

الجمهورية الجزائرية الديمقراطية الشعبية

Republic of Algeria

People's Democratic Republic

Ministry of Higher Education and
Scientific Research

National Higher School of
Management – Koléa



وزارة التعليم العالي والبحث العلمي

المدرسة الوطنية العليا للمناجمنت

Dissertation Submitted

In Partial Fulfilment of the Requirements for a Master's Degree in

"E-Government"

Theme:

Digital Transformation and its Role in Information Governance, Digital Identity
and Digital Sovereignty Enhancement in the Algerian Banking Sector
– A Case Study of Crédit Populaire d'Algérie (CPA) –

Prepared by:

Messaoudi Asma

Supervised by:

Dr. Horri amar

Academic Year: 2025 / 2026

Acknowledgements

In the name of Allah, the Most Gracious, the Most Merciful.

I extend my deepest gratitude and appreciation to my dear parents, my mother **Fatima Chichoun** and my father **Aissa**, whose unlimited support and sincere prayers have been the most important reason for completing this work.

To my brothers **Ahmed Mahdi** and **Monsef**, and my sisters **Malak** and **Rahef**, thank you for your patience and continuous encouragement. I also extend special thanks to my friends who stood by me and supported me at every stage.

My sincere thanks and appreciation go to my supervisor, **Dr. Horri Ammar**, for his valuable guidance and precise feedback, which greatly contributed to improving this research.

I also extend my thanks to the management of **Crédit Populaire d'Algérie (CPA) – Batna branch**, and especially to the person in charge of my internship from the human resources department, for facilitating my field work and for their kind cooperation. I also thank all the employees who contributed to the success of this work.

Messaoudi Asma.

Abstract

This study analyzes the digital transformation strategy within the Algerian banking sector by integrating four interdependent concepts: information governance, digital identity, digital accountability, and digital sovereignty. A quantitative-led approach with qualitative support was adopted, based on a case study of the CPA Batna branch, combining semi-structured interviews (Legal, Credit, and HR departments),

Administered among 12 employees, and a documentary analysis. The results show that the bank possesses operational digital tools, but their integration into a formalized governance framework remains incomplete: the digital strategy is not institutionalized transversally, authentication relies primarily on passwords, technical traceability exists without being accessible to non-IT stakeholders, and the legal department remains structurally excluded from decisions relating to data sovereignty. The study provides an empirical diagnosis of the CPA Batna branch, highly relevant to the Algerian context, along with operational suggestions for both the bank and the regulatory authorities.

Keywords: Digital transformation, IT governance, digital identity, digital accountability, digital sovereignty, CPA.

الملخص

تتناول هذه الدراسة استراتيجية التحول الرقمي في القطاع المصرفي الجزائري من خلال دمج أربعة مفاهيم مترابطة: حوكمة المعلومات، الهوية الرقمية، المساواة الرقمية، والسيادة الرقمية. وقد اعتمد منهج كمي ذو دعم نوعي، استناداً إلى دراسة حالة لوكالة القرض الشعبي الجزائري (CPA) بباتنة، حيث جُمعت البيانات عبر مقابلات نصف موجهة (مع أقسام الشؤون القانونية، والقروض، والموارد البشرية)، واستبيان وزع على 12 موظفاً، بالإضافة إلى تحليل وثائقي أظهرت النتائج أن البنك يمتلك أدوات رقمية تشغيلية، لكن إدماجها ضمن إطار حوكمة رسمي لا يزال غير مكتمل؛ إذ أن الاستراتيجية الرقمية ليست مُمأسسة بشكل عرضي، وعمليات التحقق من الهوية تعتمد أساساً على كلمات المرور، كما أن التتبع التقني موجود بالفعل لكنه غير متاح للأطراف المعنية غير المتخصصة في المعلوماتية، ويظل القسم القانوني مُستبعداً هيكلياً من القرارات المتعلقة بسيادة البيانات. تُقدم الدراسة تشخيصاً ميدانياً لوكالة القرض الشعبي الجزائري فرع باتنة، يكتسي أهمية بالغة في السياق الجزائري، بالإضافة إلى مقترحات عملياتية موجهة للبنك والسلطات التنظيمية.

كلمات مفتاحية: تحول رقمي، حوكمة، هوية رقمية، مساواة، سيادة رقمية، CPA.

Résumé

Cette étude analyse la stratégie de transformation numérique dans le secteur bancaire algérien en intégrant quatre concepts interdépendants : la gouvernance de l'information, l'identité numérique, la responsabilisation numérique et la souveraineté numérique. Une approche quantitative avec volet qualitatif a été adoptée, fondée sur une étude de cas approfondie de l'agence CPA de Batna, combinant des entretiens semi-directifs (départements juridique, crédit et RH), un questionnaire administré à 12 employés, et une analyse documentaire. Les résultats montrent que la banque dispose d'outils numériques opérationnels, mais que leur intégration dans un cadre de gouvernance formalisé reste incomplète : la stratégie numérique n'est pas institutionnalisée de manière transversale, l'authentification repose essentiellement sur des mots de passe, la traçabilité technique existe sans être accessible aux parties prenantes non-informatiques, et le département juridique demeure structurellement écarté des décisions relatives à la souveraineté des données. L'étude fournit un diagnostic empirique de l'agence CPA Batna, extrêmement pertinent dans le contexte algérien, ainsi que des suggestions opérationnelles pour la banque et les autorités de régulation..

Mots clés : Transformation numérique, gouvernance, identité numérique, responsabilisation, souveraineté numérique, CPA.

List of Figures

- **Figure 1:** Defining Governance and Management in COBIT 2019. Adapted from "COBIT 2019 Framework: Governance and Management Objectives" **by ISACA, 2019**..... 29
- **Figure 2:** Governance Objectives in COBIT 2019 – Value Creation. Adapted from "COBIT 2019 Framework: Governance and Management Objectives" **by ISACA, 2019**..... 30
- **Figure 3:** The ITIL 4 Service Value System (SVS). Adapted from "ITIL 4 Service Value System" **Axelos/PeopleCert (2019). ITIL 4 Foundation**..... 31
- **Figure 4:** The ITIL 4 Service Value Chain. Adapted from "Service Value Chain Diagram" **Axelos/PeopleCert (2019). ITIL 4 Foundation**. 31
- **Figure 5:** Key Dimensions of Digital Accountability. Adapted from "Objectives" **Pearson et al. (2012). Accountability as a Way Forward for Privacy Protection in the Cloud**..... 34
- **Figure 6:** Compliance Flowchart for Personal Data Protection in Algerian Banks. **Based on CMS Law (2025) and DataGuidance (2025)**..... 40
- **Figure 7:** [Data Sovereignty Cloud Market Forecast \(2026-2030\). Data Sovereignty Cloud Market" by Research and Markets, 2026 \(https://www.researchandmarkets.com/reports/6191053\)](https://www.researchandmarkets.com/reports/6191053). 42
- **Figure 8:** Top Benefits of Technology in Compliance (**Source: PwC Global Compliance Survey 2025, via Secureframe**). 43
- **Figure 9:** Integrated Conceptual Framework — Digital Transformation, Information Governance, Digital Identity, Accountability, and Digital Sovereignty. 49
- **Figure 10:** Data Warehouse 57

- Figure 11: Distribution of respondents by department.	68
- Figure 12: Distribution of respondents by years of experience	68
- Figure 13 :word cloud from NVIVO.	109
- Figure 14: Organizational Structure of the Bank.	110

List of tables

- Table 1: the difference between IT governance & information governance	24
- Table 2: the 5 th levels of digital sovereignty. (Shoker, 2022)	36
- Table 3: key technologies of supporting digital identity.....	46
- Table 4: means and standard deviations.....	69
- Table 5: ANOVA by years of experience	70
- Table 6: CODING MATRIX	71

List of Abbreviations

- 2FA– Two-Factor Authentication. Security mechanism requiring two verification factors (password + token or biometric).
- AD – Active Directory. Microsoft directory service for managing identities and access rights.
- AI – Artificial Intelligence. Simulation of human intelligence in machines.
- AML – Anti-Money Laundering. Laws and procedures to prevent disguised conversion of illegal funds.
- ANOVA – Analysis of Variance. Statistical test to compare means across several groups.
- BCP – Business Continuity Plan. Plan to ensure recovery of services and data after incidents.
- CAGR – Compound Annual Growth Rate. The rate needed an investment to grow from its beginning to its ending balance.
- COBIT – Control Objectives for Information and Related Technologies. IT governance framework by ISACA.
- CPA – Crédit Populaire d’Algérie. Algerian public bank (case study institution).
- DSI – Direction des Systèmes d’Information. Information Systems Directorate of the bank (French acronym).
- EPE – Entreprise Publique Économique. State-owned economic enterprise (CPA’s legal status).
- FATF – Financial Action Task Force. Intergovernmental body combating money laundering.
- GDPR – General Data Protection Regulation. EU regulation on data protection and privacy.
- IDS – Intrusion Detection System. System that monitors network traffic for suspicious activity.
- IGF – Information Governance Framework. Framework by Faria, Maçada & Kumar (2013) with three dimensions: People, Policies, Technology.
- ISACA – Information Systems Audit and Control Association. Professional association for IT governance and audit.
- IT – Information Technology. Use of computers, storage, and networks to create, process, and exchange data.

- ITIL – Information Technology Infrastructure Library. Best-practice framework for IT service management.
- KYC – Know Your Customer. Process of verifying client identity to prevent fraud.
- PDG – Président-Directeur Général. Chairman and Chief Executive Officer (French acronym).
- SOC – Security Operations Centre. Centralized unit that monitors and responds to security incidents.
- SWIFT – Society for Worldwide Interbank Financial Telecommunication. Global network for financial messaging between banks.
- V07 – Delta V07. An older version of the Delta core banking system.
- V11 – Delta Supra V11. Advanced, omnichannel version of the Delta banking system.
- VPN – Virtual Private Network. Secure connection over a public network, enabling remote access.
- Wazuh – Wazuh (platform). Open-source security platform for log analysis and threat detection.

Table of Contents

General introduction	1
Chapter I:	
Literature Review and Conceptual Framework.....	7
Section One: Literature Review.....	9
Subsection one: the four key concepts of the study.	9
Subsection two: Research Gaps analysis.	14
Section two: Conceptual Framework.	16
Subsection one: Theoretical Foundations	18
Subsection two: Digital Accountability, Sovereignty, and Identity in the Banking Environment.....	33
Chapter II:	
Case Study Presentation (CPA) and the Methodological Framework.....	50
Section One: Introduction to “Crédit Populaire d’Algérie (CPA)”.....	51
Subsection One: History, Organizational Structure, and Information Systems of CPA.	51
Subsection two: Digitalization Tools and Electronic Banking Services at CPA.....	57
Section Two: Methodological Framework.	58
Subsection One: Research Variables and Epistemological Foundations.....	59
Subsection Two: Data Collection, Analysis, and Quality Assurance Procedures.....	61
Chapter III:	
Results Presentation, Discussion, and Assessment.....	66
Section one: Presentation of Field Study Results.	67
Subsection one: Quantitative Analysis Results.....	67
Subsection two: Qualitative Results and Technical Background.....	71
Section two: Discussion of Results.	75
Subsection one: Answering Sub-Questions and Testing Hypotheses.....	75
Subsection two: Explaining Unexpected Findings, Limitations and Suggestions.....	80
General conclusion	86
References	Error! Bookmark not defined.
Appendices	100

General introduction

The Fourth Industrial Revolution has fundamentally restructured Algeria's banking system, surpassing mere technical upgrades and compelling a strategic shift toward comprehensive digitalization at the very core of its administrative and regulatory frameworks. In this context, the transition to comprehensive digitalization is no longer optional but an inevitable necessity for survival and competitiveness.

Within the Algerian banking sector, the challenge is no longer restricted to technical features or service interfaces. Instead, it has evolved into a delicate balance between establishing an advanced information system governance on one hand, and ensuring the integrity of digital identity and data management on the other.

From this perspective, innovation is not only measured by technological adoption, but by a bank's ability to ensure digital sovereignty, transparency in governance, and the fostering of digital accountability. Ultimately, the relationship between a bank and its customers is no longer built solely on service delivery, but on sovereign trust and digital resilience in managing automated decision-making and digital identities.

In this context, the Algerian banking system is not isolated from these changes. **Crédit Populaire d'Algérie (CPA)** is seeking to adopt and develop digital transformation strategies that integrate governance, identity management, accountability, and sovereignty. However, a successful digital transformation strategy requires more than technology adoption. It requires a coherent strategic framework that aligns IT governance with business objectives, ensures data sovereignty, and builds customer trust through digital identity and accountability. This study examines how such a strategy can be formulated and implemented in the Algerian banking context, with a focus on CPA.

Study Context

The global banking sector has witnessed an unprecedented digital transformation, requiring the development of advanced frameworks for data governance, digital identity, accountability, and digital sovereignty. However, banks in developing countries, including Algeria, face major challenges in keeping pace with this transformation due to weak infrastructure, a lack of clear regulatory frameworks, and limited specialized human competencies.

In Algeria, Law No. 18-07 on personal data protection was enacted in 2018. It became enforceable in practice after the establishment of the National Authority for the Protection of Personal Data (ANPDP) in 2023 and its subsequent amendment by Law No. 25-11. Despite this legislative progress, the Bank of Algeria has not yet issued any detailed regulations regarding the storage of banking data on cloud servers, data localization requirements, or mechanisms for responding to foreign authorities' requests to access customer data. This regulatory ambiguity places Algerian banks in a state of legal uncertainty and limits their ability to adopt secure and sustainable digital transformation strategies.

Complementing this, the Bank of Algeria issued Instruction No. 02-25 of March 2025, which specifies the licensing conditions for digital banks, further indicating a gradual move toward regulatory clarity (Banque d'Algérie, 2025). Furthermore, Algerian public banks suffer from outdated and fragmented information systems, a lack of written data governance policies, limited adoption of advanced digital identity technologies, and a weak culture of digital accountability and transparency. These issues necessitate studying the reality of digital transformation in these banks and assessing their responsiveness to governance, accountability, and digital sovereignty requirements in the absence of clear regulatory guidance.

The importance of this study lies in two levels:

Academically (Scientific): The study contributes to filling a knowledge gap in the Arab and international literature by providing a theoretical framework that integrates four interrelated concepts rarely examined together in a banking context: information governance, digital identity, digital accountability, and digital sovereignty. It also provides an applied methodology for a case study of an Algerian public bank, thereby enriching the literature on digital transformation in developing economies.

Practically (Applied): The study benefits decision-makers in Algerian public banks (particularly CPA) by providing diagnostic tools and actionable suggestions to enhance data governance and achieve digital accountability. It also draws the attention of monetary and regulatory authorities (the Bank of Algeria, ANPDP) to existing legal gaps and provides practical arguments for the necessity of issuing clear implementing regulations on cloud computing and data localization.

Research problem

Consequently, and based on the interplay between digitalization ambitions and governance framework, this study aims to address the following central question: **How can Algerian banks formulate and implement a digital transformation strategy that integrates IT governance, digital identity management, digital accountability, and digital sovereignty? And what are the key strategic, technical, and organizational challenges hindering the development of such a strategy? – A case study of Crédit Populaire d'Algérie (CPA).**

Research Sub-question

1. What are the main strategic components of a digital transformation strategy in banking, and how can IT governance, digital identity,

accountability, and sovereignty be integrated into a coherent strategic framework?

2. How can a strategic framework of data governance and digital accountability enhance sovereign decision-making in Algerian banks amid digital transformation?
3. What is the current state of digital governance at **Crédit Populaire d'Algerie** (CPA)-Batna branch, and what are the actual organizational and technical hurdles to achieving sovereign and accountability?

Research hypotheses

- **H1:** An integrated IT governance framework enhances the reliability of digital identities and safeguards information assets within the banking environment.
- **H2:** Effective data governance and accountability mechanisms are fundamental to ensure digital transparency in automated decision-making processes.
- **H3:** Achieving full digital sovereignty at the CPA- Batna branch is primarily hindered by technical and organizational challenges related to data localization and digital safeguards.

In the context of a quantitative-led study, these hypotheses function as analytical propositions tested through both descriptive statistics and qualitative triangulation. They serve to focus data collection and guide thematic analysis, and are assessed through the convergence of qualitative and quantitative evidence.

Significance of the study

- Scientific importance:

This study addresses a relatively recent topic that brings together information systems governance, digital identity, and the concepts of sovereignty and accountability. These areas are still developing in academic literature, especially at the local level, which makes this research an attempt to contribute to this field of knowledge.

- Practical importance:

The practical value of this study lies in providing an analytical view of the state of information systems at CPA Bank (Batna branch), helping to highlight strengths and areas for improvement, as well as offering general suggestions that may support efforts to enhance digital governance and manage digital transformation in a more secure and organized way.

Research objectives

This research aims to achieve a set of interconnected objectives:

- **Conceptual grounding:** to build a comprehensive theoretical framework that clarifies the relationship between information systems governance, digital identity, and sovereignty within the banking environment.
- **Field assessment:** to evaluate the governance mechanisms applied at CPA Bank (Batna branch) and examine how well they respond to the requirements of accountability and transparency.
- **Gap analysis:** to identify the technical and organizational challenges that may hinder the full adoption of data governance and digital accountability mechanisms.
- **Practical suggestions:** to propose actionable measures that contribute to strengthening digital safeguards and reinforcing national sovereignty over financial and banking data.

Methodology of the study

This study adopts a descriptive and analytical approach based on a quantitative-led design with qualitative support. A quantitative approach was primarily adopted, supplemented by qualitative methods to deepen and validate the findings given the small sample size. The research strategy is a single in-depth case study of the CPA Batna branch.

To achieve the research objectives, the study relies on two main aspects: a theoretical part and a practical part. In the theoretical part, a number of recent references and studies related to IT governance, digital identity, and digital sovereignty were reviewed.

As for the practical part, a field study was conducted at the CPA Batna branch using multiple data collection tools: semi-structured interviews (3 interviews: legal, credit, human resources departments), a questionnaire (12 employees – used only for descriptive purposes due to the small sample), documentary analysis of internal reports, and participant observation during an internship period (29 March – 29 April 2026). Quantitative data were analysed using SPSS (descriptive statistics, Cronbach's alpha, ANOVA), while qualitative data were analysed using thematic analysis (Braun & Clarke, 2006) supported by NVivo software.

Structure of the Dissertation

This dissertation is structured into three chapters. The first chapter presents the theoretical framework and literature review. The second chapter details the research methodology and variables. The third chapter presents the descriptive results followed by their discussion and analysis. The dissertation ends with a general conclusion.

Chapter I:

Literature Review and Conceptual Framework.

In recent decades, the banking sector has undergone a profound transformation, moving from traditional branch-based models to integrated digital ecosystems that rely entirely on technology (Naimi-Sadigh et al., 2021; Munira, 2025). This transformation is no longer merely a response to passing trends; it has become a necessity for banks to remain competitive and survive, especially with the emergence of FinTech companies and the changing expectations of customers who demand instant, personalized, and easy-to-use services (Diener & Špaček, 2021; Widharto et al., 2020).

In this context, information systems governance plays a key role in managing technology investments and aligning them with business strategy. Parallel to this, concepts such as digital identity, digital accountability, and digital sovereignty have emerged as essential pillars for building secure and transparent banking relationships (Khattak et al., 2023; Al-Rashdi, Dick & Storey, 2017; Shoker, 2022). For Algerian banks, the challenge is particularly acute due to the absence of clear regulations from the Bank of Algeria regarding cloud data localization (DataGuidance, 2025; Radio Algérienne, 2024), creating a gap between documented security policies and enforceable legal sovereignty.

Despite the competitive advantages offered by digital transformation, banks face significant difficulties in integrating these technologies, particularly regarding infrastructure, regulatory compliance, and change management, especially in developing economies such as Algeria (Mohan, 2016; Diener & Špaček, 2021).

This chapter is divided into two sections. The first section reviews the literature on IT governance, digital identity, digital accountability, and digital sovereignty. The second section presents the legal framework for personal data

protection in Algeria, including Law No. 18-07 and a comparative analysis with the GDPR.

Section One: Literature Review.

This section reviews the existing academic literature on the four key concepts of this study: digital transformation in banking, information governance, digital identity and accountability, and digital sovereignty. Each subsection synthesises recent findings from peer-reviewed journals, identifies the main research gaps, and explains how the present case study of CPA Batna contributes to filling these gaps.

Subsection one: the four key concepts of the study.

1. Digital transformation

- Bughrara et al. (2025) conducted a systematic literature review of 287 articles on digital transformation strategies in commercial banks. They proposed a comprehensive multilevel framework distinguishing between macro strategies (digital-only banks, FinTech partnerships), meso strategies (agile structures, automation), and micro strategies (value co-creation, security, digital inclusion). The framework connects digital transformation to general-purpose technology and dynamic capabilities theories. However, the study remains entirely theoretical; it does not test the framework in a real-world banking environment, particularly in a developing country with weak infrastructure and ambiguous regulations. This gap is addressed by the present study, which provides the first field-based application of such strategies in an Algerian public bank (CPA).

- Obaid (2025) conducted a PRISMA-guided systematic review of 20 empirical studies (2015-2025) on digital transformation in retail banking. The review found that AI-enabled controls and API-mediated partnerships

are consistently associated with higher digital maturity, but only when supported by robust model-risk governance and third-party management. Nevertheless, the study focuses exclusively on developed markets; local case studies in the Algerian context are almost absent. The present study fills this gap by examining how an Algerian public bank implements – or fails to implement – those governance conditions.

- Three recent Algerian studies offer useful context but leave important questions unanswered. Taleb, Slimani & Bennouna (2025) used multiple linear regression (2010-2023) to evaluate the impact of digitalisation on Algerian banking performance. They found that digital banking services processed by the ATCI contribute to profitability. However, their quantitative approach does not examine internal governance mechanisms, digital identity practices, or accountability structures. Khaoui (2025) conducted a case study of digital transformation at the National Bank of Algeria (BNA) and concluded that the bank has made significant progress in implementing digital technology. Yet, the study focuses on service quality, not on governance frameworks, digital identity, or accountability, leaving internal governance unexamined. Khelalfa (2025) assessed the impact of AI-driven digital transformation on the Algerian economy (2015-2024) and found significant legislative progress (Law No. 23-09) but also structural challenges: weak banking localisation of digitisation and a sharp increase in cybersecurity incidents. Critically, the study operates at the macroeconomic level and does not capture bank-level governance practices.

Taken together, these studies demonstrate a clear gap: no existing research has examined the simultaneous integration of information governance, digital identity, accountability, and digital sovereignty within a single Algerian public bank. The present case study of CPA Batna directly addresses this gap by providing a fine-grained, field-based diagnosis of all four dimensions.

2. Information and IT Governance in Banking

- Faria, Maçada & Kumar (2013) remains the most influential study on information governance in banking. Based on research across thirteen banks in Brazil, the United States, and Hong Kong, they proposed the Information Governance Framework (IGF) comprising three dimensions (People, Policies, Technology) and twenty factors, validated with senior executives. Nevertheless, the IGF has never been applied or tested in a developing-country banking sector, particularly in North Africa. Moreover, it has never been connected to the concepts of digital sovereignty, digital identity, or digital accountability. This study fills that gap by applying the IGF diagnostically at the CPA Batna branch and linking it to the other three concepts.

- Simuni, G., & Atla, A. (2023) discuss data governance in cloud data warehouses and big data environments, emphasising data lineage, access control, and compliance monitoring. However, these technical frameworks focus on data management, not on strategic governance of digital identity, accountability, or sovereignty. More importantly, they assume a cloud-native environment, whereas CPA operates with legacy systems and no clear cloud strategy. The present study addresses this gap by examining governance in a low-resource, non-cloud environment, showing that governance begins with written policies and procedures before any technological upgrade.

3. Digital Identity and Digital Accountability

- Khattak et al. (2023) studied digital transformation and bank stability across a large sample and found that digital identity solutions – particularly biometrics, unified platforms, and digital wallets – directly enhance customer trust, loyalty, and satisfaction. However, the study does not examine how digital identity is governed or made accountable within the bank; it treats

identity as a technology, not as a governance pillar. The present study fills this gap by examining the internal mechanisms that enable – or disable – accountable digital identity in a public bank, revealing that without written policies and transparent audit trails, even basic password-based identity remains weak.

- Al-Rashdi, Dick & Storey (2017) identified nine core elements of accountability in cloud information security, of which five (responsibility, transparency, assurance, remediation, compliance) are directly relevant to banking. Nevertheless, these elements have not been operationalised into a diagnostic tool for evaluating bank-level accountability, nor have they been tested in a single-branch case study. The present study operationalises these five elements using concrete indicators (e.g., existence of a responsible person, clarity of audit procedures, existence of compliance reports) and reveals a critical gap in CPA: although transaction logging exists, audit clarity is low, and the legal department is entirely disconnected from digital sovereignty matters.

- Elliott et al. (2022) examined KYC practices, highlighting the balance between innovation and regulation. Zuo, Strauss & Zuo (2021) found that digital identity solutions increase customer loyalty and satisfaction. However, both studies assume a relatively mature regulatory environment. In Algeria, by contrast, the Bank of Algeria has not yet issued detailed regulations on cloud storage or data localisation (DataGuidance, 2025; Radio Algérienne, 2024), creating a fundamental regulatory gap that makes the innovation-regulation balance nearly impossible to achieve. The present study addresses this gap by documenting how a public bank navigates – or fails to navigate – this regulatory ambiguity, showing that legal clarity is a prerequisite for any effective digital identity and accountability system.

4. Digital Sovereignty in the Financial Sector:

- Patil et al. (2025) conducted the most comprehensive systematic review on data sovereignty in the financial sector. They identified 741 initial studies, narrowed them down to 52 papers (2014-2024), and found that of 13 data sovereignty methods examined, only five explicitly addressed security concerns, which are viewed as the most important component. Their research highlights significant variations across jurisdictions in regulating AI and maintaining sovereignty over financial data, emphasising that legal clarity matters more than strong supervision. However, the review is predominantly theoretical, based on analysis of legal frameworks. It does not provide field-based evidence from a single bank on how sovereignty is implemented – or hindered – in practice. This gap is precisely what the present case study of CPA Batna addresses.

- Shoker (2022) defined digital sovereignty as the bank's complete control over its digital data, encompassing security, governance, user rights, infrastructure, storage location, access rights, and the ability to refuse foreign authorities access. Codagnone & Weigl (2023) traced digital sovereignty to two problems – the difficulty of governing cyberspace and the excessive power of large technology companies. Stürmer, Nussbaumer & Stöckli (2021) warned of “data colonialism” where powerful states or companies exploit the data of less powerful states. All three studies, however, remain at the conceptual or geopolitical level. They do not provide practical measurement indicators for evaluating a single bank's sovereign capabilities. The present study fills this gap by translating these general principles into field-based indicators: where data are stored, what policies exist to prevent foreign access, whether local alternatives to foreign software are available, and how legal departments are involved in sovereignty decisions. The findings show that even when data are stored locally (as in CPA), legal sovereignty remains weak in the absence of clear implementing regulations from the Bank of Algeria.

Subsection two: Research Gaps analysis.

1. Summary of Research Gaps and Contributions

Based on the systematic literature review, four major research gaps have been identified. The following points summarise what previous studies lack and what the present case study of CPA Batna contributes to each gap:

a. Digital transformation strategies in developing-country banks:

- What previous studies lack: Bughrara et al. (2025) presented a multilevel framework that has not been empirically tested in a developing-country bank.
- What the present study contributes: Provides the first field-based assessment of digital transformation strategy implementation in an Algerian public bank (CPA), examining governance, identity, accountability, and sovereignty simultaneously.

b. Application of the Information Governance Framework (IGF) in a North African context

- What previous studies lack: Faria, Maçada & Kumar (2013) developed the IGF but did not test it in a developing-country banking environment.
- What the present study contributes: Applies the IGF framework diagnostically at a branch level to evaluate the current state of information governance and identify policy gaps.

c. Data sovereignty as a bank-level operational challenge

- What the present study contributes: Conducts the first micro-level empirical investigation of digital sovereignty constraints in a

public bank in Algeria, documenting the gap between documented security policies and enforceable legal sovereignty.

d. Integration of four interconnected concepts

- What previous studies lack: Most studies treat governance, identity, accountability, and sovereignty separately.
- What the present study contributes: Proposes an integrated theoretical framework that brings together all four concepts in a single case study.

2. Analysis of Research Gaps and Contributions of the Present Study

Based on the literature review presented in Subsection One, four main research gaps have been identified that have not been adequately addressed in previous academic studies. The present study is designed to address these gaps

Key Research Gaps

Lack of field application of digital transformation strategies in Algerian public banks: Despite advanced theoretical frameworks (Bughrara et al., 2025; Obaid, 2025), these strategies have not been empirically tested in a developing-country banking environment characterised by weak infrastructure and ambiguous regulatory frameworks.

Non-application of the Information Governance Framework (IGF) in a North African context: The IGF developed by Faria, Maçada & Kumar (2013) was tested in developed economies but has never been used diagnostically in a public bank in the Maghreb region that suffers from legacy systems and undocumented policies.

Absence of micro-level empirical investigation of digital sovereignty challenges: Studies on digital sovereignty (Shoker, 2022) have remained at the theoretical or regulatory level, without providing field-based indicators to measure a specific bank's control over its data in a regulatory vacuum.

Separate treatment of the four interconnected concepts (governance, identity, accountability, sovereignty): Previous literature has largely examined these concepts in isolation, whereas this study assumes they are interrelated and need to be addressed together in the context of banking digital transformation.

How the Present Study Addresses These Gaps

Lack of field application of digital transformation strategies (Research questions 1 & 3; Hypothesis H1): The present study provides the first field-based assessment of digital transformation strategy implementation in CPA (CPA Batna).

Non-application of IGF in North Africa (Research question 3; Hypotheses H2 & H3): The present study applies the IGF framework diagnostically to evaluate the state of information governance at the branch level.

Absence of micro-level investigation of digital sovereignty (Research questions 2 & 3; Hypothesis H3): The present study documents the gap between local data storage and enforceable legal sovereignty due to the absence of implementing regulations from the Bank of Algeria.

Section two: Conceptual Framework.

Digital transformation is not merely about adopting new technologies. It is a strategic choice that reshapes how banks create value, manage risks, and interact with customers. A successful digital transformation strategy requires a strong foundation in IT governance, digital identity management, digital

accountability, and digital sovereignty. This section examines these four pillars and their role in formulating and executing a digital transformation strategy for Algerian banks.

Digital transformation has changed how banks work; banks now use AI, cloud computing, and blockchain in their daily operations. Governance therefore plays a critical role. Clear governance helps banks stay secure, helps them follow the rules, and protects their strategy (Munira, 2025; Widharto et al., 2020).

This section covers two connected ideas: IT governance and digital identity.

IT governance sets the rules for technology investments. It makes sure these investments match the bank's goals. According to Weill and Ross (2004), IT governance is about who makes decisions and who is responsible. Without good governance, banks can end up with disconnected systems, broken rules, and security problems (Faria, Maçada & Kumar, 2013). Digital identity represents the second key concept. It helps banks build secure relationships with customers online. It makes authentication smooth and services personal. As banks move toward remote onboarding and real-time transactions, good digital identity solutions become necessary (Khattak et al., 2023; Zuo et al., 2021). Thus, IT governance and digital identity are complementary. Governance makes sure systems are managed well. Identity makes sure users are real and trusted.

This section has two parts. The first part looks at IT governance in banking: what it means, how it differs from information governance, the main theories behind it, the IGF framework, why governance matters, practical tools like COBIT and ITIL, and the key challenges. The second part covers digital identity. It looks at the technology behind it, how it improves customer

experience and financial inclusion, and what makes it hard to adopt in the banking sector.

Subsection one: Theoretical Foundations

This subsection lays the conceptual groundwork for analysing digital transformation in the Algerian banking sector. It is organised into two parts. The first part, “Banks and Digital Transformation in the Banking Sector”, introduces the Algerian banking context, digital banking services, information systems, and electronic governance. The second part, “Information and IT Governance: Theoretical Foundations and Frameworks”, presents core governance concepts, including the IGF framework, COBIT 2019, and ITIL 4, as well as key organisational theories (agency, resource-based view, dynamic capabilities). Together, these perspectives provide the analytical lens for interpreting the empirical findings of this case study.

1. Banks and Digital Transformation in the Banking Sector

a. Definition and Types of Banks

A bank is defined as a licensed financial institution that operates under the law, with the primary functions of receiving deposits, granting loans, and providing payment and transfer services, acting as a financial intermediary between surplus units (savers) and deficit units (investors and borrowers) (Weill & Ross, 2004; Rose & Hudgins, 2012). Banks are an integral part of any country's banking system and are supervised by a central monetary authority (the Central Bank), which sets the rules and regulations governing their activities.

In Algeria, the banking system is classified into three main categories (Ministère des Finances, 2026; Banque d'Algérie, 2023):

Public Banks (Banques publiques): Banks that are 100% state-owned and governed by the laws of state-owned economic enterprises (EPE). Prominent examples include Crédit Populaire d'Algérie (CPA), Banque Nationale d'Algérie (BNA), Banque de Développement Local (BDL), and Banque

Extérieure d'Algérie (BEA). These banks are characterised by their extensive branch networks but often suffer from partial technological accumulation and outdated centralised systems.

Private Banks (Banques privées): Banks with foreign or joint capital, such as Société Générale Algérie, BNP Paribas El Djazaïr, and Gulf Bank Algeria. They are generally distinguished by more modern governance systems and greater operational efficiency compared to public banks.

Islamic Banks (Banques islamiques): Financial institutions that comply with Sharia law in their operations and are subject to internal and external Sharia supervision. Examples include Al Baraka Bank Algeria and Islamic windows within some public banks.

The Central Bank (Bank of Algeria), as the supreme monetary authority, is responsible for regulating and supervising the sector by issuing laws and instructions that ensure the safety and stability of the banking system.

b. The Concept of Digital Banks and Digital Banking Services

The concept of the Digital Bank emerged as a result of the Fourth Industrial Revolution. It is a banking institution that operates entirely through electronic channels and digital platforms, using modern information technologies without relying on a physical branch network to conduct banking transactions. These banks automate all their operations, from account opening and identity verification (Digital Onboarding) to risk management and compliance.

Digital Banking Services, on the other hand, refer to the use of digital technologies to deliver traditional banking services (such as payments, transfers, and financing) in more convenient and faster ways. Digital banking differs from a digital bank, as the latter is an independent entity, while digitalisation is a transformation process within a traditional bank aimed at modernising its services and channels. These services are delivered via the

internet and mobile phones, and are characterised by their ease of use, lower costs, and speed.

c. The State of Digitalization and Digital Transformation in the Algerian Banking Sector

Evidence and sources indicate that the pace of digitalization in the Algerian banking sector remains relatively slow compared to other Arab and African countries. Most banks still use old, centralized systems (sometimes called legacy systems) and face challenges related to infrastructure and the availability of appropriate human resources. Nevertheless, monetary authorities are seeking to drive digital transformation through:

The establishment of a legal and regulatory framework that encourages the establishment of digital banks and defines the necessary licensing and activity rules and conditions (Khoukhi, 2025; Slitani, 2025).

The launch of a national payment strategy aimed at achieving a cashless society by 2028. This strategy promotes the use of modern payment methods and integrates new actors such as payment processing centres and digital banks (Banque d'Algérie, 2023).

The emergence of limited digital initiatives in some public banks, such as BDL's "Wimpay" application for instant payments, which is a local example of the uneven, gradual transformation across banking institutions (Khoukhi, 2025).

d. Banking Information Systems

A Banking Information System is an integrated set of technical components (hardware, software, databases), processes, and human resources that work in a coordinated manner to collect, process, store, and distribute information and data within the bank and between the bank, its customers, and external parties. Therefore, the banking information system is the cornerstone upon which all

forms of banking digitalization are built. It enables the automated execution of daily operations (e.g., deposits, withdrawals, transfers), facilitates risk management, data analysis, and regulatory compliance monitoring (e.g., anti-money laundering and personal data protection).

This system can generally be classified into two main branches (Khoukhi, 2025):

The Accounting System (Accounting Information Systems): Concerned with recording, classifying, summarising, and retaining all of the bank's daily financial transactions and operations.

The Management Information System (MIS): Complementary to the accounting system, focused on providing the reports and analyses necessary to support the bank's top management in strategic decision-making.

e. Electronic Banking Governance

Electronic Banking Governance is defined as the integrated framework of policies, procedures, and guidelines designed to ensure that electronic banking operations and services are managed and operated in a manner consistent with the bank's overall strategy and the regulatory rules issued by monetary authorities. It also aims to protect the bank's assets and customer information and to improve performance efficiency and transparency (Barry, 2020).

This governance framework typically includes:

- Defining the mechanisms and authority for decision-making regarding investments in digital projects.
- Establishing strict security policies to protect data and systems from cyber-attacks and threats.
- Ensuring the continuity of digital banking services (Business Continuity).

2. Complying with regulations and laws relevant to the financial sector, especially the Personal Data Protection Law (Law No. 18-07) (CMS Law, 2025; DataGuidance, 2025)

Information and IT Governance: Theoretical Foundations and Frameworks.

1) What is IT Governance?

Despite variations in emphasis, the scholarly literature converges on a common understanding of IT governance as a structured mechanism for distributing decision-making authority over technology within an organisation. Weill and Ross (2004, p. 1) offer one of the most cited formulations, characterising it as the specification of “decision rights and accountability” designed to generate desirable IT behaviour. This decisional focus is complemented by Peterson’s (2004, p. 7) dual-component definition, which distinguishes between the allocation of decision-making responsibilities across stakeholders and the procedural rules that govern strategic IT choices.

Van Grembergen and De Haes (2009, p. 5) broaden this perspective by emphasising the organisational infrastructure through which governance operates — namely the processes and structures that allow both business and IT actors to fulfil their mandates while maximising the value derived from technology investments. The IT Governance Institute (ITGI, 2003, p. 15) further situates IT governance within the wider enterprise framework, assigning responsibility to board-level leadership and insisting that IT must actively sustain and extend overall organisational strategy. Taken together, these definitions reveal a consistent thread: IT governance is fundamentally about alignment — aligning technology decisions with business objectives, and aligning accountability with authority.

For the purposes of this study, information governance is adopted as the broader concept encompassing policies, procedures, and structures for managing information as a strategic asset, while IT governance is considered a subset focusing on technology-related decision rights and accountability. This distinction follows the IGF framework proposed by Faria, Maçada and Kumar (2013).

2) IT Governance vs. Information Governance

Scholarly definitions of information governance span a spectrum from narrow policy-oriented frameworks to broad organisational mandates. At the policy end, Soares (2011, as cited in Faria, Maçada & Kumar, 2013, p. 2) emphasises the strategic function of governance, defining it as the formulation of cross-functional policy to optimise, secure, and leverage information as an enterprise asset. Complementing this, Kooper, Maes and Lindgreen (2011, as cited in Faria, Maçada & Kumar, 2013, p. 2) stress the procedural dimension, presenting information governance as the creation of an environment of rules and decision-making rights that covers the entire information lifecycle — from creation and collection through to storage, use, and disposal.

Synthesising these perspectives, Faria, Maçada and Kumar (2013, p. 9) define information governance as the establishment of formal policies, structures, and decision-making rights over information management, with the explicit objectives of reducing regulatory and operational risk, lowering costs, and optimising performance. The American Health Information Management Association (AHIMA, 2020) extends this scope further, framing information governance as an organisation-wide framework that addresses not only operational needs but also strategic, regulatory, legal, and risk-related requirements across the full information lifecycle. What emerges from these definitions is a clear progression: governance of information begins with policy

and rules, but ultimately serves the organisation's broader strategic and compliance obligations.

Comparison between IT Governance and Information Governance

This table shows the differences between IT governance & Information governance:

Table 1: the difference between IT governance & information governance

Criterion	IT Governance	Information Governance
Primary focus	The tools: network, software, hardware, computers, and IT infrastructure.	The content: Data, documents, records, and knowledge assets.
Main objective	Ensure IT investments are efficient, secure, and aligned with business strategy.	Optimize the value, security, and lawful use of information as a strategic enterprise asset.
Scope	IT systems, applications, architecture, and technical operations	All structured and unstructured information across the entire organization (lifecycle management)
Key questions	Does the system work? Is it safe? Does it help the bank do its job?	Is the data correct? Is it private? Are we following the rules? Are we using it the right way?
Accountability	The IT department and top tech managers	Shared responsibility across all departments (legal, compliance, HR, operations, etc.).
Risk focus	System crashes, cyber-attacks, late projects, old technology problems	Regulatory and legal risks: non-compliance, data breaches, privacy violations, poor data quality.
Value	System reliability, cost-effective IT services, technical agility	Trustworthy data, regulatory compliance, transparency, informed decision-making

3) Three Theories behind Information Governance

The following theories explain why governance works the way it does. Faria, Maçada and Kumar (2013) mention them.

Faria, Maçada and Kumar (2013) built their work on three main theories. Each theory looks at governance from a different angle. Together, they give a full picture of why governance matters and how it works in banks.

Agency theory

Agency theory is built on simple steps. There is a boss, called the principal, and an employee, called the agent. The agent makes decisions for the boss. But what if the agent does things the boss would not want? For example: an employee might take too much risk or hide bad news.

Resource-based view (RBV)

RBV asks a different question. What makes a bank successful? The answer: resources that are valuable, hard to copy, hard to replace, and rare. Information fits this description perfectly. A bank that manages its data well can make better decisions and spot fraud faster. Competitors cannot easily copy that advantage.

Dynamic capabilities theory

Markets change quickly. The shift from cash transactions to electronic payments happens in a short time. Banks cannot remain passive in this environment. They have to respond fast. Teece, Pisano and Shuen (1997) argued that owning resources is not enough. Banks also need the ability to reshape those resources when conditions change. For example, a bank may have large amounts of customer data. That is positive. However, if the bank does not know how to use that data for better decisions, the data becomes useless. Similarly, a bank may have skilled employees. That is also positive. However, if those employees do not receive training on new systems, their skills become a weakness.

Dynamic capabilities rest on three main elements: flexibility, continuous learning, and the ability to reconfigure existing resources.

Because the banking environment keeps changing, governance cannot be static. It must allow the bank to adapt. Otherwise, governance becomes an obstacle rather than a support.

4) The Information Governance Framework (IGF)

Faria, Maçada and Kumar (2013) went further than just theories. They came up with something that can actually be used. A framework. They called it the Information Governance Framework or “IGF” for short. This framework has three main parts: the dimensions; each dimension contains several factors, in total, twenty factors.

The three dimensions

- a) People: This dimension focuses on the human part, then three important factors appear here: Context; the environment around information, how does the bank handle data day to day. Culture; shared value. Does the bank care about privacy? Are there clear rules about what staff can and cannot do?
- b) Policies: this is the biggest dimension, as it includes 14 factors; these consist of the rules and policies that govern the information cycle, including:
 - Accessibility: can the right people find the information they need at the right time?
 - Accountability: who is responsible when something goes wrong? And who faces the consequences of misusing data & information?
 - Privacy: is customer data protected from people who should not to see it? Does the bank ask permission before sharing data?
 - Security: are systems safe from hackers? Is data encrypted? Can someone break in and steal customer records?

- Quality: is the information accurate, complete, up to date? Or full of errors and duplicates?
- Retention: How long does the bank keep information? Is there a rule for safely deleting old data?
- Compliance: Does the bank follow laws? Anti-money laundering rules? Data protection laws?
- Sharing: Is information exchanged between departments safely? With outside partners? With clear rules?
- Standardization: Does all data follow the same format? Or does each department use its own system?
- Transparency: Can everyone (auditors, managers, customers) see how information is used and who changed it?
- Value: Does the information help the bank make money? Save costs? And Serve customers better? Or is it just sitting there?
- Communication: How does information move between people and departments? Are there clear channels?
- Formal Structure: Is there a clear organization chart for information management? Who reports to whom?
- Monitoring: Is there regular checking of who accessed what? Are there audits?

c) Technology:

There are three factors:

- Consumerization: Using the bank's tools and technology instead of external or employee-owned means in transactions, which increases the risks that governance must handle.
- Mobility: Control access to data.

- Systems: The software and infrastructure that store and process information. Old systems cause problems. New systems need oversight.

5) Why Governance Matters for Banks?

Good governance matters for banks for several reasons.

- Compliance: Banks must follow rules issued by the central bank, anti-money laundering laws, and data protection regulations. Governance helps banks meet these requirements.
- Cost reduction: Disorganized data creates storage costs, duplicates, and errors that need correction. Clean governance lowers these costs.
- Better performance: Reliable information leads to sound decisions. Unreliable information leads to poor decisions. The link between information quality and decision quality is direct.
- Trust: Customers and shareholders need to feel that their data is safe. Governance builds that trust.

A senior banker in Hong Kong explained: "Without proper governance, one can use information for improper activities which may damage a firm's reputation, revenue, credibility, and may be subject to regulatory and legal litigations" (Faria, Maçada & Kumar, 2013, p. 6). An advisor to China's banking regulator added: "Reliable information is the real asset for banks. It helps bankers to make good decisions. Reliable information comes from governance" (Faria, Maçada & Kumar, 2013, p. 6).

6) Practical Frameworks – COBIT and ITIL

Theoretical knowledge about governance is necessary, but banks also need practical tools to apply that knowledge in daily operations. Two frameworks are widely used in the banking sector.

COBIT 2019

COBIT stands for Control Objectives for Information and Related Technologies. This framework was developed by ISACA (2019). Its main purpose is to help banks align their IT activities with business goals. COBIT also helps manage technology-related risks, comply with regulations, and generate value from IT investments.

COBIT 2019 separates governance from management. Two different jobs. Governance sets the direction. It watches performance. Management does the work. It plans, builds, and runs things day to day. Figure 1 illustrates this separation.

Defining Governance and Management

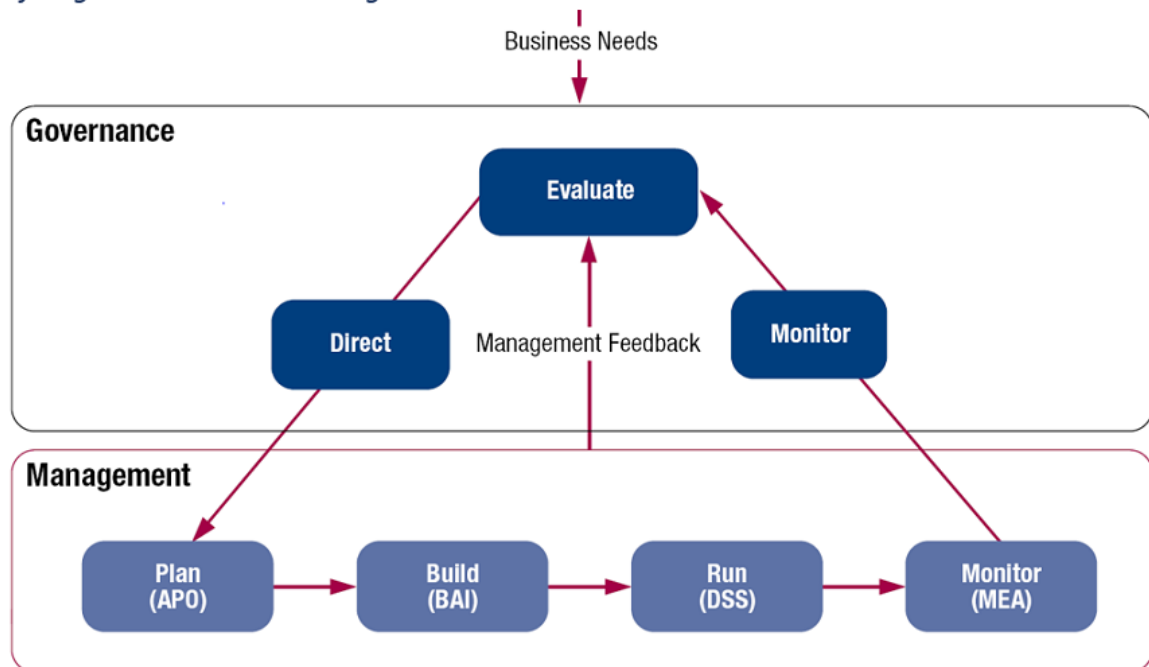


Figure 1: Defining Governance and Management in COBIT 2019. Adapted from "COBIT 2019 Framework: Governance and Management Objectives" by ISACA, 2019

Creating value is the main goal of IT governance. COBIT breaks this goal into three parts. Delivering benefits. Reducing risks. Using resources wisely. Figure 2 shows how stakeholder needs drive these three objectives.



Figure 2: Governance Objectives in COBIT 2019 – Value Creation. Adapted from "COBIT 2019 Framework: Governance and Management Objectives" by ISACA, 2019

ITIL 4: it stands for Information Technology Infrastructure Library. Axelos (2019) defined it as a set of best practices for managing IT services. Unlike COBIT, which focuses on governance and strategy, ITIL focuses on service quality and customer satisfaction.

ITIL 4 has a new model. It is called the Service Value System. The SVS has five parts. Guiding principles. Governance. The service value chain. Practices. Continual improvement. Figure 3 shows how they fit together.

 The picture can't be displayed.

Figure 3: The ITIL 4 Service Value System (SVS). Adapted from "ITIL 4 Service Value System" **Axelos/PeopleCert (2019). ITIL 4 Foundation.**

Inside the SVS, there is the service value chain. It is the engine. Six activities are connected. Plan. Engage. Design and transition. Obtain or build. Deliver and support. Improve. Figure 4 shows how demand turns into value through these steps.

 The picture can't be displayed.

Figure 4: The ITIL 4 Service Value Chain. Adapted from "Service Value Chain Diagram" **Axelos/PeopleCert (2019). ITIL 4 Foundation.**

Combining COBIT and ITIL

Neither framework is sufficient on its own. Boadu et al. (2025) argue that combining COBIT and ITIL provides a more complete approach. COBIT handles strategic oversight and high-level governance. ITIL handles operational processes and day-to-day service management. Together, they help banks maintain smooth operations, strengthen security, and comply with regulatory demands.

This subsection aimed to establish the theoretical foundations of IT governance in banks, covering its definitions and theoretical frameworks. The findings of the subsection are as follows:

It became clear that IT governance is not limited to the technical side; it also includes decision-making rights and accountability frameworks. Four definitions were reviewed, the most prominent being that of Weill and Ross (2004). The definitions confirmed that IT governance is the responsibility of top management and the board of directors, not merely a technical task.

A distinction was made between the two terms IT governance and information governance. The analysis showed that information governance emerged as a response to the shortcomings of IT governance in managing information as a strategic asset.

It was also shown that governance helps banks in four main areas: regulatory compliance, cost reduction, performance improvement, and building trust. This was evidenced by statements from senior officials in global banks.

The subsection reviewed two practical frameworks for implementing governance: COBIT, which focuses on strategic governance and risk management, and ITIL, which focuses on the quality of technical services. The analysis showed that combining COBIT and ITIL provides a comprehensive approach that brings together strategic oversight and effective operations.

This subsection represents the first building block in constructing the conceptual framework of the study and paves the way for the second chapter, where these concepts will be applied in the real banking context.

Subsection two: Digital Accountability, Sovereignty, and Identity in the Banking Environment.

After examining IT governance and its theoretical foundations in the previous subsection, this subsection focuses on three interrelated concepts that are essential for a comprehensive digital transformation strategy in banking: digital accountability, digital sovereignty, and digital identity. Each concept is defined and analyzed in relation to the banking context. The subsection also discusses governance mechanisms, the Algerian regulatory framework (notably Law No. 18-07 and its amendment Law No. 25-11), and future trends. Together, these elements complete the conceptual framework that will guide the empirical investigation of the CPA Batna branch.

1) Digital Accountability

A coherent digital transformation strategy cannot succeed without clear accountability and sovereign control over data. This subsection explores how banks can integrate digital accountability and sovereignty into their strategic planning. It covers the core concepts, governance mechanisms, regulatory frameworks in Algeria, and future trends that should inform strategic decision-making.

Digital accountability is about who takes responsibility for data in the digital world. For individuals. For banks. For every action. Every click. Every change. Someone must be in charge. Every data access, every modification, every share must have a clear owner. According to Al-Rashdi, Dick and Storey (2017), nine core elements make up accountability in cloud information security. Not all are equally important. The most relevant for banking are: responsibility (a clear person in charge), transparency (actions visible and

traceable), assurance (proof that rules were followed), remediation (fixing mistakes), and compliance (following laws and rules). That is the core. Accountability does not stand alone. In banking, it is tied to governance and transparency. Ibáñez Zapata (2017) makes this clear.

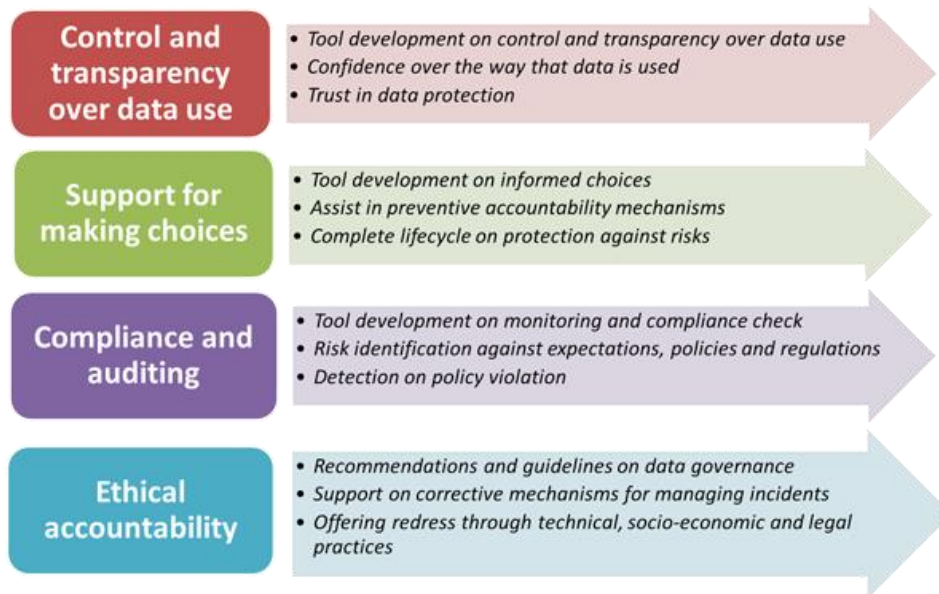


Figure 5: Key Dimensions of Digital Accountability. Adapted from "Objectives" **Pearson et al. (2012). Accountability as a Way Forward for Privacy Protection in the Cloud.**

As shown in Figure 5, digital accountability is built on control and transparency, informed choice, compliance and auditing, and ethical accountability. These dimensions align with the nine core elements discussed earlier and provide a practical framework for banks.

Strong governance and transparent reporting, he argues, are the very foundation of banking accountability. Without them, no compliance. No customer trust. Nothing. Then comes digital transformation. It changes things. It widens the scope. Sewpaul (2018) notes that as banks go digital, they must still stay accountable. Customer data must be protected. Customers must know how their data is used. No secrets. Guerin (2022) goes even further. He pulls cyber risks into the picture. Boards and managers, he says, are no longer just

about money. They are also about data security. About digital resilience. Cyber risks are now central to governance. That is the new reality.

So, in short, digital accountability rests on a few clear pillars. Clear responsibility. Transparency. Compliance. Cyber risk management. Without these, banks cannot operate safely today. Not really.

2) Digital sovereignty

Digital sovereignty means the bank's complete control over its digital data. It includes security, governance, user rights, and infrastructure. It also relates to where data is stored and who can access it. It also includes the ability to refuse foreign authorities access to customer data (Shoker, 2022). The root of the concept of digital sovereignty goes back to the Treaty of Westphalia in 1648. However, it emerged as an independent term in the 1990s as states sought to develop and regulate their digital infrastructure (Codagnone & Weigl, 2023).

Digital sovereignty is a complex concept. In the analog world, sovereignty is multifaceted. In the digital world, complexity increases. The reason is the interconnection between the two domains and the absence of a supreme authority in cyberspace (Tretter, 2022). Major technology companies such as Microsoft, Google, and Meta own vital infrastructure. They can, theoretically, disconnect parts of the digital world. Stürmer and his colleagues (2021) warn of the danger of "data colonialism," where powerful states or companies exploit the data of less powerful states.

Movements such as "global digital constitutionalism" seek to establish regulatory frameworks that protect the rights of states and individuals in digital space (Gurumurthy & Chami, 2021). In the banking sector, the challenges of digital sovereignty are particularly evident. Banks rely on global digital infrastructure. They use cloud services from foreign companies. Customer data may be stored on servers outside the country. This exposes it to foreign laws that may conflict with local laws. Therefore, banks seek to adopt digital

sovereignty strategies, such as hybrid cloud computing and data localisation. There are multiple mechanisms for achieving digital sovereignty. States enact data protection laws (such as the General Data Protection Regulation, GDPR in the European Union). They also develop strategies to reduce dependence on foreign technology (Shoker, 2022).

In conclusion, digital sovereignty is a multidimensional and multi-level concept (Shoker, 2022; Codagnone & Weigl, 2023). It is not merely a technical or legal matter, but a geopolitical, economic, and social issue (Gurumurthy & Chami, 2021). It poses significant challenges to banks and financial institutions that operate across borders and use global digital infrastructure. Achieving digital sovereignty requires a delicate balance between protecting national security, respecting user rights, promoting innovation, and international cooperation.

Table 2: the 5 th levels of digital sovereignty. (Shoker, 2022)

Level	Description	Key Risk
Full reliance on US services	Both the software and hosting are owned and operated by US companies, often with data stored in US data centres.	Data is subject to US surveillance laws (e.g., Cloud Act) with no European protection.
European services with US hosting	A European SaaS provider, but their underlying infrastructure is a standard US cloud (AWS, Azure, GCP) located in the US.	A European contract, but the data is physically stored in the US and subject to US jurisdiction.
European hosting by US companies	The data is stored on European soil, operated by EU staff of a US cloud provider.	The jurisdictional link to the US remains via the parent company's ownership, creating a potential legal risk.
Zero-Trust data security (SKS)	Data is hosted on a US-owned cloud in Europe, but encryption	The provider cannot access the decrypted data, neutralising the risk of foreign access.

	keys are managed separately by a European entity.	
Fully European sovereign stack	Both the software provider and the data Centre are European-owned and operated, with no jurisdictional link to non-EU laws.	The gold standard. Total digital autonomy and no exposure to non-EU laws.

3) Governance mechanism

Governance is not just a definition. It needs practical mechanisms. Tools. Clear lines of responsibility. Institute of Internal Auditors (2020) described a widely adopted model in banks with three lines of defence.

- First line: consists of business and support functions. These functions set the rules and implement them. They manage daily operations. They are responsible for applying governance.
- Second line: risk oversight and compliance. This function monitors adherence to rules. It makes sure the first line does not deviate from policies and regulations.
- Third line: internal audit. It reports on the effectiveness of governance, risk management, and compliance. It provides independent assurance to the board. Unlike the first two lines, it works away from any managerial influence.

Besides these lines, other mechanisms support accountability. Ramesh and his colleagues (2022) highlighted written policies, regular audits, and disclosure to stakeholders. Written policies set clear expectations. Audits verify that policies are followed. Disclosure informs stakeholders about both processes and outcomes.

These mechanisms work together. They turn abstract governance principles into concrete actions. Without them, accountability remains just a concept, not a practice.

4) Regulatory Frameworks in Algeria: Developments and Challenges

Recently, Algeria has witnessed legislative developments in the field of personal data protection, reflecting an awareness of the importance of regulatory frameworks and digital sovereignty. Law No. 18-07 of 10 June 2018 on the protection of natural persons with regard to the processing of personal data was issued, but it was not effectively applied until the establishment of the National Authority for the Protection of Personal Data (ANPDP) in August 2023 (CMS Law, 2025). This law is the reference legal framework that regulates the collection, processing, storage, and transfer of personal data by public and private entities, including banks. With the aim of aligning Algerian legislation with international standards such as the European General Data Protection Regulation (GDPR) (DataGuidance, 2025), Law No. 25-11 amending and supplementing Law No. 18-07 was enacted. This amendment introduced new obligations for institutions, including the requirement to appoint a Data Protection Officer, maintain records of processing activities, conduct data protection impact assessments, and report personal data breaches within specified deadlines (CMS Law, 2025). It also strengthened the powers of the National Authority (ANPDP) in supervision, investigation, and the imposition of administrative fines.

Alongside the data protection law, Algeria ratified a new law on anti-money laundering and counter-terrorism financing (AML/CFT) in July 2025, which aligns with the updated suggestions of the Financial Action Task Force (FATF) and imposes stringent obligations on financial institutions, including banks, regarding customer due diligence (KYC) and the reporting of suspicious transactions (Arab, 2025). This law creates additional compliance requirements

that intersect with data protection obligations, potentially placing banks before coordination challenges. Despite these developments, the regulatory frameworks related to digital sovereignty for banks remain incomplete. The Bank of Algeria (Banque d'Algérie) has not yet issued detailed regulations specifying the rules for storing banking data on cloud servers, the conditions for using foreign cloud service providers, or the requirements for localising sensitive data (DataGuidance, 2025; Radio Algérienne, 2024). This regulatory gap places Algerian banks, in a state of legal uncertainty, hinders their ability to develop clear digital sovereignty strategies, and limits their investments in cloud computing and cross-border digital services. Although Algeria has established an initial legal framework for personal data protection, the path towards achieving genuine digital sovereignty in the banking sector remains long. Banks need clear implementing regulations from the Bank of Algeria that determine where data can be stored, the terms for contracting with foreign cloud providers, and mechanisms for dealing with foreign legal requests for data access. Without these regulations, banks remain in a grey area, unable to achieve full compliance or benefit from the opportunities offered by digital transformation.

It is important to acknowledge, however, that Algeria has taken a partial step toward regulating digital banking through Regulation No. 24-64 of October 2024, which introduced the legal framework for digital banks. This regulation mandates that licensed digital banks must host their operational platforms locally within Algeria. While this represents legislative progress, it does not resolve the broader regulatory ambiguity identified in this study for two reasons. First, Regulation 24-64 applies only to newly established digital banks, not to traditional public banks such as CPA. Second, it does not address critical issues of data sovereignty for existing banks, such as cloud storage conditions, data localization requirements for customer data, or mechanisms for responding to foreign legal requests. Therefore, the regulatory vacuum

concerning banking data sovereignty for conventional banks remains largely unaddressed (DataGuidance, 2025; Radio Algérienne, 2024).

Figure 6 shows the key steps that Algerian banks must follow to comply with Law No. 18-07 as amended by Law No. 25-11 regarding personal data protection:

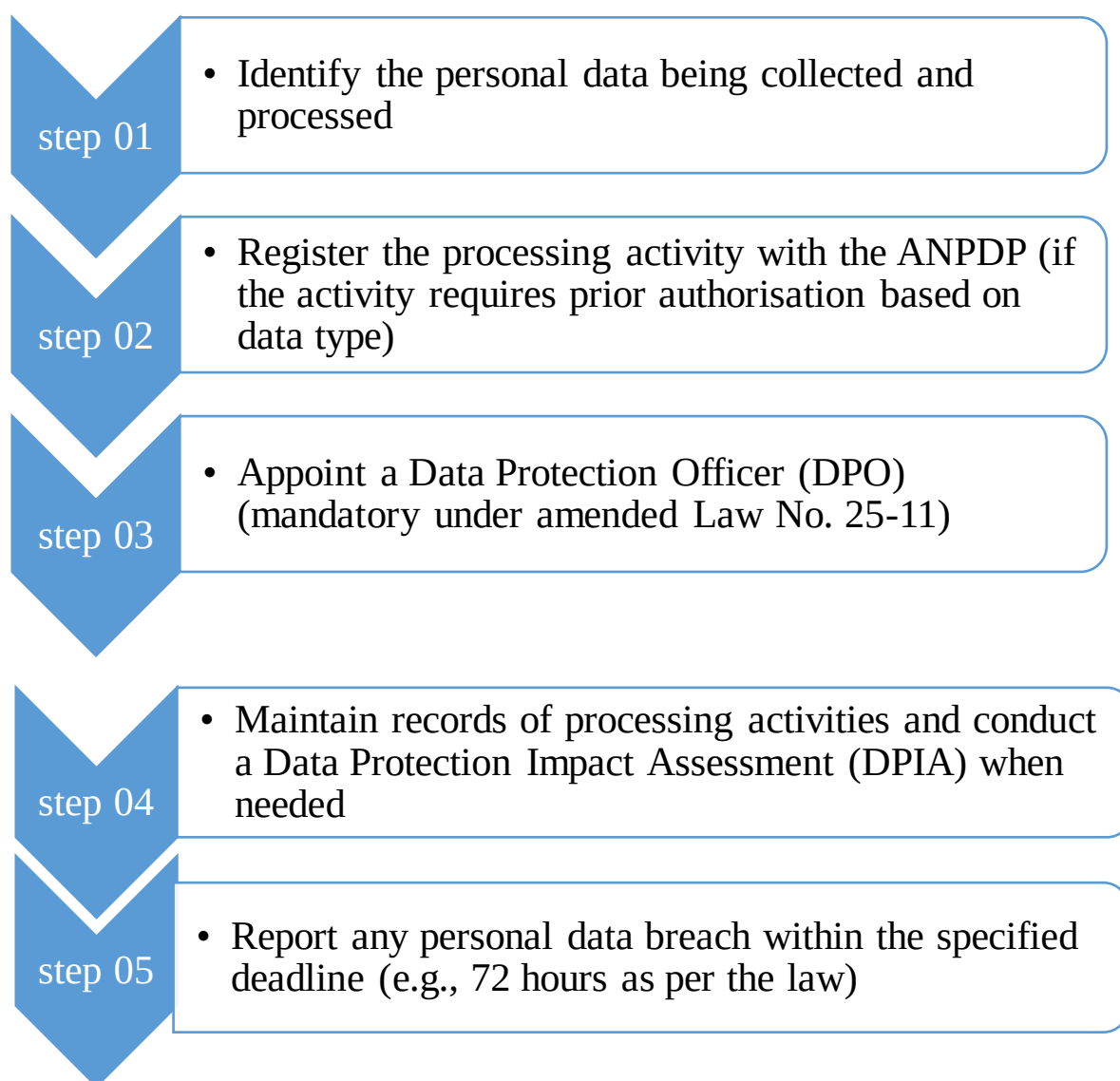


Figure 6: Compliance Flowchart for Personal Data Protection in Algerian Banks. **Based on CMS Law (2025) and DataGuidance (2025)**

5) Future Outlook: General Perspectives

Digital accountability and digital sovereignty will matter more in the coming years. Banks cannot ignore them. Several trends are already visible. Each trend has its own implications for banking.

Data protection laws

Data protection laws are spreading. More countries are adopting GDPR-style rules. The European Commission has proposed a digital simplification package. One part is the Data Union Strategy. Its aim? To reduce fragmented data rules and strengthen the EU's hand in international data flows (Moody's, 2025).

Then there is the FiDA Regulation. It is expected to take effect in mid-2026. It creates a common legal framework for data exchange. Who is involved? Customers, financial institutions, and other financial information service providers (CMS Law, 2025). Across the Atlantic, the US has its own rules. The CFPB's Personal Financial Data Rights Rule (effective 2026-2030) requires banks to support consumer-directed data access and secure API-based sharing (CFPB, 2024). So what does this mean for banks? Those that operate across borders will face multiple legal requirements. Sometimes these requirements conflict. The bottom line? Rules are getting stricter, not looser.

Cloud computing

Cloud computing will keep growing. But concerns about data sovereignty will grow too. Banks will still rely on major cloud providers. Yet regulators are warning against over-dependence on a small number of non-European IT vendors. They now see this as a systemic risk (Corporater, 2025).

How are banks responding? Many are turning to hybrid cloud strategies. They keep sensitive customer data and core systems in private clouds. They use public clouds for customer-facing applications and analytics (International Banker, 2025). Some banks are creating dedicated sovereign regions. Others

are partnering with hyperscalers to run segregated environments with sovereign controls. And many are demanding local data storage options from cloud providers.

The growing demand for data sovereignty solutions is reflected in market projections. Figure 07 shows the expected growth of the data sovereignty cloud market between 2026 and 2030:



Figure 7: Data Sovereignty Cloud Market Forecast (2026-2030). Data Sovereignty Cloud Market" by Research and Markets, 2026 (<https://www.researchandmarkets.com/reports/6191053>).

Accountability mechanisms

Accountability mechanisms will become more automated. Regulators will expect real-time monitoring and reporting. Manual audits will no longer be enough. In 2026, financial institutions will need stronger controls around AI-driven compliance. This applies especially to AML transaction monitoring, sanctions screening, and alert triage (FATF, 2023).

The benefits of using technology for compliance are well documented. Figure 8 shows the top five benefits identified by the PwC Global Compliance Survey 2025:

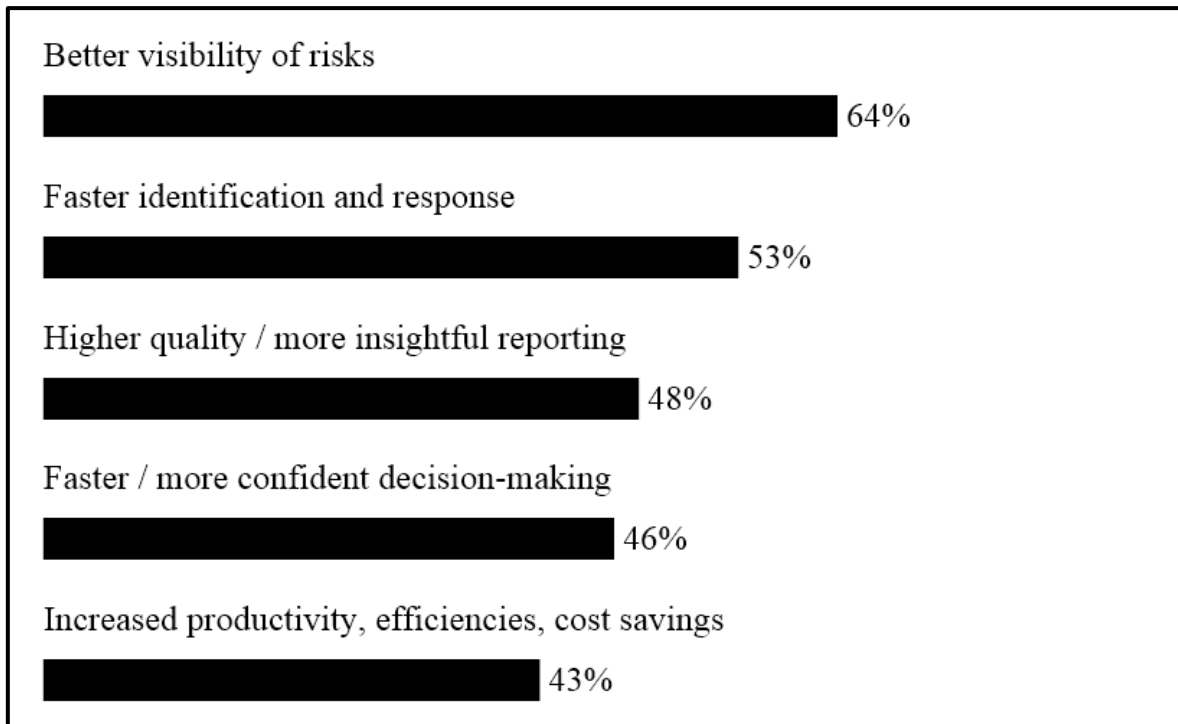


Figure 8: Top Benefits of Technology in Compliance (Source: PwC Global Compliance Survey 2025, via Secureframe).

RegTech solutions that automate compliance are already widely adopted. They reduce costs and ensure regulatory adherence (GetFocal, 2025).

Banks that fail to invest in automated accountability systems? They will struggle to keep up.

Customers

Customers will demand more transparency. Recent surveys confirm this shift. A 2025 Harris Poll found that 90% of Americans believe they, not their banks, should control how and when their financial data is used (Financial Technology Association, 2025). The 2025 EY Canada Open Banking Survey reported that 72% of Canadian consumers insist that their data be used only for its intended purpose. It also found that security, data control, and trust combined are 27% more important to consumers than the ease of banking processes (EY, 2025). Banks that cannot answer basic questions about where

data is stored, who has access, and how it is used will lose customer trust. Those that provide clear, transparent answers will gain a competitive advantage.

International cooperation

International cooperation on data governance will increase. But it will remain difficult. The era of a single, borderless global cloud is over. Legal and geopolitical conflicts have fractured it. Think of the US CLOUD Act versus the EU's GDPR (Futurum Group, 2025).

This fragmentation is sometimes called the “Westphalian World Web.” It has created a new “Splinternet.” In this world, data sovereignty is a primary concern. Cross-border data flows are caught between conflicting priorities. Data protection. National security. Free digital trade. China, the EU, and the US are each developing their own policies. Each has different priorities (ETH Zurich, 2025). Some countries will work together on common standards. Others will push for digital sovereignty through localization requirements. Banks will need to navigate this fragmented landscape carefully. For developing economies such as Algeria, the future presents both challenges and opportunities. The lack of clear, fully implemented regulations today is a problem, as discussed in the previous section on regulatory frameworks. However, it is also a chance to build a modern framework from the start.

Algerian banks can learn from the experiences of other countries and adopt best practices without repeating past mistakes. They can observe how European and North American banks are responding to the trends outlined above, and they can design their own digital governance strategies accordingly. However, time is not unlimited. Global standards are emerging. Banks that delay in implementing accountability and sovereignty mechanisms will fall behind. They will find it harder to partner with foreign banks, which increasingly require demonstrable compliance with international data protection norms. They will struggle to serve customers who expect

international-level data protection. And they will face growing scrutiny from regulators who are themselves adapting to the new digital reality.

In conclusion, the future of digital banking belongs to those who take accountability and sovereignty seriously. Not as an afterthought. Not as a compliance burden. As a strategic priority. Banks that invest now in robust data governance, transparent customer communication, automated compliance systems, and flexible cloud architectures will be ready for the challenges ahead. Those that wait will face a difficult path.

6) Digital Identity: Definitions, Technologies, and Challenges.

a) Digital identity

Digital identity is the electronic representation of a person's identity in the digital space. It includes attributes such as name, national identification number, biometric data (fingerprint, facial recognition, voice recognition), and digital certificates. In practical terms, digital identity serves two purposes. First, it identifies who is logging into a banking system. Second, it helps the bank verify that the person is legitimate. Without digital identity, online banking would not function properly. Customers could not open accounts remotely, make payments from their phones, or check their balances without visiting a branch.

Khattak et al. (2023) explain that digital identity helps banks build secure relationships with customers. Zuo, Strauss and Zuo (2021) add that digital identity increases customer loyalty and satisfaction, particularly when authentication processes are smooth and efficient.

b) Importance of Digital Identity for Banks

- Security. Biometric authentication and multi-factor verification reduce fraud and make impersonation more difficult for criminals.

- Customer experience. Fingerprint or facial recognition is faster than remembering long passwords. Customers generally appreciate this convenience.
- Regulatory compliance. Banks must comply with Know Your Customer (KYC) and anti-money laundering (AML) regulations. Digital identity enables remote verification without requiring customers to visit a branch (Elliott et al., 2022).
- financial inclusion. Individuals without traditional identification documents can still open accounts using digital identity solutions, thereby bringing more people into the formal banking system.

c) Key Technologies Supporting Digital Identity

Table 3: key technologies of supporting digital identity.

Technology	Description	Strength	Weakness
Biometrics	Uses fingerprints, facial recognition, or voice	Difficult to forge; convenient	Privacy concerns; cannot be changed if compromised
Multi-factor authentication	Combines password, phone, and biometric	Highly secure	Adds an extra step for users
Self-sovereign identity	Stores identity and payment data on mobile devices	Fast and seamless	Requires a smartphone
Digital wallets	User controls own data via blockchain	High privacy; no central point of failure	Still emerging; requires legal recognition

Sources: Based on Khattak et al. (2023); Zuo, Strauss & Zuo (2021); Goodell, Al-Nakib & Tasca (2021).

Challenges in Implementing Digital Identity

- Technical challenges: Different banks use different systems, making interoperability difficult. Biometric systems can fail due to poor lighting, dirty sensors, or changes in a person's appearance.
- Regulatory challenges: Collecting biometric data requires strong legal developing. A digital identity issued in one country may not be accepted in another.
- Social challenges: Elderly customers may not own smartphones. Some customers fear that their biometric data will be misused. Others simply do not understand how digital identity works.

Elliott et al. (2022) highlight the tension between innovation and regulation. Banks must innovate to remain competitive, but they must also protect customer data and comply with the law.

This subsection covered three main concepts. Digital accountability. Digital sovereignty. And digital identity. Digital accountability simply means: who is responsible for the data? Who saw it? Who changed it? Who shared it? Every action must have an owner. It rests on four pillars: clear responsibility, transparency, compliance with laws, and cyber risk management. Digital sovereignty means the bank's full control over its data. Where is it stored? Who can access it? Can the bank refuse foreign authorities' requests? Cloud computing creates challenges, but hybrid solutions and data localization help address them.

Digital identity is how the bank knows its customer online. Key technologies include biometrics, facial recognition, multi-factor authentication, and digital wallets. They help with security, customer experience, and compliance.

Governance mechanisms rely on three lines of defense: daily operations, risk oversight, and internal audit. Along with written policies and regular audits.

In Algeria, two data protection laws have been issued (Law No. 18-07 and Law No. 25-11). But detailed regulations for banking digital sovereignty are still missing. The future outlook points to five trends: stricter data laws, cloud growth with sovereignty concerns, automated accountability, customer demand for transparency, and fragmented international cooperation.

Figure 9 illustrates how the four concepts of this study are nested and interrelated. Digital transformation provides the enabling context. The IGF of Faria, Maçada & Kumar (2013) serves as the analytical lens through which digital identity (H1), accountability (H2), and digital sovereignty (H3) are examined.

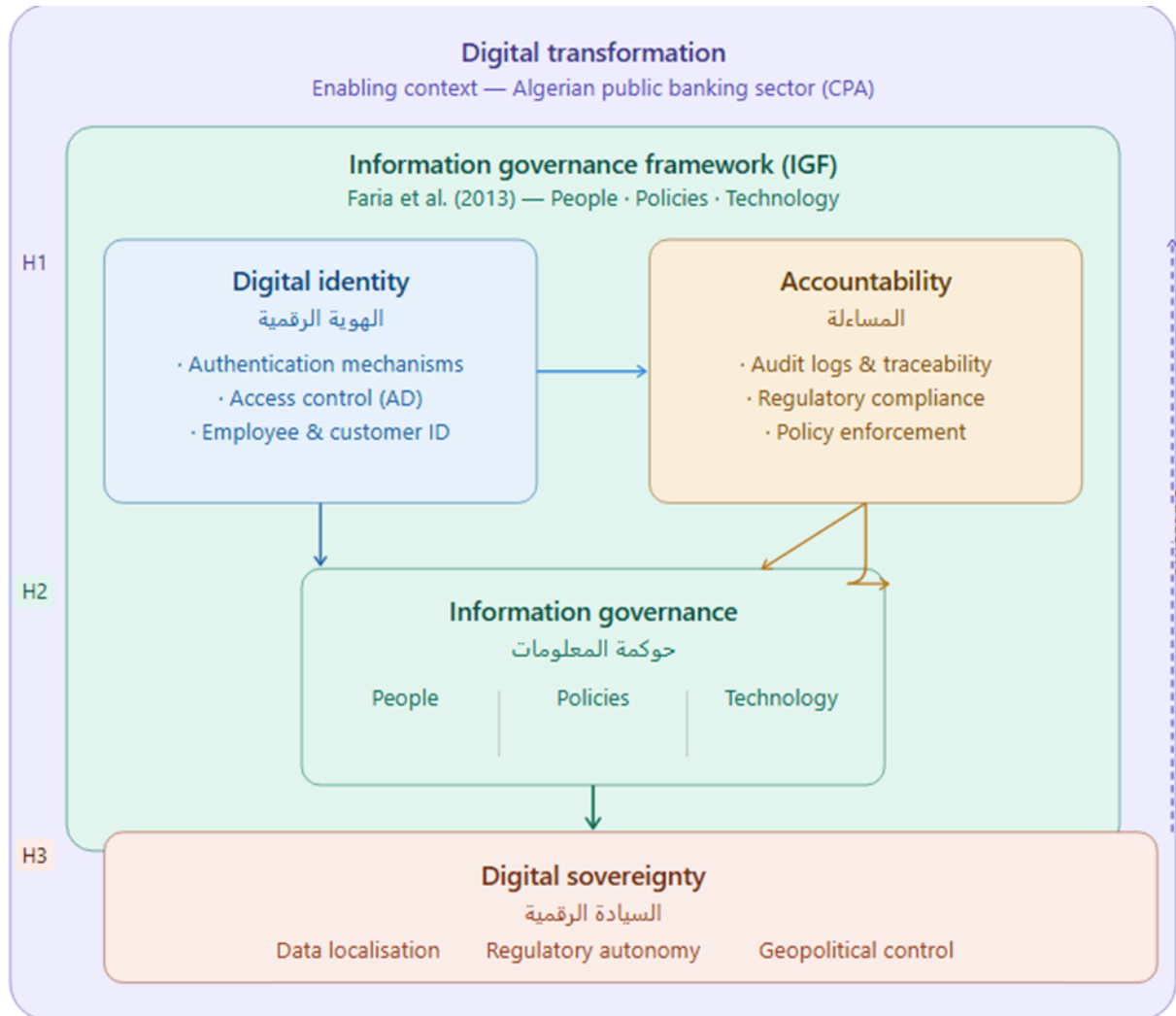


Figure 9: Integrated Conceptual Framework — Digital Transformation, Information Governance, Digital Identity, Accountability, and Digital Sovereignty.

Chapter II:

Case Study Presentation (CPA) and the Methodological Framework.

This chapter presents the methodological framework adopted to answer the research questions, as well as the case study institution. The chapter is divided into two main sections. The first section introduces Crédit Populaire d'Algérie (CPA) in terms of its history, organisational structure, information systems, and digital tools. The second section is dedicated to the methodological framework, which defines the research variables, explains the epistemological foundations (interpretivism) and the logic of reasoning (abduction), and then details the data collection instruments (interviews, questionnaire, documentary analysis, observation), analysis procedures (SPSS and NVivo), quality criteria, ethical considerations, and research limitations. This division ensures a clear understanding of both the case study context and the methodology employed, before presenting and discussing the findings in Chapter Three.

Section One: Introduction to “Crédit Populaire d’Algérie (CPA)”.

This section presents the case study of Crédit Populaire d’Algérie (CPA), with a focus on the Batna branch (Agence 120 / Groupe d’Exploitation 835). It is divided into two subsections. The first subsection provides a general overview of the bank: its history, organizational structure, and current information systems. The second subsection examines the existing digital strategy, or rather the lack of a coherent one, based on internal reports and field observations. Understanding this context is essential before analyzing the survey and interview results in the next chapter.

Subsection One: History, Organizational Structure, and Information Systems of CPA.

1. A Brief History of CPA

“Crédit Populaire d’Algérie (CPA)” is one of the largest public banks in the country. It was established in 1966 by Ordinance No. 66/366 of 29 December 1966, and its statutes were approved by Ordinance No. 67/78 of 11 March 1967. The bank inherited the activities of several popular banks that existed during the colonial period in Algiers, Oran, Constantine and Annaba. In 1972, its structure was strengthened by taking over foreign banks such as the Society Marseillaise of Credit and the Bank” Mixte Algérie-Misr”. In 1985, CPA created the Bank of Development Local (BDL) by transferring 40 branches, 550 employees and 89,000 accounts.

In 1997, the bank obtained approval from the Bank of Algeria under the monetary and credit law 90/10. Since then, CPA has operated as a state-owned commercial enterprise (EPE) under the supervision of the Ministry of Finance. Its current share capital is 48 billion Algerian dinars. According to an internal report, the bank started with an initial capital of 15 million dinars and is now the second largest commercial bank in Algeria.

This historical background shows that CPA has gone through several reorganizations. However, none of these transformations were driven by a digital vision. The focus was always on expanding the branch network and increasing the volume of operations, not on modernizing the information system.

2. The General Organizational Structure

CPA is organized as a classic public bank. At the top, there is a board of directors and a general assembly. The bank is headed by a Chairman and Chief Executive Officer (PDG). Four deputy general directorates assist the PDG: one for operations, one for administration and development, one for commitments and foreign affairs, and one for information systems. The bank also has an

internal audit directorate, a regulation and control unit, and two statutory auditors.

The branch network is divided into 15 “exploitation groups” spread across the national territory. These groups supervise about 159 branches (the exact number varies slightly across reports). The Batna branch studied in this thesis belongs to exploitation groups 835.

3. Structure of the Exploitation Group (Group 835)

Within the exploitation group, the organization is more detailed. According to an internal report, the group includes:

- An **exploitation sub-directorate**, which itself contains:
 - A commercial animation unit.
 - A commitments unit, subdivided into a loan study and analysis cell, and a commitments follow-up and statistics cell.
- A legal and disputes cell.
- A foreign trade cell (for assistance, not direct execution).
- An administration and human resources sub-directorate, with:
 - A human resources, training, and social affairs division.
 - A budget and administration division.
 - A logistics and general means division (property management, security, supplies, archives).
 - A general control cell.
 - An IT cell.
 - A secretariat and a registry office.

This structure is essentially administrative and hierarchical. It does not include any dedicated unit for information governance, digital identity, or cyber

risk management. The IT cell is mainly responsible for maintaining hardware and the Delta software, not for designing a digital strategy.

4. Structure of a Branch (Agency 356 or 360)

At the branch level, the organization follows a classic banking model. Internal reports describe three main services:

- The cash desk service: this is the front and back office. It handles deposits, withdrawals, account opening, checks, transfers, clearing, account freezing, and safe rental.
- The credit service: it studies and analyses loan applications, follows up on outstanding loans, collects bad debts, and deals with disputes.
- The control service: it performs the daily accounting, monitors accounts, checks bad checks, and corrects staff errors.

In larger branches, there is also a foreign trade service that deals with domiciliation, documentary credits, documentary collections, exchange operations, and special accounts. However, this service is not present in all agencies.

This branch-level structure shows that accountability and oversight are still based on manual procedures. The control service focuses on accounting and financial correctness, not on data traceability or digital accountability.

5. The Central Information System Division

Beyond the local branch level, CPA has a centralized Information Systems Division located in Algiers. This division is responsible for overseeing the bank's entire IT infrastructure, including software development, network management, production, and telecommunications. Its structure includes several specialized directorates:

- Engineering Directorate.

- Infrastructure Directorat.
- IT Installations and Production Directorat.
- IT Production.
- The automate clearing system.

The division operates from multiple addresses in Algiers, including 78 Avenue Ahmed Ghermoul, Rue Bouzid Bouezid, and Rue Trabouni Belkacem.

This centralized structure shows that IT management is highly concentrated at the headquarters level. Local branches, such as the Batna agency, have only basic IT cells for maintenance and user support. They do not have decision-making power over system design, security policies, or digital strategy. This centralization can be both a strength (uniform standards) and a weakness (slow responsiveness to local needs).

6. Current Information Systems in CPA.

The main information system used in CPA is a software package called **Delta Bank**. According to several internal reports, Delta is used for daily transaction processing, customer account management, credit operations, and domiciliation follow-up. However, the system is widely criticized. One report describes it as “very complex and not practical”. Employees find it difficult to use, and many tasks still require manual processing (arrière-guichet). The software does not support full automation, and it lacks integration with other potential digital tools.

A second tool mentioned is a **scoring system**, used only for real estate loans. It automatically suggests a loan amount based on pre-defined criteria. This system helps frontline staff make quick decisions for simple cases, but it is not connected to a broader digital governance framework.

For international transfers and documentary credits, CPA uses the **SWIFT network**. This is a standard tool in the banking industry. However, no specific information about its configuration or security level appears in the available reports.

For internal communication, the bank relies on traditional methods: meetings, telephone calls, service notes, and physical committees to study loan files. There is no mention of an intranet, a unified email system, or any collaborative digital platform.

One relatively successful digital initiative is the automated clearing system. It allows electronic exchange of checks and operations between banks without the need for physical presence in a clearing room. This system saves time and reduces costs. Yet it remains a limited automation of a single process, not part of a comprehensive digital strategy.

In summary, the current information systems in CPA are fragmented, mostly outdated, and heavily reliant on manual work. The core software (Delta) is complex and inefficient. No integrated system supports information governance, digital identity, or automated accountability.

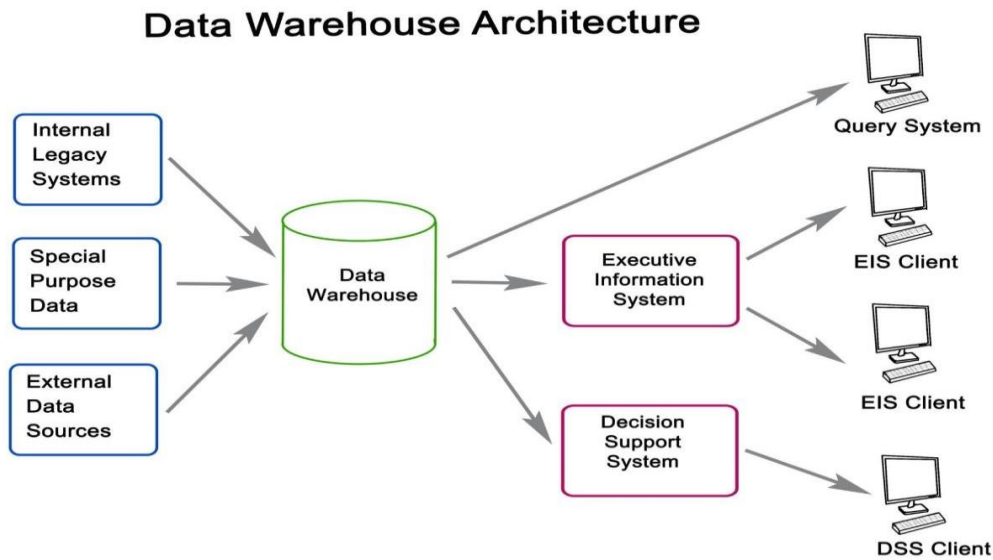


Figure 10: Data Warehouse

Subsection two: Digitalization Tools and Electronic Banking Services at CPA.

1. Core Tools and Services

CPA Bank offers an integrated set of digital tools and services aimed at facilitating banking operations and improving the customer experience:

- a. Mobile CPA Application: The bank's primary digital service platform, providing users with:
 - Access to account balances and transaction history.
 - Location of the nearest branch.
 - Monitoring of balance trends.
 - Currency exchange.
 - Instant transfers to savings accounts.
- b. e-Banking Service: An online electronic banking system that provides a secure and complete environment for customers to perform all their

banking operations remotely, with a focus on high efficiency and fast execution.

- This service includes e-Payment and Electronic Data Interchange (EDI).
- c. e-cp@ Service: An innovative electronic banking service that enables secure online payment by linking the account to CPA CIB bank cards.

2. Advanced Service Tools and Modern Models

The bank offers advanced tools and modern models to cover a variety of needs:

- Wimpay CPA Application (Web App): A web application for electronic payment, with dedicated training content explaining the registration process.
- Specialised Digital Spaces: The bank provides dedicated digital spaces, such as a space for lease-purchase contract holders and the "CPA e-Moussahim" platform for managing stock market buy and sell orders.
- Monétique System: Includes electronic payment solutions and bank cards that ensure service continuity for customers.

3. Infrastructure and Human Resources

To support these digital services, the bank employs approximately 4,451 staff members, who have been directed and trained to deliver professional services.

Section Two: Methodological Framework.

This section presents the methodological framework adopted to answer the research questions. It first outlines the main research variables (independent, dependent, mediating, and moderating) and their operationalisation. It then explains the epistemological foundations (interpretivism), the logic of reasoning (abduction), and the case study strategy. Subsequently, the section details the data collection instruments, analysis procedures (SPSS and NVivo), quality assurance measures, ethical considerations, and methodological limitations.

Subsection One: Research Variables and Epistemological Foundations.

1. Research Variables

- a. Independent Variable (Digital Transformation Strategy): Refers to the degree to which a bank adopts a comprehensive digital strategy that changes its business models, processes, and customer relationships (Bharadwaj et al., 2013; Vial, 2019; Wessel et al., 2021). This variable is measured using four practical indicators: clarity of the digital strategy, alignment with overall business objectives, existence of a dedicated digital transformation budget, and level of adoption of AI and cloud computing technologies (five-point Likert scale). The essence of this variable lies in moving from theory to practice in a context – an Algerian public bank – that has never been empirically tested before.
- b. Composite Dependent Variable (Information Governance, Digital Identity, Digital Accountability, and Digital Sovereignty): Brings together four interrelated concepts that have rarely been examined together in previous literature:
 - Information Governance: policies for data quality, security, and compliance, based on the IGF framework (Faria, Maçada & Kumar, 2013), which provides 14 diagnostic factors that enabled the study to assess gaps between documented policies and actual practice.
 - Digital Identity: biometric and multi-factor authentication technologies (Cameron, 2005; Khattak et al., 2023); measured by the actual availability of such technologies at the CPA Batna branch.
 - Digital Accountability: five core elements from Al-Rashdi et al. (2017) – responsibility, transparency, assurance, remediation, and compliance – selected because they are most relevant to banking and can be translated into measurable indicators (e.g., existence of a responsible person, clarity of audit procedures, compliance reports).

- Digital Sovereignty: full control over where data are stored and the ability to refuse foreign access (Shoker, 2022; Codagnone & Weigl, 2023); measured using practical indicators: storage location, existence of policies preventing foreign access, and the legal department's awareness of such policies.
- c. Mediating Variable (Governance Implementation Mechanisms): Assumes that the impact of digital transformation strategy on outcomes is not direct but operates through mediating mechanisms such as: existence of an IT governance organisational structure, application of the three lines of defence model, frequency of internal audits, and level of stakeholder disclosure.
- d. Moderating Variables (Technical, Organisational, and Regulatory Challenges): These variables strengthen or weaken the relationship between strategy and governance. Based on the literature (Boadu et al., 2025; Mohan, 2016; Diener & Špaček, 2021; DataGuidance, 2025), they include: outdated IT systems and poor infrastructure (technical); untrained staff and resistance to change (organisational); and the absence of detailed regulations from the Bank of Algeria on cloud storage and data localisation (regulatory). Questionnaire and interview questions were designed to capture them directly.

2. Epistemological Foundations and Logic of Reasoning

Because the primary aim is to understand how employees perceive digital transformation strategy and governance in a unique context – and not to produce statistically generalisable laws – the study adopts an interpretivist (Interprétativisme) stance. This position recognises that social and organisational reality is constructed through individuals' interactions and interpretations; therefore, the researcher's task is to uncover these interpretations as they are lived by CPA Batna employees, rather than testing predefined causal relationships.

The logic of reasoning is abductive. The study moves back and forth between theory (the conceptual framework of Chapter One) and the field (interview and questionnaire results) interactively. When unexpected findings emerged – such as the legal department’s zero references to digital sovereignty – the researcher returned to theory to explain this gap, then returned to the field for deeper understanding through additional interviews. This logic is appropriate for exploratory studies dealing with relatively new phenomena.

3. Nature of the Methodology and Research Strategy

The study is quantitative-led with qualitative support. The questionnaire (12 employees) was used for descriptive purposes only (calculating means and standard deviations) and not for hypothesis testing. This decision was made for two reasons: (a) the small sample size does not allow reliable statistical inference; (b) the main focus is on understanding processes and meanings, not on quantitative measurements.

- A single in-depth case study of CPA Batna (Agency 120 / Exploitation Group 835) was chosen because it provided:
- Access to internal information (reports, interviews with key employees) during the internship period (29 March – 29 April 2026);
- Deep understanding of the unique context of an Algerian public bank, rather than a superficial picture of several banks, which aligns with the exploratory purpose of the research.

Subsection Two: Data Collection, Analysis, and Quality Assurance Procedures.

Research design adjustment due to small sample size:

The study was originally designed as a quantitative research project aimed at testing hypotheses through a representative sample. However, because the

number of accessible respondents was limited (only 12 employees from the Batna branch), the quantitative results alone could not be considered sufficiently robust for statistical generalisation. Therefore, I added a qualitative component to complement and confirm the quantitative findings. The quantitative data (from the questionnaire) remain the primary source. They provide descriptive statistics (means, standard deviations, Cronbach's alpha, and an exploratory ANOVA). The qualitative data (semi-structured interviews, direct observation, and documentary analysis) serve a supporting role: they allow me to verify, deepen, and substantiate the statistical results through direct testimonies and on-site observations. Thus, the small sample size does not invalidate the study; rather, the qualitative material offers cross-validation and strengthens the credibility of the conclusions.

1. Data Collection Instruments (Systematic Triangulation)

- Four integrated tools were used to achieve triangulation and enhance credibility:
- Semi-structured interviews: three interviews with employees from the legal, credit, and human resources departments, covering six themes (digital strategy, governance, digital identity, accountability, digital sovereignty, and challenges). Notes were taken immediately after each interview to ensure accuracy while respecting participants' preference not to be audio-recorded.
- Online questionnaire: distributed to 12 employees, containing 12 Likert-scale items (five points) plus two open-ended questions. Designed to capture general perceptions and provide complementary descriptive data.
- Documentary analysis: review of six internal reports concerning the Batna branch, plus technical documents from the Information Systems Directorate (DSI) describing the Delta system and security procedures

(e.g., Active Directory, 2FA, SOC). This helped compare documented policies with actual practices as reported in interviews.

- Direct observation: during the internship, the researcher recorded observations of daily interactions related to digital transformation without interfering in work processes, allowing the detection of gaps between stated views and actual behaviour.

2. Data Analysis (Quantitative and Qualitative)

- Quantitative analysis (SPSS): means and standard deviations for each item, Cronbach's alpha to check internal consistency (0.878), and a one-way ANOVA to explore whether years of experience produced differences in perceptions (all $p > 0.05$, meaning that weak governance affects everyone regardless of seniority). These results are used descriptively only and not for statistical generalisation.
- Qualitative analysis (NVivo and thematic analysis): interview notes, observation notes, and documents were analysed using NVivo 14, following the six steps of Braun & Clarke (2006): (1) familiarisation, (2) generating initial codes, (3) searching for themes, (4) reviewing themes, (5) defining and naming themes, and (6) writing the final analysis. Main nodes were created corresponding to the six study themes, with sub-nodes to capture nuances (e.g., "absence of written policies", "reliance only on Outlook reminders").

3. Research Quality (Lincoln & Guba's Criteria:

The four quality criteria for qualitative research (Lincoln & Guba, 1985) were applied with specific practical procedures:

- Credibility: achieved through data triangulation (interviews, questionnaire, documents, observation). Preliminary summaries were also shared with two participants for member checking to verify the accuracy of interpretations.

- Transferability: a thick description of the CPA Batna branch context (organisational structure, nature of systems, infrastructure challenges) is provided, allowing readers to assess the applicability of findings to similar contexts.
- Dependability: all research steps (from data collection to analysis) were clearly documented in an auditable trail, including coding decisions and theme development.
- Confirmability: a daily reflexive journal was kept to record the researcher's prior assumptions and reflections, ensuring a clear distinction between data description and interpretation and avoiding the imposition of personal views on the findings.

4. Ethical Considerations

- Each participant was informed (in writing via the questionnaire, or orally before interviews) about the nature of the research, voluntary participation, the right to withdraw at any time, and the guarantee of data confidentiality.
- No personal identifiers that could lead to participant identification were collected (pseudonyms were used).
- All data were stored on a password-encrypted computer, accessible only to the researcher and the supervisor.
- Formal authorisation from the CPA Batna branch management was obtained before data collection began.

5. Study Limitations (Explicit Acknowledgment of Weaknesses)

- Generalisability: The study is limited to one branch (Batna) and a small sample (12 questionnaires, 3 interviews). Therefore, results cannot be statistically generalised to other CPA branches or the entire Algerian banking sector. However, generalisation was never the goal; the objective was in-depth understanding (analytical, not statistical, generalisation).

- Technical data: The study relies on employee perceptions without full technical verification of centralised security systems (e.g., SOC, whether 2FA is activated for regular employees), as such information remains under the authority of the central management in Algiers.
- Audio recording: The absence of audio recording (due to participant preferences) may have led to the loss of some subtle details, but notes were transcribed immediately after each interview to minimise this limitation.

After this methodological framework, Chapter Three presents the study's findings. It is divided into two subsections: the first presents descriptive results (SPSS tables, verbatim interview quotations, document summaries) without analytical commentary; the second discusses these results in light of the theories presented in Chapter One, including hypothesis assessment and prioritised practical suggestions.

Chapter III:

Results Presentation, Discussion, and Assessment.

Data were collected from 12 employees through a questionnaire and from three interviews (legal, credit, and human resources). Quantitative data were analysed using SPSS, qualitative data using NVivo, in addition to technical documents from the Information Systems Directorate (DSI) and conversations with the branch's IT engineer. This chapter first presents the numbers and quotations without commentary (first section), then discusses them in light of the research questions and hypotheses (second section).

Section one: Presentation of Field Study Results.

This section presents the empirical findings of the field study conducted at the CPA Batna branch. It is divided into two subsections. The first subsection reports the quantitative results derived from the questionnaire administered to 12 employees, including sample characteristics, reliability of the instrument (Cronbach's alpha), means and standard deviations of the Likert-scale items, and an exploratory analysis of variance (ANOVA) by years of experience. The second subsection presents the qualitative results, consisting of a coding matrix from NVivo, verbatim quotations from the semi-structured interviews, open-ended questionnaire responses, and technical information obtained from internal documents and the branch IT engineer. All results are presented descriptively, without interpretation or theoretical discussion; analysis and interpretation are reserved for Section two of this chapter.

Subsection one: Quantitative Analysis Results.

1. Sample characteristics

Out of 12 employees, 7 were from credit (58.3%), 2 from guarantees (16.7%), 2 from human resources (16.7%), and 1 was unspecified. Years of experience: 3 employees less than 5 years (25%), 7 between 5 and 10 years (58.3%), and 2 more than 10 years (16.7%).

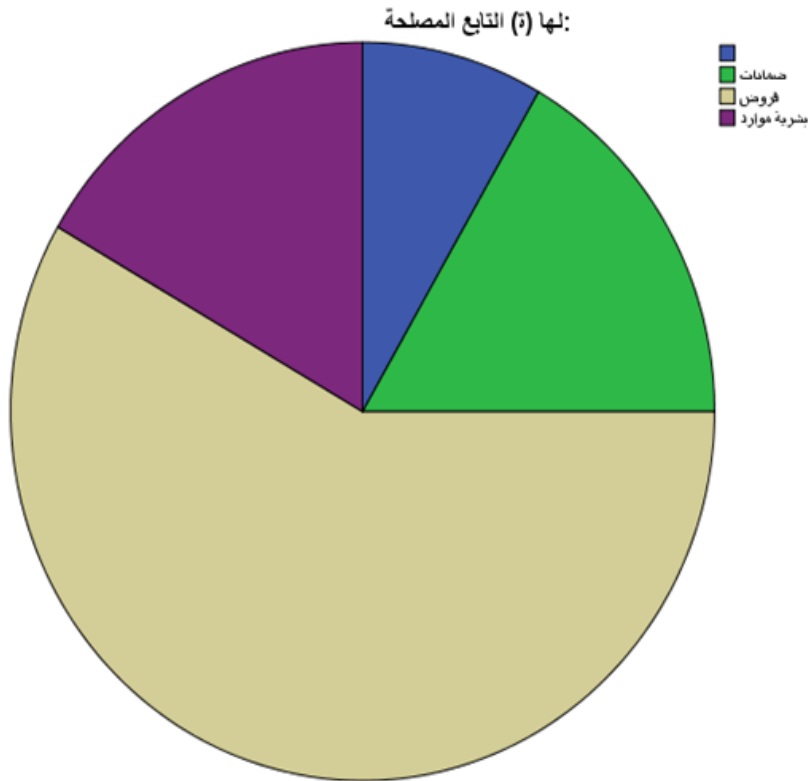


Figure 11: Distribution of respondents by department.

Years of experience: 3 employees less than 5 years (25%), 7 between 5 and 10 years (58.3%), and 2 more than 10 years (16.7%).

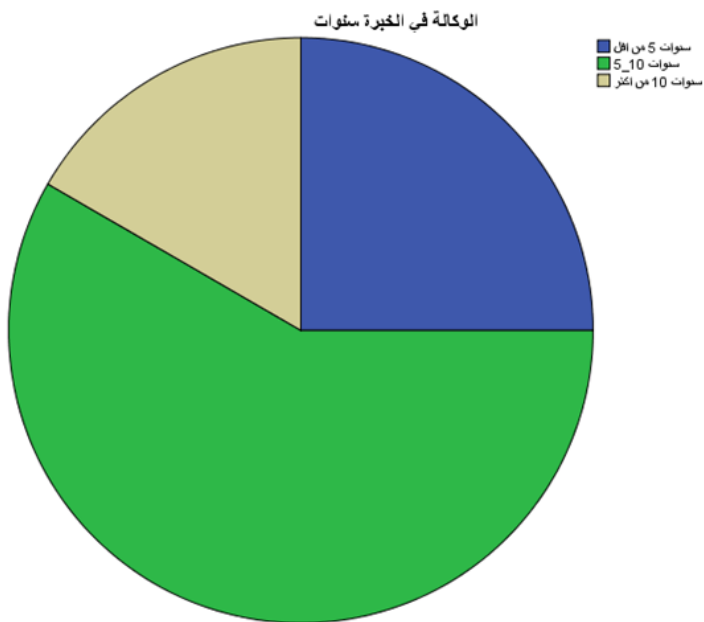


Figure 12: Distribution of respondents by years of experience

2. Reliability of the instrument

Cronbach's alpha for all 12 items: 0.878.

3. Means and standard deviations

Table 4: means and standard deviations

Statement	N	Mean	Std. Dev
The bank has a clear digital strategy.	12	2.75	1.3568
Current systems allow interoperability between departments	12	3.08	1.2401
The system records every operation I perform to trace responsibility	12	3.67	1.3027
When I enter an error, the system immediately warns me and prevents completing the operation	12	3.50	1.0000
The bank relies on software from foreign companies	12	3.25	1.6026
A scanned digital copy is legally acceptable as an original paper document	12	3.00	1.6514
Most employees prefer to work with paper rather than digitalization	12	3.08	1.3790
Logging in with only a password is sufficiently secure for my position	12	3.58	1.0836
Audit procedures are clear and can be implemented from digital records	11	3.09	0.9439
I feel well-qualified in information and digital data security	12	3.00	1.2792
There are written policies regarding data security and confidentiality, and they are effectively applied	12	2.92	1.3114
The technical infrastructure (network, servers, equipment) is reliable and efficient	12	2.91	1.4460

4. ANOVA by years of experience

Values and significance levels:

- Strategy: $F=1.063$, $p=0.385$.
- Interoperability: $F=1.649$, $p=0.245$.
- Transaction logging: $F=0.774$, $p=0.490$.

- Reliance on foreign software: $F=3.031$, $p=0.099$.
- Written policies: $F=3.323$, $p=0.083$.
- Infrastructure reliability: $F=2.729$, $p=0.125$.

As an exploratory supplement to the descriptive statistics, a one-way analysis of variance (ANOVA) was conducted to examine whether years of experience (less than 5 years, 5–10 years, more than 10 years) might be associated with differences in employees' perceptions. Given the small sample size ($N=12$), these results should be interpreted with caution and are not intended for statistical generalization. The table below presents the F-values and significance levels (p-values) for each statement.

Table 5: ANOVA by years of experience

Statement	F	P
The bank has a clear digital strategy	1.063	0.385
Current systems allow interoperability	1.649	0.245
The system records every operation	0.774	0.490
The bank relies on foreign software	3.031	0.099
There are written policies	3.323	0.083
Technical infrastructure is reliable	2.729	0.125

All p-values are above 0.05, meaning that, within the limits of this exploratory analysis, no strong patterns emerged linking years of experience to perceptions. This suggests that the governance gaps observed (e.g., absence of written policies, low audit clarity) are perceived similarly by both new and veteran employees. However, because of the small sample size, the absence of statistical significance does not necessarily imply the absence of real differences; it may simply reflect low statistical power. Therefore, these

ANOVA results are used only as a descriptive complement and not as a basis for inferential claims.

Subsection two: Qualitative Results and Technical Background.

1. Coding matrix (NVivo)

To organize and compare the qualitative data from the three interviews (legal, credit, and human resources), a matrix coding query was generated using NVivo 14. The matrix cross-tabulates the six main themes of the study (digital strategy, information governance, digital identity, accountability and transparency, digital sovereignty, and challenges) against the three participants. Each cell in the matrix contains the number of coding references (i.e., text segments coded to that theme) for that participant. This matrix serves two purposes: first, it provides a transparent overview of which themes were most discussed by each participant; second, it allows a quick visual detection of thematic gaps – notably, the legal participant's zero references to digital sovereignty, which was a critical finding. The matrix is presented below.

Table 6: CODING MATRIX

Node	Credit	Legal	Human Resources
Challenges	1	1	1
Information governance	2	2	2
Digital identity	2	2	2
Digital sovereignty	1	0	2
Digital strategy	3	3	2
Accountability / transparency	2	2	2

One of the most striking findings of this study is the zero reference (0) recorded by the legal department employee regarding digital sovereignty, despite the fact that data are stored locally in Algiers according to other employees. How can this disconnect be explained?

Drawing on Parker & Gilad's (2011) model of the "Three Implementation Nodes", we find that CPA suffers from a disconnection between Node 1 (top management attention and resources) and Node 3 (employee internalisation). The absence of any formal document or circular from senior management on digital sovereignty requirements – itself due to the lack of implementing regulations from the Bank of Algeria – leaves the legal department, despite its pivotal role, entirely out of the loop. This confirms the theoretical proposition that organisational structure alone does not guarantee compliant behaviour without clear communication and accountability mechanisms.

Moreover, this phenomenon can be linked to the concept of "window dressing" compliance (Coglianese & Nash, 2020): the focus may be on displaying "security policies" without actually connecting them to legal departments, creating the illusion of compliance without its substance. Therefore, the recommendation of this study to involve the legal department in digital sovereignty matters is not merely an administrative improvement, but a prerequisite for transitioning from cosmetic to genuine compliance.

The legal participant was the only one who did not refer to digital sovereignty (0). Strategy received three references from credit and legal, and two from human resources.

2. Quotations from interviews

- Digital strategy: When asked whether the bank has a clear digital strategy, responses varied significantly across departments. The credit employee stated: "Yes, the bank has a strategy ... its objective is to improve and speed up operations. We were told that the new Delta Supra system will make things faster." However, the legal department employee gave a contradictory answer: "We were not informed of the existence of a strategy. There is no formal document, and we in legal were never consulted about digital transformation plans." The human

resources employee provided a third perspective: "Yes ... its main objective is speed of execution. But it's not a written document; it's more of an informal direction from the regional management." This divergence suggests that if a strategy exists at all, it has not been formally documented or communicated across all departments.

- Information governance: Regarding written policies for data governance, the legal employee explained: "There are no formal written policies, only reminders via Outlook. When a new instruction about data protection comes, we get an email, but there is no signed policy document that everyone can refer to." The human resources employee confirmed: "Policies are sent as notifications via Outlook, not formal documents. I have never seen a printed or signed data governance policy. Employees are expected to follow email instructions, but nothing is binding or traceable." This absence of formal, written policies leaves the bank without a clear governance framework.
- Digital identity: On customer and employee authentication, the credit employee stated: "There is no fingerprint, there is a code (ID number), and accounts cannot be opened remotely. The only thing we have is a password. If a customer forgets it, they must come to the branch." The human resources employee added: "Recognition is by name, surname, and a code in Delta. No biometrics. For employees, we also use simple passwords. I have heard of two-factor authentication, but it is only for managers, not for regular staff." This confirms that digital identity remains at a primitive stage, relying entirely on password-based authentication.
- Accountability and transparency: When asked about traceability of operations, the credit employee said: "I don't know if operations are recorded, but the system warns when there is an error. It stops me from completing a transaction if something is wrong. But I cannot see who

accessed a customer file before me – that information is not visible to us." The human resources employee added: "Access to view records is limited, not for everyone. Only certain people can see audit logs. I think the system records everything, but regular employees cannot access those logs. There is no dashboard or simple report for us." This indicates that while technical logging exists (mean 3.67), transparency mechanisms are weak (audit clarity mean 3.09), and ordinary staff are excluded from reviewing logs.

- Digital sovereignty: Regarding data storage location, the human resources employee stated: "Data is stored on a central server and intranet, no external cloud. Everything is inside the bank's own network, I believe." The credit employee confirmed: "Stored centrally (data center). I think it is in Algiers, at the head office." However, the legal employee admitted: "I have no idea where data is stored. This is not something legal was asked about. We assume it is local, but I cannot confirm." This reveals that even when data are stored locally (a positive finding), the legal department is entirely disconnected from sovereignty matters – a critical governance gap.
- Challenges: Summarising the main difficulties facing digital transformation, the human resources employee said: "The customer resists change, the system is inefficient, lack of competencies and infrastructure problems. Many employees still prefer paper. The network is slow, and the Delta system crashes sometimes. Also, there is no training – only one person per department gets trained, then they have to teach others."

3. Open-ended questions in the questionnaire

Most demands: system integration, eliminating paper, faster network speed. Optimism about "Delta Supra": mostly medium to high, except one low.

4. Technical information (DSI documents + branch engineer)

- Core system: Delta Supra V11 (multi-channel). The older version V07 is still partially used.
- Security: Active Directory, password change every two months, 2FA for remote administrative access, SOC and **Wazuh** platform, Business Continuity Plan (BCP).
- Branch engineer's note: these systems are documented and partially implemented, but frontline staff are not aware of them.

Section two: Discussion of Results.

After presenting the descriptive results – both quantitative (SPSS tables) and qualitative (NVivo coding matrix, verbatim quotations, and technical background) – in the previous section, this section moves from pure description to analytical interpretation. The discussion is organised around the three research sub-questions and the three hypotheses formulated in the general introduction. Each sub-question is answered by integrating quantitative and qualitative evidence, and each hypothesis is tested by comparing theoretical expectations with field findings. The discussion then addresses unexpected results, compares the findings with previous studies, and concludes with prioritised practical suggestions for the CPA Batna branch and for the regulatory authorities (the Bank of Algeria and ANPDP) regarding issues that directly affect this branch.

Subsection one: Answering Sub-Questions and Testing Hypotheses.

1. Strategic components and possibility of integration (sub-question 1)

Mean strategic clarity is 2.75/5. While credit and HR employees confirmed the existence of a digital direction, they described operational tools (Delta Supra migration, DocuWare, Outlook reminders) rather than a formal document. The legal employee stated he was never informed of any strategy.

This triangulated evidence points not to the total absence of digital activity, but to the absence of a formally documented, institutionalised, and cross-departmentally communicated digital strategy. This means that if a strategy exists at all, it has not been communicated to all department; The contradiction between the credit/HR employees' affirmative answers and the legal employee's denial is not a simple misunderstanding. It indicates that the 'strategy' known to operational staff (credit, HR) is likely an informal set of directions – perhaps related to the Delta Supra migration – rather than a formally documented, board-approved digital strategy. The legal department's ignorance is particularly telling because any formal strategy would require legal review; its absence from legal's awareness strongly suggests that no such document exists. Moreover, the policies mentioned (Outlook reminders) are not formal documents.

According to the IGF framework (Faria, Maçada & Kumar, 2013), the absence of formal policies and clear accountability makes it impossible to integrate governance, identity, accountability and sovereignty. These concepts cannot be merged into a coherent framework before policies become written, binding and known to everyone.

2. Role of data governance and accountability in enhancing sovereign decision-making (sub-question 2)

10 out of 12 agreed that operations are logged (mean 3.67), but audit clarity was low (3.09). The credit employee said he does not know whether operations are recorded. Logs exist technically, but they are not transparent to users. The problem is not technological but organizational. The system is capable of logging; what is missing is an interface that translates raw logs into a readable audit trail for non-IT staff. The credit employee's statement "I don't know if operations are recorded" is the clearest evidence of this interface gap. From a governance perspective, resources spent on advanced logging without

a corresponding investment in transparency tools are partially wasted. Moreover, the legal department – which should ensure compliance with sovereignty regulations – had zero references to digital sovereignty (0).

According to Al-Rashdi et al. (2017), accountability requires transparency and assurance. Without employees (especially legal) being able to see and understand audit logs, technical logging cannot enhance sovereign decision-making. The gap is not the existence of logging but its unavailability in an intelligible form.

3. Current state and actual challenges (sub - question 3)

- Written policies: 2.92 (below neutral). Qualitative confirmation: "only Outlook reminders". Not a single formal document.
- Digital identity: no fingerprint, no remote account opening, reliance on a code (ID number). approximately 10 out of 12 respondents were neutral or agreed that a password alone is sufficient.

Accountability: logging exists but is opaque, and legal is not involved.

- Data storage: local (central server) – positive – but legal "has no idea".
- Challenges: HR mentioned customer resistance, weak systems, lack of competencies. Credit and legal mentioned none (zero or one reference).
- Actual challenges:
- Organizational: no governance unit, limited training (one employee per department), resistance to digitalization (mean paper preference 3.08).
- Technical: infrastructure reliability 2.91, fragmentation between V07 and V11.

- Regulatory: The Bank of Algeria has not issued clear regulations on cloud and data localization (DataGuidance, 2025;Radio Algérienne, 2024).

4. Hypothesis testing

- H1 (Integrated governance enhances digital identity): Accepted. Absence of policies (mean 2.92) and lack of knowledge about who is responsible for data security (interviews) is associated with primitive identity and weak security awareness (3.58). The link is direct.
- H2 (Effective accountability ensures transparency): Partially accepted. Logging exists (3.67), but lack of transparency (3.09) and the credit employee's unawareness show that effectiveness is missing. Specifically: the technical dimension is confirmed (logging exists, mean 3.67), whereas the organisational dimension is not met (audit transparency mean 3.09; the credit employee stated he does not know whether operations are recorded; the legal department had zero references to sovereignty-related oversight). That is, current mechanisms are not effective, not that accountability is useless. As an assessment, the partial acceptance is actually the most instructive outcome: it confirms the theoretical proposition (accountability mechanisms can ensure transparency) while revealing that the bank has not yet implemented such mechanisms. The failure is not in the theory but in the practice. If CPA were to build a simple audit dashboard, the same logging infrastructure could become a transparency tool overnight.

Therefore, it is recommended to prioritise this over more complex security investments. This finding aligns with the IGF framework proposed by Faria, Maçada & Kumar (2013), which posits that clear policies (the 'Policies' dimension) are a prerequisite for accountable information management. The absence of formal written policies at CPA

directly violates this principle, confirming that without a documented framework, even basic governance mechanisms cannot function effectively.

- H3 (Sovereignty is hindered by technical and organizational challenges): Fully accepted. Infrastructure reliability 2.91, reliance on foreign software 3.25, absence of policies, and legal's absence from sovereignty. Local storage exists but legal does not know about it, and regulations are incomplete.

5. Comparison with previous Algerian studies

The findings of this study contrast with several macro-level Algerian studies. Taleb, Slimani & Bennouna (2025) used multiple linear regression (2010–2023) to evaluate the impact of digitalisation on Algerian banking performance and found that digital banking services contribute to profitability at the macroeconomic level. While their study suggests a positive aggregate effect, the present micro-level investigation at CPA Batna reveals a different picture. At the branch level, digital transformation is severely hampered by the absence of written data governance policies (mean 2.92), weak accountability mechanisms (audit clarity mean 3.09), and the exclusion of the legal department from digital sovereignty matters (0 references). This divergence indicates that positive macro-level performance indicators may mask persistent governance and accountability gaps at the operational level – a critical insight that only a micro-level qualitative case study can uncover.

Similarly, Khaoui (2025) conducted a case study of digital transformation at the National Bank of Algeria (BNA) and concluded that the bank has made significant progress in implementing digital technology. However, the study focused on service quality rather than on governance frameworks, digital identity, or accountability. The present study complements Khaoui's findings by showing that even in a public bank that has invested in technical

infrastructure (Delta Supra V11, SOC, 2FA for managers), governance fundamentals – formal policies, legal involvement, transparent audit trails – may still be absent.

Khelalfa (2025) assessed the impact of AI-driven digital transformation on the Algerian economy (2015–2024) and found significant legislative progress (Law No. 23-09) but also structural challenges: weak banking localisation of digitisation and a sharp increase in cybersecurity incidents. The present study adds a micro-level dimension to Khelalfa's macroeconomic analysis by documenting that at the branch level, the absence of written governance policies and the legal department's unawareness of sovereignty constitute concrete operational manifestations of those structural challenges.

Subsection two: Explaining Unexpected Findings, Limitations and Suggestions.

1. Unexpected findings

- Legal department and data sovereignty (0 reference): Not a lack of competence, but evidence that the bank has not involved the legal department in sovereignty matters. Possibly due to the absence of central bank instructions, or because management treats sovereignty as a purely technical issue. This zero reference is, it is considered, the most alarming finding of the entire study.

It means that the bank is potentially non-compliant with Algeria's Law 25-11 without knowing it. The legal officer cannot monitor data breaches, cannot advise on cloud contracts, and cannot prepare compliance reports – because he has never been asked to. This can be understood as a structural governance failure: digital transformation has been delegated solely to the IT department, bypassing legal and compliance functions entirely. Until this is reversed, any claim to 'digital sovereignty' is hollow.

- High agreement on logging (83%) together with low audit clarity (3.09): Not a contradiction in answers, but confusion between the existence of technical logs (understood by IT) and making those logs available in an intelligible format for ordinary employees and legal staff. The system logs, but there is no interface to review those logs.
- No differences by experience (ANOVA): Means that the weak governance state affects everyone regardless of seniority. New and veteran employees face the same ambiguity and the same absence of policies.

2. Study limitations

- 12 questionnaires and 3 interviews do not allow generalizing results beyond the Batna branch.
- Convenience (non-random) sample; the more interested may have participated.
- Single-branch case study – cannot compare with other branches.
- Reliance on employee perceptions without technical verification of SOC or 2FA effectiveness.
- No interviews with central DSI staff; technical information came from documents and an informal conversation with the branch engineer.
- No audio recording of interviews may have led to loss of some detail, but notes were written immediately.

4. Practical suggestions (based on specific results)

Before listing the suggestions, it is noted that not all gaps have the same weight. The analysis identifies two gaps are foundational and must be addressed first: (a) the absence of a formally documented, institutionalised, and cross-departmentally communicated digital strategy, and (b) the complete exclusion of the legal department from

sovereignty affairs. Without these two, other measures (2FA, audit dashboard, training) will remain isolated technical fixes rather than parts of a coherent governance framework. Therefore, I propose the following order of priority, starting with the most urgent.

- Formalise and institutionalise the digital strategy: Since two out of three interviewed departments described only informal operational tools (Delta Supra, DocuWare, Outlook reminders) when asked about the strategy, and the legal department was never informed of its existence (mean strategic clarity 2.75/5), a formal written strategy document must be drafted, endorsed at board level, reviewed by the legal department, and distributed to all departments as a binding instrument.
- Implement multi-factor authentication for all employees: Because 10 out of 12 employees consider a password alone sufficient (mean 3.58), 2FA must be enforced for everyone, not only managers.
- Create an internal audit dashboard: Because logging exists (3.67) but transparency is low (3.09), a dashboard should present operation logs in a simplified format to employees (especially legal).
- Mandatory training for all employees: Since current training is limited to one employee per department (according to interviews), monthly courses on information security and using the new system should be generalized.
- Involve the legal department in sovereignty affairs: Because the legal officer had zero references to sovereignty, a legal officer should be formally assigned to monitor data protection regulations (Law 18-07 and 25-11) and prepare periodic compliance reports.
- Complete the migration to Delta Supra V11: Because the old system V07 is still partially used (according to DSI documents), a final decommissioning date should be set, together with a written user manual.

4. Future research directions

- Apply the same questionnaire and interviews in other branches (Constantine, Oran) to see whether the gaps are specific to Batna or general.
- Conduct a technical audit (in coordination with DSI) to verify the actual activation of SOC and 2FA.
- A comparative study with a private Algerian bank to see whether these problems are typical of the public sector.

this chapter has shown that the CPA Batna branch suffers from the absence of a formally documented, institutionalised, and cross-departmentally communicated digital strategy (mean 2.75 and contradictions in interviews), from the absence of written governance policies (mean 2.92 and only Outlook reminders), and from primitive digital identity (no fingerprint, no remote account opening, with 81.9% considering a password sufficient). Although transaction logging exists (3.67), audit procedures lack transparency (3.09). The legal department is completely disconnected from the digital sovereignty file (0 references). The results supported the three hypotheses. Suggestions were made based on specific gaps. The general conclusion of the thesis will be built on these findings.

A reflection on the entire chapter reveals a paradox: CPA Batna has invested in relatively advanced technical infrastructure (Delta Supra V11, documented SOC, 2FA for managers), yet it has neglected the basic governance building blocks – written policies, legal involvement, and transparent audit trails. This suggests a mindset that treats digital transformation as an IT project rather than an organizational change initiative. In my view, the bank's leadership should reallocate resources from 'shiny new technology' to 'boring but essential governance' – starting with a one-page strategy document and a monthly legal-IT meeting. Without such a shift, the technical investments will continue to underperform.

6. Suggestions for regulatory authorities (Bank of Algeria and ANPDP)

Based on the findings of this study – particularly the legal department’s zero awareness of digital sovereignty (0 references) and the absence of formal written policies – the following suggestions are addressed to the monetary and regulatory authorities:

Issue clear implementing regulations for cloud storage and data localisation: The Bank of Algeria should publish detailed regulations specifying the conditions under which banking data may be stored on cloud servers, the requirements for data localisation, and the legal mechanisms for responding to foreign authorities' requests for customer data. This would transform the current regulatory ambiguity (DataGuidance, 2025) into enforceable legal sovereignty.

Provide practical guidelines and model documents: ANPDP, in coordination with the Bank of Algeria, should develop and disseminate practical guidelines for banks, including model documents such as data protection policies, consent forms, breach reporting procedures, and simplified compliance checklists – particularly for public banks with limited resources.

Strengthen coordination between the Bank of Algeria and ANPDP: Ensure that data protection obligations under Law No. 18-07 (as amended by Law No. 25-11) and monetary regulations on cloud computing are fully aligned, avoiding contradictory requirements. Joint circulars or guidance notes would help banks navigate compliance more effectively.

Launch awareness and training campaigns for the banking sector: ANPDP and the Bank of Algeria should organise sector-wide workshops and training sessions on digital sovereignty, data governance, and accountability, targeting not only IT departments but also legal and compliance functions, which were found to be disconnected from these issues at CPA Batna.

General conclusion

The digital transformation of the Algerian banking sector places growing demands on institutional governance. This study focused specifically on the CPA Batna branch and was driven by a central question: how can this branch formulate and implement a digital transformation strategy that genuinely integrates IT governance, digital identity, digital accountability, and digital sovereignty? The CPA Batna branch (Agency 120 / Exploitation Group 835) provided the concrete field in which this question was examined during the internship period from 29 March to 29 April 2026.

The findings reveal an instructive paradox that carries important lessons for the sector. CPA Batna has demonstrated a genuine commitment to digital progress through tangible technical investments — the Delta Supra V11 core banking system, a Security Operations Centre, and two-factor authentication for senior management. These achievements confirm that the bank possesses the technological foundation upon which a complete governance framework can be built. What remains to be developed is the institutionalisation of this progress: formalising the digital direction into a cross-departmental strategy document (mean strategic clarity 2.75/5), translating Outlook-based policy reminders into signed governance instruments (mean 2.92/5), extending authentication beyond passwords to all frontline staff, and making existing technical audit logs accessible to non-IT stakeholders (audit transparency mean 3.09/5 against logging mean 3.67/5).

The most significant finding concerns the legal department's structural distance from digital sovereignty decisions — not as a failure of competence, but as a reflection of the absence of implementing regulations from the Bank of Algeria on cloud storage and data localisation. Where data are stored locally and securely (CPA's central servers in Algiers), the governance architecture needed to protect and legitimise that sovereignty simply awaits formalisation. Closing this gap — by involving the legal department in governance decisions

and by seeking clearer regulatory guidance — would convert CPA Batna's existing technical assets into genuine sovereign infrastructure.

In response, this study formulates prioritised suggestions. For the CPA Batna branch: endorse a formal written digital strategy and distribute it across all departments; formally integrate the legal department into sovereignty and data governance decisions; extend multi-factor authentication to all employees; and develop an audit dashboard that renders existing logs intelligible to all stakeholders. Regarding the regulatory environment: the absence of clear Bank of Algeria implementing regulations on cloud computing and data localisation was identified as a direct constraint on the branch's ability to formalise its sovereignty posture, and this gap warrants attention by the competent authorities.

This study contributes to filling a documented gap in the Arabic and North African academic literature by providing a field-based simultaneous diagnosis of information governance, digital identity, digital accountability, and digital sovereignty at the CPA Batna branch. Its core message is ultimately one of opportunity: the CPA Batna branch has already made the harder investment — the technology. What remains is the governance architecture that will make that technology sovereign, accountable, and trustworthy. For CPA Batna to fulfil its mandate as a modern public bank, the institutionalisation of that architecture — through written policies, legal involvement in sovereignty decisions, and transparent audit mechanisms — must be the immediate next step.

References

Books

Cameron, K. (2005). The laws of identity. Microsoft Corporation.

Creswell, J. W. (2014). Research design: Qualitative, quantitative, and mixed methods approaches (4th ed.). SAGE Publications.

IT Governance Institute. (2003). Board briefing on IT governance. ITGI.

Lincoln, Y. S., & Guba, E. G. (1985). Naturalistic inquiry. SAGE Publications.

Mohan, A. (2016). Digital transformation challenges in developing economies: Infrastructure, skills, and regulatory gaps. Routledge.

Peterson, R. (2004). Integration strategies and tactics for information technology governance. In W. Van Grembergen (Ed.), Strategies for information technology governance (pp. 37–80). IGI Global.

Van Grembergen, W., & De Haes, S. (2009). Enterprise governance of information technology: Achieving alignment and value. Springer.

Weill, P., & Ross, J. W. (2004). IT governance: How top performers manage IT decision rights for superior results. Harvard Business School Press.

Journal Articles

Al-Rashdi, Z., Dick, M., & Storey, I. (2017). Core elements in information security accountability in the cloud. In C. Valli (Ed.), Proceedings of the

- 15th Australian Information Security Management Conference (pp. 125–131). Edith Cowan University. <https://doi.org/10.4225/75/5a84f2e4b3f7a>
- Bharadwaj, A., El Sawy, O. A., Pavlou, P. A., & Venkatraman, N. (2013). Digital business strategy: Toward a next generation of insights. *MIS Quarterly*, 37(2), 471–482. <https://doi.org/10.25300/MISQ/2013/37:2.3>
- Boadu, R. O., Adu, V. W., & Boadu, K. A. O. (2025). Examining frameworks, policies, and strategies for effective information governance in healthcare organizations. *PLOS ONE*, 20(7), Article e0327496. <https://doi.org/10.1371/journal.pone.0327496>
- Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, 3(2), 77–101. <https://doi.org/10.1191/1478088706qp063oa>
- Codagnone, C., & Weigl, L. (2023). Leading the charge on digital regulation: The more, the better, or policy bubble? *Digital Society*, 2(1), Article 4. <https://doi.org/10.1007/s44206-023-00033-7>
- Diener, F., & Špaček, M. (2021). Digital transformation in banking: A managerial perspective on barriers to change. *Sustainability*, 13(4), Article 2032. <https://doi.org/10.3390/su13042032>
- Elliott, K., et al. (2022). Know your customer: Balancing innovation and regulation for financial inclusion. *Data & Policy*, 4, Article e34. <https://doi.org/10.1017/dap.2022.23>
- Faria, F. A., Maçada, A. C. G., & Kumar, K. (2013). Information governance in the banking industry. *Business Process Management Journal*, 19(1), 117–132. <https://doi.org/10.1108/14637151311294883>

- Goodell, G., Al-Nakib, H., & Tasca, P. (2021). A digital currency architecture for privacy and owner-custodianship. *Future Internet*, 13(5), Article 130. <https://doi.org/10.3390/fi13050130>
- Gurumurthy, A., & Chami, N. (2021). Toward a global digital constitutionalism: A radical new agenda for UN75. *Development*, 64(1–2), 29–38. <https://doi.org/10.1057/s41301-021-00287-z>
- Khattak, M. A., Ali, M., Azmi, W., & Rizvi, S. A. R. (2023). Digital transformation, diversification and stability: What do we know about banks? *Economic Analysis and Policy*, 78, 122–132. <https://doi.org/10.1016/j.eap.2023.03.004>
- Kooper, M. N., Maes, R., & Roos Lindgreen, E. E. O. (2011). On the governance of information: Introducing a new concept of governance to support the management of information. *International Journal of Information Management*, 31(3), 195–200. <https://doi.org/10.1016/j.ijinfomgt.2010.05.009>
- Munira, M. S. K. (2025). Digital transformation in banking: A systematic review of trends, technologies, and challenges. SSRN Working Paper. <https://ssrn.com/abstract=5161354>
- Pearson, S., et al. (2012). Accountability as a way forward for privacy protection in the cloud. In S. Fischer-Hübner, S. Katsikas, & G. Quirchmayr (Eds.), *Trust, Privacy and Security in Digital Business* (pp. 131–142). Springer. https://doi.org/10.1007/978-3-642-32287-7_11
- Naimi-Sadigh, A., Asgari, T., & Rabiei, M. (2021). Digital transformation in the value chain disruption of banking services. *Journal of the Knowledge Economy*, 12(3), 1212–1242. <https://doi.org/10.1007/s13132-020-00655-7>

- Shoker, A. (2022). Digital sovereignty strategies for every nation. *Applied Cybersecurity & Internet Governance*, 1(1), 1–17. <https://doi.org/10.5604/01.3001.0016.0943>
- Simuni, G., & Atla, A. (2023). The role of AI and machine learning in optimizing cloud migration processes. SSRN Working Paper. <https://doi.org/10.2139/ssrn.4982496>
- Stürmer, M., Nussbaumer, P., & Stöckli, P. (2021). Security implications of digitalization: The dangers of data colonialism and the way toward sustainable and sovereign management of environmental data. *ResearchGate preprint*. <https://doi.org/10.13140/RG.2.2.24791.80807>
- Teece, D. J., Pisano, G., & Shuen, A. (1997). Dynamic capabilities and strategic management. *Strategic Management Journal*, 18(7), 509–533. [https://doi.org/10.1002/\(SICI\)1097-0266\(199708\)18:7<509::AID-SMJ882>3.0.CO;2-Z](https://doi.org/10.1002/(SICI)1097-0266(199708)18:7<509::AID-SMJ882>3.0.CO;2-Z)
- Tretter, M. (2022). Sovereignty in the digital and contact tracing apps. *Digital Society*, 1(1), Article 2. <https://doi.org/10.1007/s44206-022-00030-2>
- Vial, G. (2019). Understanding digital transformation: A review and a research agenda. *The Journal of Strategic Information Systems*, 28(2), 118–144. <https://doi.org/10.1016/j.jsis.2019.01.003>
- Wessel, L., Baiyere, A., Ologeanu-Taddei, R., Cha, J., & Blegind Jensen, T. (2021). Unpacking the difference between digital transformation and IT-enabled organizational transformation. *Journal of the Association for Information Systems*, 22(1), 102–129. <https://doi.org/10.17705/1jais.00655>
- Zuo, W., Strauss, J., & Zuo, S. (2021). The effects of digital identity on customer loyalty and satisfaction in banking. *Journal of Financial*

Services Marketing, 26, 89–102. <https://doi.org/10.1057/s41264-021-00093-3>

Theses and Dissertations

Khaoui, S. (2025). *Digital transformation at the National Bank of Algeria (BNA): A case study on service quality and technology adoption* [Master's thesis, University of Algiers].

Sewpaul, S. (2018). *Digital strategies senior bank executives in Mauritius use to improve customer service* [Doctoral dissertation, Walden University]. ProQuest Dissertations & Theses (No. 10977634).

Reports and Institutional Documents

Banque d'Algérie. (2023). *Stratégie nationale de paiement – Vers une société sans espèces d'ici 2028*. Banque d'Algérie.

Banque d'Algérie. (2025). *Instruction n° 02-25 du 2 mars 2025 relative aux conditions et modalités d'agrément et de fonctionnement des banques numériques*. Banque d'Algérie.

EY. (2025). *EY Canada Open Banking Survey: Consumer trust and data control*. Ernst & Young. https://www.ey.com/en_ca

Financial Technology Association. (2025). *Harris Poll survey: Consumer control over financial data in 2025*. <https://financialtechnologyassociation.org>

Institute of Internal Auditors. (2020). *The IIA's three lines model: An update of the three lines of defense*. The IIA. <https://www.theiia.org/globalassets/documents/resources/the-iias-three-lines-model-an-update-of-the-three-lines-of-defense-july-2020/three-lines-model-updated-english.pdf>

Ministère des Finances, Algérie. (2026). *Classification du système bancaire algérien*. Ministère des Finances.

PricewaterhouseCoopers. (2025). *Global Compliance Survey: Top benefits of technology in compliance*. PwC. <https://www.pwc.com>

Research and Markets. (2026). *Data sovereignty cloud market forecast (2026–2030)*. <https://www.researchandmarkets.com/reports/6191053>

Legal Texts

Loi n° 18-07 du 10 juin 2018 relative à la protection des personnes physiques dans le traitement des données à caractère personnel. *Journal Officiel de la République Algérienne Démocratique et Populaire*.

Ordonnance n° 25-11 modifiant et complétant la loi n° 18-07 relative à la protection des données à caractère personnel. (2025). *Journal Officiel de la République Algérienne Démocratique et Populaire*.

Banque d'Algérie. (2024). *Règlement n° 24-64 du 28 octobre 2024 relatif aux conditions d'agrément et de fonctionnement des banques numériques*. *Journal Officiel de la République Algérienne Démocratique et Populaire*.

Online Sources

CMS Law. (2025). *Algeria: New data protection law amendment (Law No. 25-11) and its impact on financial institutions*. <https://cms.law/en/dza/>

DataGuidance. (2025). *Algeria: ANPDP enforcement and amendments to Law 18-07*. <https://www.dataguidance.com>

- Khelalfa, Y. (2025). Impact of AI-driven digital transformation on the Algerian economy (2015–2024): Legislative progress and structural challenges. *Journal of North African Economics*, 12(3), 45–67.
- Khoukhi, M. (2025). *Les banques numériques en Algérie: Cadre réglementaire et initiatives locales*. Les Enjeux de l'Économie Algérienne. <https://www.enjeux.dz>
- Radio Algérienne. (2024). *Retard de la Banque d'Algérie dans la publication des règlements sur le cloud computing bancaire*. <https://www.radioalgerie.dz>
- Taleb, A., Slimani, N., & Bennouna, M. (2025). L'impact de la digitalisation sur la performance bancaire algérienne (2010–2023): Une approche par régression linéaire multiple. *Revue Algérienne d'Économie et Management*, 14(2), 33–52.
- CFPB. (2024). Personal Financial Data Rights Rule. <https://www.consumerfinance.gov/rules-policy/final-rules/personal-financial-data-rights/>.
- FATF. (2023). Guidance on a risk-based approach for virtual assets. <https://www.fatf-gafi.org>.
- AHIMA. (2020). Information governance: Principles for healthcare. American Health Information Management Association. <https://www.ahima.org>
- Arab, M. (2025). New anti-money laundering and counter-terrorism financing law in Algeria: Implications for the banking sector. *Revue Algérienne de Droit et d'Économie*, 8(1), 12–28.
- Axelos/PeopleCert. (2019). ITIL 4 foundation. AXELOS Global Best Practice.

Barry, T. (2020). Electronic banking governance: Frameworks, policies, and regulatory compliance in emerging markets. *Journal of Banking Regulation*, 21(3), 215–230. <https://doi.org/10.1057/s41261-019-00110-3>

Bughrara, S. S., et al. (2025). A systematic review of digital transformation strategies in commercial banks. *Financial Innovation*, 11(2), 1–34. <https://doi.org/10.1186/s40854-025-00651-7>

Coglianese, C., & Nash, J. (2020). Compliance management and regulation: Moving from cosmetic to genuine compliance. *University of Pennsylvania Law Review*, 168(4), 885–940.

Corporater. (2025). Regulatory risks of IT vendor concentration in the banking sector. <https://corporater.com/regulatory-risk-vendor-concentration>

ETH Zurich. (2025). The splinternet and digital sovereignty: Geopolitical fragmentation of cyberspace. ETH Zurich Digital Society Initiative. <https://ethz.ch/en/the-eth-zurich/digital-society-initiative.html>

Futurum Group. (2025). Cloud sovereignty and the fragmentation of global digital infrastructure. <https://futurumgroup.com/insights/cloud-sovereignty>

GetFocal. (2025). RegTech adoption in financial services: Automating compliance to reduce costs. <https://getfocal.com/regtech-compliance-automation>

Ibáñez Zapata, A. (2017). Accountability and transparency in digital banking: Governance frameworks for the information age. *Journal of Information Systems and Technology Management*, 14(2), 203–218. <https://doi.org/10.4301/S1807-17752017000200004>

International Banker. (2025). Hybrid cloud strategies in global banking: Balancing sovereignty and scalability. <https://internationalbanker.com/technology/hybrid-cloud-banking-2025>

Rose, P. S., & Hudgins, S. C. (2012). Bank management and financial services (9th ed.). McGraw-Hill.

ISACA. (2019). COBIT 2019 framework: Governance and management objectives. ISACA. <https://www.isaca.org/resources/cobit>

Moody's. (2025). EU data union strategy and its implications for the financial sector. Moody's Analytics. <https://www.moody's.com/insights/data-union-strategy>

Obaid, A. (2025). The role of AI-powered controls and maturity in retail banking digital transformation: A systematic review (2015–2025). SSRN Working Paper. <https://ssrn.com/abstract=5198423>

Parker, C., & Gilad, S. (2011). Internal corporate compliance management systems: Structure, culture and agency. In C. Parker & V. L. Nielsen (Eds.), *Explaining compliance: Business responses to regulation* (pp. 170–199). Edward Elgar.

Patil, S., et al. (2025). Data sovereignty in the financial sector: A systematic review. *Journal of Data and Information Quality*, 17(1), 1–38. <https://doi.org/10.1145/3702631>

Ramesh, B., et al. (2022). Digital accountability frameworks: Governance, audit, and transparency in banking institutions. *International Journal of Accounting and Information Management*, 30(3), 395–416. <https://doi.org/10.1108/IJAIM-09-2021-0185>

Slitani, K. (2025). Digital banking regulation in Algeria: Current framework and future prospects. *Revue des Sciences Commerciales*, 24(1), 77–92.

Widharto, H., et al. (2020). Digital transformation in banking: Drivers, challenges, and strategic implications. *Asia Pacific Journal of Management and Technology*, 1(2), 14–26. <https://doi.org/10.46977/apjmt.2020v01i02.003>

Appendices

Appendix A: Interview Guide

Digital Transformation Strategy, Information Governance,
Digital Identity, Accountability and Sovereignty — CPA Batna

Introduction

I am a research student at ENSM, conducting a study on digital transformation at CPA. This interview will take approximately 30_45 minutes. Your information is confidential and your name will not be mentioned.

Do you consent to having this conversation recorded?

Yes no

Participant Information (10 minute)

Position	
Department	
Years of Experience	

Interview Questions (30_45 minutes)

1. Digital Transformation Strategy

- Does the bank have a clear digital transformation strategy? What are its main objectives?
- Who makes the major decisions regarding technology investments?

2. Information Governance

- Are there written policies for collecting, storing, and protecting customer data?
- Who is responsible for data quality and security? Is there any employee training on data governance?

3. Digital Identity

- How does the bank identify and authenticate its customers online? (biometrics, code, application?)
- Can new accounts be opened remotely? How is identity verified?

4. Accountability and Transparency

- Is every access to or modification of customer data recorded?
- How is the responsible party identified in the event of an error or data breach?

5. Digital Sovereignty

- Where is the bank's data stored — locally or abroad?
- Does the bank use foreign cloud services (e.g., Microsoft, Google)?

6. Challenges and Future Outlook

- What are the three main difficulties facing digital transformation at the bank?
- What is the most urgent improvement needed to strengthen information governance and digital sovereignty?

Closing

Thank you very much for your time. Is there anything you would like to add?
May we contact you later for clarification if needed?

Researcher's Notes (post-interview)

Appendix A2: Interview Guide — Axes and Key Questions

Semi-structured Interview | CPA Batna Branch | ENSM Master's Dissertation 2025/2026

Axe	Theme / محور	Key Question	
Axe 1	Digital Transformation Strategy	Q1	Does the bank have a clear digital transformation strategy? What are its main objectives?
		Q2	Who makes major technology investment decisions?
		Q3	Is the strategy documented and communicated to all departments?
Axe 2	Information Governance	Q1	Are there written policies for collecting, storing and protecting customer data?
		Q2	Who is responsible for data quality and security?
		Q3	Is there any employee training on data governance?
Axe 3	Digital Identity	Q1	How does the bank recognise and authenticate customers online? (biometrics, password, app?)
		Q2	Can new accounts be opened remotely? How is identity verified?
		Q3	Is there any use of multi-factor authentication or biometrics?
Axe 4	Accountability and Transparency	Q1	Is every access to or modification of customer data recorded?
		Q2	How is the person responsible for an error or data breach identified?
		Q3	Are audit logs accessible to non-IT staff?

Axe	Theme / محور	Key Question	
Axe 5	Digital Sovereignty	Q1	Where is the bank's data stored (locally / on-premises or on foreign cloud servers)?
		Q2	Does the bank use foreign cloud services (Microsoft, Google, AWS)?
		Q3	Is the legal department involved in sovereignty decisions?
Axe 6	Challenges and Future Prospects	Q1	What are the three main difficulties facing digital transformation at the bank?
		Q2	What is the most urgent improvement to strengthen information governance and digital sovereignty?

Note: Questions were used as flexible prompts during semi-structured interviews. Responses were recorded, transcribed, and thematically analysed using NVivo 14.

Total: 6 axes | 17 key questions | 3 respondents (Legal Department, Credit Department, Human Resources Department)

Appendix B: Online Questionnaire

Digital Transformation and Information Governance

CPA Batna Branch — Employee Survey

This survey is conducted as part of a Master's dissertation at the École Nationale Supérieure de Management (ENSM). It examines digital transformation strategy and its impact on information governance, digital identity, accountability, and digital sovereignty. Your participation is voluntary and strictly confidential. Thank you for your time.

Please mark (✓) the box that best reflects your opinion, where:

1 = Strongly Disagree	2 = Disagree	3 = Neutral	4 = Agree	5 = Strongly Agree
-----------------------	--------------	-------------	-----------	--------------------

Section 1 — Participant Information

Department	Loans (Quroud)	Guarantees	Human Resources	Counter (Shabak)
------------	----------------	------------	-----------------	------------------

Years of Experience

Less than 5 years

5–10 years

More than 10 years

Section 2 — Questionnaire Items (Likert Scale 1–5)

#	Statement	1 Disagree	Str. 2 Disagree	3 Neutral	4 Agree	5 Str. Agree
1	The branch has a clear digital strategy.	1	2	3	4	5
2	Current systems allow interoperability between different departments.	1	2	3	4	5
3	The system records every operation I perform (e.g., who accessed a customer file and when), enabling accountability tracing.	1	2	3	4	5
4	When I enter an error, the system immediately warns me and prevents completing the operation before correction.	1	2	3	4	5
5	The bank relies on software from foreign (non-Algerian) companies.	1	2	3	4	5
6	A scanned digital copy is legally accepted in the same way as the original paper document.	1	2	3	4	5
7	Most employees prefer paper-based work over digital processes.	1	2	3	4	5
8	Logging into the system with a password alone is sufficiently secure for my position.	1	2	3	4	5
9	Audit procedures are clear and can be executed from digital records.	1	2	3	4	5
10	I feel well-qualified in the area of information security and digital data protection.	1	2	3	4	5
11	There are written policies on data security and confidentiality, and they are effectively implemented.	1	2	3	4	5
12	The technical infrastructure (network, servers, hardware) is reliable and effective.	1	2	3	4	5

Section 3 — Open-Ended Questions

13. In your opinion, what is the most important technical improvement that would facilitate your daily work?

14. How optimistic are you that the new system will resolve the issues of digital integration and sovereignty?

Very High High Moderate Low Very Low

This questionnaire is also accessible via the QR code below:



https://docs.google.com/forms/d/e/1FAIpQLScmVZNhf6KbJe-ZKyUrEN13e_5_ctUNrIpTYksUJhGreZYvCA/viewform

Thank you very much for your time and cooperation.

Appendix C: SPSS Statistical Output

Digital Transformation & Information Governance Survey — CPA Batna Branch

N = 12 | SPSS v26 | Data collected: April 2026

Table C1 — Reliability Statistics (Cronbach's Alpha)

Scale	Cronbach's α	No. of Items
All 12 questionnaire items	.878	12
Valid observations	10 (83.3%)	
Excluded (listwise)	2 (16.7%)	

Note: $\alpha = .878$ exceeds the Nunnally (1978) threshold of .70, indicating good internal consistency.

Table C2 — Frequency Distribution by Department

Department	N	Frequency %	Valid %	Cumulative %
Counter (Shabak)	1	8.3	8.3	8.3
Guarantees	2	16.7	16.7	25.0
Loans (Quroud)	7	58.3	58.3	83.3
Human Resources	2	16.7	16.7	100.0

Total	12	100.0	100.0	—
--------------	-----------	-------	-------	---

Table C3 — Frequency Distribution by Years of Experience

Experience	N	Frequency %	Valid %	Cumulative %
Less than 5 years	3	25.0	25.0	25.0
5–10 years	7	58.3	58.3	83.3
More than 10 years	2	16.7	16.7	100.0
Total	12	100.0	100.0	—

Table C4 — Descriptive Statistics (All 12 Items)

Scale: 1 = Strongly Disagree → 5 = Strongly Agree | Mean interpretation: < 2.5 = Low | 2.5–3.5 = Moderate | > 3.5 = High

Statement	N	Min	Max	Mean	Std. Dev.
The branch has a clear digital strategy.	12	1.0	4.0	2.750	1.357
Current systems allow interoperability between departments.	12	1.0	4.0	3.083	1.240
The system records every operation performed (e.g. file access logs), enabling accountability tracing.	12	1.0	5.0	3.667	1.303
When an error is entered, the system immediately warns and prevents completion before correction.	12	2.0	5.0	3.500	1.000
The bank relies on software from foreign (non-Algerian) companies.	12	1.0	5.0	3.250	1.603
Scanned digital copies are legally accepted equivalently to original paper documents.	12	1.0	5.0	3.000	1.651
Most employees prefer paper-based processes over digital ones.	12	1.0	5.0	3.083	1.379
Password-only login is sufficiently secure for my position.	12	1.0	5.0	3.583	1.084
Audit procedures are clear and executable from digital records.	11	1.0	4.0	3.091	0.944

I feel well-qualified in information security and digital data protection.	12	1.0	5.0	3.000	1.279
There are written data security and confidentiality policies that are effectively implemented.	12	1.0	5.0	2.917	1.311
The technical infrastructure (network, servers, hardware) is reliable and effective.	11	1.0	5.0	2.909	1.446

Colour guide: Green (> 3.5) = High agreement | Orange (2.5–3.5) = Moderate | Red (< 2.5) = Low agreement

Table C5 — One-Way ANOVA by Years of Experience

Factor: Years of Experience (3 groups: < 5 yrs / 5–10 yrs / > 10 yrs) | Dependent variables: 12 items

Statement	Between SS	df	Between MS	F	Within SS	df	Within MS	Sig.
Q1 — Clear digital strategy	3.869	2	1.935	1.063	16.381	9	1.820	.385
Q2 — System interoperability	4.536	2	2.268	1.649	12.381	9	1.376	.245
Q3 — Operation logging / accountability	2.738	2	1.369	.774	15.929	9	1.770	.490
Q4 — Error warning system	.119	2	.060	.049	10.881	9	1.209	.952
Q5 — Reliance on foreign software	11.369	2	5.685	3.031	16.881	9	1.876	.099
Q6 — Legal validity of digital copies	5.405	2	2.702	.989	24.595	9	2.733	.409
Q7 — Preference for paper	3.488	2	1.744	.901	17.429	9	1.937	.440
Q8 — Password-only security	.702	2	.351	.259	12.214	9	1.357	.778
Q9 — Audit procedure clarity	2.409	2	1.205	1.483	6.500	8	.813	.283
Q10 — InfoSec qualification	4.286	2	2.143	1.406	13.714	9	1.524	.294
Q11 — Written data security policies	8.036	2	4.018	3.323	10.881	9	1.209	.083
Q12 — Technical infrastructure	8.481	2	4.240	2.729	12.429	8	1.554	.125

Note: All p-values > .05 — no statistically significant differences across experience groups, indicating homogeneity of perceptions. Red cells would indicate p < .05.

SPSS v26 | CPA Batna Branch | April 2026 | N = 12 respondents | Messaoudi Asma — ENSM Master's Dissertation 2025/2026



Figure 13 :word cloud from NVIVO.

