulatory** complexity and demand for real-time, transparent financial reporting. Banks face heightened scrutiny under frameworks such as IFRS 9, Basel III/IV, and local supervisory standards, which require accurate, timely, and auditable accounting data. Meeting these requirements with legacy systems alone can be challenging, as conventional IT infrastructures often lack the agility and automation needed to process large transaction volumes and generate continuous reports. FinTech firms, in contrast, offer specialized technologies ranging from artificial intelligence (AI) for automated classification and anomaly detection, robotic process automation (RPA) for repetitive journal entries, to blockchain-based ledgers for immutable audit trails which can be integrated into banking accounting systems to enhance compliance and efficiency (Deloitte, 2023).

Another significant driver is the speed of innovation. Digital transformation in banking is rapid, and internal development cycles can be slow and resource-intensive. Partnering with FinTechs allows banks to access cutting-edge solutions without incurring the full costs and risks of in-house development. For instance, deploying AI-driven provisioning tools or real-time financial dashboards can be implemented faster through collaboration, enabling banks to respond to market changes, customer expectations, and regulatory updates more effectively. Moreover, these partnerships facilitate scalability, as cloud-native FinTech solutions can handle large transaction volumes and complex accounting processes without proportional increases in staffing or IT overhead.

Strategically, collaboration also supports risk management and operational resilience. By leveraging FinTech expertise, banks can implement robust internal controls, continuous reconciliation, and real-time monitoring of accounting data. This reduces the likelihood of errors, fraud, or compliance breaches, enhancing overall financial integrity. Additionally, working with external technology providers allows banks to experiment with new accounting innovations—such as predictive analytics for credit provisioning or automated financial reporting—without fully committing internal resources, thereby mitigating implementation risk.

## 2. Key Collaboration Models

Collaboration between banks and FinTech firms can take several distinct forms, each offering unique advantages for accounting processes and financial reporting. The Technology Vendor Model represents the most common approach, where FinTechs provide specialized software and platforms for accounting tasks such as automated reconciliations, AI-driven financial close, or regulatory reporting solutions. In this model, banks retain full control over accounting policies and decisions, while the FinTech supplies technical infrastructure, maintenance, and updates. The accounting impact is significant: journal entries and reconciliations become automated, financial closing cycles accelerate, and data accuracy and auditability improve. This approach is favored by large, established banks because it minimizes implementation risk while maintaining a clear governance structure (PwC, 2023).

A more integrated approach is the Platform and API-Based Integration Model, which leverages open banking and standardized APIs to connect bank accounting systems directly with FinTech platforms. This allows transactional data to flow seamlessly into accounting engines in real time, enabling continuous posting, validation, and reporting. As a result, banks achieve continuous accounting, near-instantaneous financial dashboards, reduced manual data transfers, and improved interoperability between sub-ledgers and general ledgers. The Bank for International Settlements (BIS, 2023) emphasizes that API-based collaboration enhances the transparency and resilience of accounting infrastructures, particularly in highly digitalized banking environments.

The Co-Creation and Joint Innovation Model goes beyond standard software adoption, involving banks and FinTechs jointly designing accounting solutions within innovation labs or sandbox environments. Both parties share intellectual property, risks, and rewards. This approach is especially useful for complex problems, enabling the development of customized AI models for financial forecasting, tailored blockchain-based audit trails, and advanced scenario analysis tools. McKinsey (2023) notes that joint innovation accelerates the creation of sophisticated solutions that cannot be achieved with off-the-shelf technologies.

Embedded FinTech Services integrate FinTech accounting functionalities directly into bank operations, covering automated tax calculations, ESG reporting, or regulatory disclosures. This model transforms the accounting function into a fully integrated digital service, enabling end-to-end automation from transaction initiation to reporting, improved compliance with IFRS and local standards, and scalable operations. It is particularly prevalent in neo banks and digital-first institutions (OECD, 2022).

## D. Lessons Learned & Strategic Recommendations

The analysis of AI-based accounting implementation, comparisons between conventional and neo bank financial systems, and FinTech collaboration models provides valuable insights into how banking accounting is evolving in the digital era. These case studies demonstrate that technology adoption alone is insufficient; success

depends on strategic alignment, governance quality, human capital readiness, and regulatory integration. This section synthesizes the key lessons learned from best practices and offers strategic recommendations to guide banks, regulators, and accounting professionals in navigating digital transformation effectively.

## 1. Key Lessons Learned from Digital Banking Accounting Practice

Case studies of digital banking accounting practices reveal several critical lessons that can guide the strategic implementation of technology in financial reporting and control. One of the foremost insights is that technology serves as an enabler, not a substitute for governance. Advanced tools such as AI, cloud computing, and blockchain significantly enhance the efficiency and accuracy of accounting processes only when paired with robust governance frameworks. Leading banks that successfully implemented AI-driven accounting systems embedded clear accountability structures, auditability, and ethical standards directly into system design. In contrast, institutions that treated technology purely as a technical upgrade frequently faced data quality challenges, model risk, and regulatory scrutiny. This underscores that digital accounting initiatives must operate within transparent policies, internal controls, and continuous oversight to maintain compliance and stakeholder trust (Basel Committee, 2023; Deloitte, 2023).

Another key lesson is that real-time accounting markedly improves decision-making quality. Neo banks and digitally advanced incumbents demonstrate that continuous accounting where transactions are recorded, validated, and consolidated in near-real time enables management to identify profitability trends, liquidity pressures, and risk exposures faster than traditional periodic reporting cycles. This shift transforms accounting from a backward-looking function into a forward-looking strategic tool, emphasizing the timeliness of information as equally important to its accuracy (Bunea et al., 2020).

The importance of collaboration over isolation also emerges clearly. Banks partnering with FinTech firms benefit from faster innovation cycles, lower development costs, and access to specialized expertise in AI, RegTech, and advanced analytics. By contrast, fully in-house development efforts often encounter longer implementation

timelines, higher operational risk, and limited scalability. These experiences highlight that ecosystem-based collaboration is more effective than isolated innovation, particularly when addressing complex accounting and regulatory challenges (Arner et al., 2017; McKinsey, 2023).

Equally critical is the role of human capital. Across case studies, the success of digital accounting initiatives heavily depends on the skills, judgment, and adaptability of accounting professionals. Banks investing in upskilling their workforce combining core accounting expertise with data analytics, technology literacy, and ethical awareness were better able to harness the full potential of digital systems. Digital transformation, therefore, is as much a human endeavor as a technological one (IFAC, 2022).

## 2. Strategic Recommendations for Digital Banking Accounting

Strategic recommendations for digital banking accounting focus on aligning technological innovation with robust governance, human capital development, and long-term value creation. One of the foremost strategies is to adopt a comprehensive accounting transformation roadmap. Leading banks are encouraged to design multi-year plans that integrate accounting transformation into the broader digital banking strategy, defining target architectures, data standards, governance protocols, and performance metrics. This approach ensures that accounting evolves from a traditional compliance function into a strategic partner capable of supporting business growth, risk management, and operational efficiency (Deloitte, 2023).

A second recommendation involves implementing hybrid accounting architectures. Rather than attempting wholesale replacement of legacy systems, banks should leverage modular, cloud-based platforms that interface with existing core systems through APIs and standardized data layers. Hybrid models reduce implementation risk, allow phased adoption, and preserve continuity of operations while enabling automation, real-time posting, and continuous reconciliation (PwC, 2023).

With increasing reliance on AI and machine learning in accounting processes—such as expected credit loss (ECL) estimation, fraud detection, and predictive analytics—it is critical to strengthen model risk management and explainability. Banks should establish

dedicated governance frameworks that encompass model validation, bias detection, audit documentation, and ethical oversight. Explainable AI ensures that auditors, regulators, and management can understand decision logic, while reducing operational and compliance risks (European Central Bank, 2023).

Human capital development is equally important. Banks are advised to invest in digital accounting talent and cultivate a culture of continuous learning. Accountants must combine professional judgment with digital fluency, including data analytics, AI oversight, and scenario-based financial planning. Cross-functional collaboration between finance, IT, and risk management enhances the strategic value of accounting outputs and promotes effective technology adoption (IFAC, 2022).

Strategic FinTech partnerships are another critical lever. Collaborations should be based on long-term strategic alignment, data governance standards, and scalability rather than short-term cost savings. Banks that engage in co-creation or embedded service models benefit from faster innovation cycles, enhanced interoperability, and access to advanced AI and RegTech solutions (McKinsey, 2023).

# BIBLIOGRAPHY


ACCA. (2023). Future Skills and the Accountant of Tomorrow: finance transformation. ACCA research report.

Accenture. (2024). Banking Top 10 trends: payments reinvention & embedded finance. Accenture.

Ahmad, M. & Hassan, R. (2024). Historical Approaches to Banking Accounting. Journal of Financial History.

AICPA. (2023). Audit considerations for AI-driven finance processes. AICPA practice aid.

Arner, D. W., Barberis, J., & Buckley, R. P. (2017). FinTech, RegTech and the Reconceptualization of Financial Regulation. Northwestern Journal of International Law & Business.

Arner, D. W., Barberis, J., & Buckley, R. P. (2022). The evolution of FinTech and RegTech.

Association of Certified Fraud Examiners (ACFE). (2022). Report to the Nations — fraud in digital payment systems. ACFE.

Baker, H. K., & Filbeck, G. (2021). Portfolio Theory & Management — applications for bank asset-liability optimization. Oxford University Press.

Bank for International Settlements (BIS). (2023). Central banking and digital finance: trends and implications. BIS.

Bank Indonesia (BI). (2023). Payment system and e-money regulations update. Bank Indonesia.

Bank Negara Malaysia (BNM). (2023). Open Finance and API frameworks — supervisory guidance. BNM publications.

Basel Committee on Banking Supervision. (2023). Principles for model governance and model risk management. BIS.

Basel Committee on Banking Supervision. (2023). Principles for operational resilience.

Basel Committee on Banking Supervision. (2023). Principles for the Sound Management of Operational and Cyber Risk. BIS.

Basel Committee. (2021). Operational resilience — sound practices. BIS.

Basel Committee. (2022). Principles for effective risk data aggregation and risk reporting (BCBS239 refresh). BIS.

BCG. (2024). Digital banking transformation and capital allocation: best practices. Boston Consulting Group.

BIS – Bank for International Settlements (2024). Digitalisation and the Prudential Framework.
BIS Committee on Payments and Market Infrastructures (CPMI). (2023). Real-time gross settlement and instant payments implications. CPMI.
BIS. (2023). Climate-related financial risks: central bank perspective. BIS.
Capgemini. (2024). World Retail Banking Report: AI & automation in banking operations. Capgemini.
COSO. (2022). Internal Control — Integrated Framework: Technology supplement. COSO.
Costa, D. (2025). Competition or cooperation? Bank-FinTech relationships and integration models. Journal of Financial Intermediation.
Damodaran, A. (2023). Valuation: digital asset valuations and platform businesses. Stern School of Business working paper.
Deloitte. (2020). Finance transformation and continuous close in banking: a how-to guide. Deloitte.
Deloitte. (2022). Robotic Process Automation in finance: a practical guide. Deloitte.
Deloitte. (2023). Digital finance: transformation, continuous accounting and automation. Deloitte Insights.
Deloitte. (2024). Internal Control 4.0 and continuous assurance in financial services. Deloitte Insights.
D-Wave Systems. (2022). Quantum annealing use cases for finance and optimization. D-Wave white paper.
Eccles, R. G., & Klimenko, S. (2021). The investor revolution.
Eccles, R. G., Klimenko, S., & Ioannou, I. (2022). The impact of ESG on financial performance.
Emerging Markets Review (2023). FinTech and bank competition — empirical studies. Elsevier.
European Banking Authority (EBA). (2023). Guidelines on ICT and security risk management for banks. EBA.
European Banking Authority. (2022). Digital Operational Resilience Act (DORA) — overview for banks. EBA.
European Central Bank (ECB). (2023). On AI in finance: governance and supervisory expectations. ECB Occasional Paper.
EY. (2023). IFRS 9 in practice: using alternative data and machine learning for ECL. EY.
FATF. (2023). International standards on combating money laundering.

Financial Action Task Force (FATF). (2023). Guidance on digital identity and AML/CFT. FATF.
Financial Conduct Authority (FCA). (2022). RegTech and supervisory technology (SupTech) developments. FCA.
Financial Stability Board (FSB). (2023). Regulatory and supervisory issues relating to crypto-assets and stablecoins. FSB.
Forrester. (2023). The Future of Banking Analytics and AI — vendor landscape and buyer recommendations. Forrester Research.
Gartner. (2023). Market Guide for Banking Core Systems and Cloud-led Core transformation. Gartner Research.
Global Reporting Initiative (GRI). (2022). GRI Standards & sustainability reporting guidance for banks. GRI.
Hong Kong Monetary Authority (HKMA). (2022). AI in Financial Services — supervisory expectations and guidelines. HKMA.
HSBC / IBM research announcement (2024–2025). Quantum computing pilots in trading and optimization (corporate reports).
IAASB. (2023). IAASB Guidance on Auditing Automated and Continuous Reporting Systems. IAASB.
IASB. (2022). Disclosure requirements for climate-related risks and expected accounting impacts. IASB discussion paper.
IBM Institute for Business Value. (2023). AI and trust in finance: algorithms, governance and outcomes. IBM.
IFAC. (2023). Ethics and technology guidance for professional accountants. IFAC.
IFRS Foundation (2023). IFRS 9 Financial Instruments: Guidance and Basis for Conclusions.
IFRS Foundation (2024). IFRS Digital Reporting Taxonomy & Digital Asset Considerations.
IFRS Foundation. (2023). IFRS Sustainability Disclosure Standards (IFRS S1 & S2). IFRS Foundation.
Institute of Chartered Accountants in England and Wales (ICAEW). (2023). AI, data and the future of accounting: professional guidance. ICAEW.
Institute of Internal Auditors (IIA). (2023). Continuous auditing in the digital age. IIA Global.
International Accounting Standards Board (IASB). (2023). IFRS 9 — Financial Instruments: Implementation and Practice. IASB.
International Association of Deposit Insurers (IADI). (2023). Digital banking and deposit insurance implications. IADI.

International Federation of Accountants (IFAC). (2022). Future of Finance: skills and competencies for accountants. IFAC.
International Journal of Accounting Information Systems — special issue (2023). Digital transformation in accounting: banking applications. Academic special issue.
International Monetary Fund (IMF). (2023). Digital money and financial stability: policy approaches. IMF Policy Paper.
International Organization of Securities Commissions (IOSCO). (2023). Crypto asset regulation overview. IOSCO.
ISO. (2021). ISO/IEC 27001: Information Security Management — implications for accounting systems. ISO.
Januszewski, A. (2025). Impact of Digital Transformation on Accounting Profession.
Jorion, P. (2021). Financial Risk Manager Handbook (7th ed.). Wiley.
Journal of Banking & Finance (2022–2024 issues). Selected articles on digital finance, platform banking and risk. Elsevier.
Journal of Financial Stability (2022–2024). Papers on operational resilience, cyber risk and digital payments. Elsevier.
Kaplan, R. S., & Norton, D. P. (2020). Strategy Maps and Balanced Scorecards for digital organizations. HBR Press.
Kogan, B., & Bunea, S. (2020). Customer-level profitability and unit economics in digital banking. Financial Analysts Journal.
KPMG. (2022). Fair value in the age of digital assets — IFRS 13 considerations. KPMG IFRS insights.
KPMG. (2023). ECL modelling and governance in digital banks. KPMG.
KPMG. (2024). Cyber risk management for banks: governance and reporting. KPMG.
Marr, B. (2021). Artificial Intelligence in Practice: case studies from finance and banking. Wiley.
Marr, B. (2022). Data-driven strategy and analytics for financial services. Kogan Page.
McKinsey & Company. (2023). The state of digital banking and profitability in 2023–2024. McKinsey Global Banking.
McKinsey. (2022). Banking's digital future: platformization and ecosystem winners. McKinsey Global Institute.
McKinsey. (2024). Money for Nothing? — Monetizing banking platforms and BaaS. McKinsey & Company.
Monetary Authority of Singapore (MAS). (2023). FinTech regulatory updates and API-led Open Banking frameworks. MAS.

Montanaro, A. (2015). Quantum algorithms: an overview. npj Quantum Information.
NIST. (2022). Post-Quantum Cryptography Standardization — NIST roadmap and guidelines. NIST.
Noor, A. S. (2024). The role of accounting digital transformation in reducing costs and impact on performance.
Noor, A.S. (2024). Accounting Digital Transformation and Performance. WEFB.
O'Halloran, P. (2024). Continuous Auditing in the Digital Age. Accounting Innovations Review.
OECD. (2021). Regulatory sandboxes and innovation facilitators in finance. OECD publishing.
OECD. (2022). Sustainable finance and banking: policy approaches and implementation. OECD Publishing.
OECD. (2023). AI in finance: ethical principles and governance. OECD AI Policy Observatory.
OECD. (2023). Corporate governance in the digital age.
Otoritas Jasa Keuangan (OJK). (2023). POJK on Digital Banking and Fintech: regulatory updates. OJK.
Porter, M., & Heppelmann, J. (2022). How Smart, Connected Products Are Transforming Competition. Harvard Business Review (relevant updates).
Preskill, J. (2018). Quantum Computing in the NISQ era and beyond. Quantum, 2, 79.
PSAK Board (Ikatan Akuntan Indonesia). (2023). PSAK convergence updates and guidance (various pronouncements). Ikatan Akuntan Indonesia.
PwC. (2020). Finance function of the future: automation and analytics. PwC Global.
PwC. (2021). E-wallets and digital payment systems: accounting and tax implications. PwC Global.
PwC. (2022). Continuous Close: Accounting Automation in Financial Services. PwC.
PwC. (2022). Crypto-asset accounting: getting ready for regulation and IFRS/PSAK implications. PwC.
PwC. (2023). AI and automation in banking finance: governance and implementation guide. PwC.
PwC. (2023). Blockchain and distributed ledgers in accounting and audit: use cases and assurance. PwC.

PwC. (2024). AI in accounting — governance, explainability and audit readiness. PwC.
PwC. (2024). Digital ESG reporting: practical approaches for banks. PwC.
Schipper, K. & Vincent, L. (2024). Financial Reporting Standards in Global Banking.
Sector press & market announcements (2023–2025): Selected corporate whitepapers and pilot reports from large banks (J.P. Morgan, HSBC, Citi, Bank of America), cloud vendors (AWS, Microsoft Azure), quantum vendors (IBM, D-Wave), and leading RegTech providers.
Stewart, G. (2021). EVA and Financial Performance Measurement in the Digital Era. Journal of Corporate Finance.
Taskforce on Nature-related Financial Disclosures (TNFD). (2023). Disclosure guidance and pilot resources. TNFD.
TCFD (Task Force on Climate-related Financial Disclosures). (2017; updated guidance 2021–2023). Recommendations and implementation guidance. TCFD.
United Nations Environment Programme Finance Initiative (UNEP FI). (2022). Principles for Responsible Banking and climate risk integration. UNEP FI.
V. B. (2021). Machine Learning for Credit Risk Modelling — Principles & Practices. Journal of Credit Risk.
Vasarhelyi, M. A., Kogan, A., & Tuttle, B. M. (2015). Big Data in Accounting: Continuous Auditing and Continuous Monitoring. Accounting Horizons, 29(2), 335–349.
Woerner, S., & Egger, D. J. (2019). Quantum risk analysis. IBM Research.
World Bank. (2022). Digital Financial Services: inclusion, identity and regulation. World Bank report.
World Economic Forum. (2022). Responsible Use of Technology in Financial Services — principles and case studies. WEF.
World Economic Forum. (2023). Future of Financial and Monetary Systems: digital finance, quantum readiness. WEF.

# GLOSARRY

| | |
|---|---|
| **Accounting** | Is the systematic process of recording, measuring, and communicating financial information to support economic decision-making. |
| **Accuracy** | Refers to the degree to which financial information is free from errors and faithfully represents transactions. |
| **Analytics** | Involves the use of data analysis techniques to support financial evaluation, forecasting, and decision-making in banking. |
| **Assets** | Are economic resources controlled by a bank that are expected to provide future financial benefits. |
| **Audit** | Is an independent examination of financial records to assess accuracy, reliability, and compliance with accounting standards. |
| **Automation** | Is the use of technology to perform accounting and banking processes with minimal human intervention to improve efficiency and accuracy. |
| **Banking** | Refers to financial activities conducted by institutions that accept deposits, provide credit, and offer payment services to the public. |
| **Blockchain** | Is a decentralized digital ledger technology that records transactions securely and transparently across multiple systems. |
| **Capital** | Refers to funds invested in or retained by a bank to support operations and absorb potential losses. |
| **Compliance** | Refers to adherence to applicable laws, regulations, and accounting standards governing banking operations. |
| **Cybersecurity** | Is the protection of digital accounting and banking systems from unauthorized access, attacks, and data breaches. |

| | |
|---|---|
| **Data** | Refers to raw financial and operational information processed through digital banking and accounting systems. |
| **Digitalization** | Is the adoption of digital technologies to transform traditional banking and accounting processes into electronic-based systems. |
| **Equity** | Is the residual interest in a bank's assets after deducting its liabilities. |
| **Fintech** | Represents technological innovations that enhance or automate financial services and accounting functions within the banking sector. |
| **Governance** | Is the framework of rules, practices, and processes used to direct and control banking institutions. |
| **Ledger** | Is a structured record, whether physical or digital, that systematically stores financial transactions of a banking institution. |
| **Liabilities** | Represent financial obligations of a bank arising from past transactions that must be settled in the future. |
| **Liquidity** | Is the ability of a bank to meet short-term financial obligations efficiently using available resources. |
| **Reconciliation** | Is the process of matching accounting records with actual financial data to ensure consistency and accuracy. |
| **Regulation** | Consists of formal rules established by authorities to ensure stability, transparency, and accountability in the banking system. |
| **Reporting** | Is the process of preparing and presenting financial information to stakeholders in accordance with accounting standards and regulations. |
| **Risk** | Represents the possibility of financial loss arising from uncertainties in banking operations and digital systems. |
| **Solvency** | Reflects a bank's capacity to meet its long-term obligations and sustain financial stability. |
| **Transparency** | Is the clarity and openness of financial information that enables stakeholders to understand a bank's financial condition. |

# INDEX

# BIOGRAPHY OF THE AUTHOR

**Dr. Jaime Soares, Lic-Eco., MBA (Advanced)., M.AP**

Dr. Jaime Soares, Lic-Eco., MBA (Advanced)., M.AP, was born in Same, Rotutu, on 19 May 1977. He is the son of Joaquim Soares (late Father) from Rotutu, Same, East-Timor and Esperança da Conceição Sarmento from Sloi, Aileu, East-Timor. He earned his Bachelor of Economics (Lic. Eco.) specializing in an accounting from Universidade da Paz, Dili, East-Timor. He subsequently pursued advanced studies, obtaining a Master of Business Administration (Advanced) from Flinders University, Adelaide, South Australia, as well as a Master of Public Administration from Universidade da Paz, Dili, East-Timor. Dr. Soares later completed his Doctoral degree in Economic Sciences from University of 17 August 1945 Surabaya (UNTAG Surabaya, Indonesia). Currently, he is active as a banking practitioner and also serves as a lecturer at the Faculty of Economics, Universidade da Paz, Dili, East-Timor, with a teaching focus on Accounting, Management, Banking and Enterpreneurship.

**Dr. Duarte Borges Loe, Lic. CSH., MA., M.Sc.**

Dr. Duarte Borges Loe, Lic. CSH., MA., MSc was born in Cailaco on January 24, 1983. He is an intellectual and military professional with an extensive and international educational background.

He completed his bachelor's and first master's degrees in International Relations at Universidade da Paz (UNPAZ), Timor-Leste. He then pursued a master's degree in Innovation and Strategic Management at Salve Regina University, Rhode Island, United States. In addition, he completed another master's degree in Military and Defence Studies at the Australia War College. He earned his doctoral degree (Ph.D.) in Economics from Universitas 17 Agustus 1945 Surabaya, Indonesia.

Currently, Dr. Duarte serves as Director of the office for coordination and international cooperation policy at Ministry of Defence while also actively serving as a naval officer in Timor-Leste. His expertise and experience bridge the fields of military affairs, diplomacy, and national development strategy.

He is widely recognized for his contributions to national defense policy development and regional strategic studies. Besides being active in writing and speaking at various academic and defense forums, he is also committed to promoting stronger integration between academics and practitioners in the fields of security and defense.

He can be reached at his office address at Palacio do Governo, Dili, Timor-Leste, or via email at duarteloe7@gmail.com

**Dr. Cristino Gusmão, L.Agr.Ec., M.Ec.Dev.**

Dr. Cristino Gusmão, L.Agr.Ec., M.Ec.Dev., is a civil servant and a lecturer in the Management Study Program at the Faculty of Economics, Universidade da Paz. He was born in Railan, Atabae, on October 10, 1965, and currently lives in Dili. He completed his primary and secondary education in Atabae and Maliana, earned his Bachelor's degree from the National University of Timor-Leste, and obtained his Master's degree from Universitas Gadjah Mada in 2009–2010. He pursued his Doctoral Program in Business Economics at Universitas 17 Agustus 1945 Surabaya from 2021 to 2025.

**Dr. Parso, S.E., M.Si., BKP.**

Dr. Parso earned his Bachelor of Economics (S.E.) and Master of Science in Accounting (M.Si.) from Universitas Trisakti, Jakarta, and subsequently obtained his Doctoral degree (Ph.D.) in Economics from Universitas 17 Agustus 1945 Surabaya. He has expertise in accounting and taxation, and has been serving as a full-time lecturer at Universitas MH. Thamrin, Jakarta, since 2010. In addition to his academic career, Dr. Parso holds an official license as a tax consultant issued by the Ministry of Finance. He also has professional experience as an audit staff member and tax consultant, and is frequently invited as a resource person and speaker in various seminars and professional training programs.

**Dr. Emi Lestari, S.E., M.M., CFP.**

Dr. Emi Lestari earned her Bachelor of Economics (S.E.) from Universitas Kristen Duta Wacana Yogyakarta, her Master of Management (M.M.) from STIE Mahardhika Surabaya, and her Doctoral degree (Dr.) from Universitas 17 Agustus 1945 Surabaya. She specializes in financial management and focuses her research on topics within this field. She is also a Certified Financial Planner (CFP). Currently, Dr. Emi Lestari serves as a lecturer at the Faculty of Business, Universitas Universal (UVERS) Batam, where she is dedicated to teaching, research, and community engagement.

# BANKING ACCOUNTING

## IN THE DIGITAL ERA

MODERN CONCEPTS AND APPLICATIONS

Banking Accounting in the Digital Era: Modern Concepts and Applications presents a comprehensive exploration of how digital transformation is reshaping accounting practices within the banking sector. This book examines the integration of traditional banking accounting principles with modern digital technologies, including core banking systems, financial technology (fintech), automation, data analytics, and real-time financial reporting. It highlights the evolving role of accounting in supporting transparency, regulatory compliance, risk management, and strategic decision-making in an increasingly complex and technology-driven financial environment. Through a balanced combination of conceptual discussion and practical application, the book addresses current challenges such as cybersecurity, digital transactions, electronic records, and regulatory adaptation. Designed for students, academics, banking professionals, and policymakers, this book serves as a valuable reference for understanding contemporary banking accounting practices and developing the competencies required to operate effectively in the digital era while maintaining accuracy, accountability, and financial integrity.

PT MEDIA PENERBIT INDONESIA

mediapenerbitindonesia.com
+6281362150605
Penerbit Idn
@pt.mediapenerbitidn

ISBN 978-634-7457-88-2