The Sankalpa: International Journal of Management Decisions
ISSN: 2454-7425
Volume 12, Issue 1 (January - June 2026)

Legal Responsibility Arising from Electronic Auditing in the Banking Sector

D Omari Aicha
Adrar University, Algeria
omari.aicha20@univ-adrar.edu.dz
D **Hamimeche Nardjes**
University of Jijel – Algeria
hamimeche_nardjes@hotmail.com

Submission date 10.10.2025 Acceptance -08.12.2025 Publication -24.02.2026

Abstract:
This research paper aims to examine the legal framework governing electronic auditing in the Algerian banking sector, while clarifying the nature of the legal responsibility resulting from the breach of electronic auditing controls, whether related to bank officials, information systems auditors, or electronic certification service providers. The study also addresses the relationship between electronic payment systems and the electronic control and auditing system, in light of rapid technological development and the consequent legislative intervention to ensure the security of banking transactions and data protection.
The study concluded that the Algerian legislator has established important legal rules to regulate the digital banking environment; however, certain aspects related to the civil and professional liability of electronic auditing still require further detailing and regulation.
Keywords: electronic auditing, legal responsibility, banking sector, electronic payment systems, electronic signature.

Introduction

The banking sector has undergone a radical transformation due to the digital revolution, as banks have shifted from traditional transactions to electronic systems that rely on complex information networks to manage accounts, execute transfers, and operate electronic payment systems. The role of control is no longer limited to traditional financial auditing but has extended to what is known as electronic auditing, which involves examining information systems, data integrity, network security, and compliance with governing legislation.
With the growing electronic risks such as hacking, data manipulation, and electronic fraud, the issue of legal responsibility arising from breaches of electronic auditing duties has emerged.
Accordingly, the main research problem is:
What is the legal framework governing electronic auditing in the Algerian banking sector? And what is the nature of the legal responsibility resulting from breaches of its controls?
To answer this problem, the research was divided into three axes:
The first axis: The nature of electronic payment means and electronic auditing in the banking sector.

The second axis: The legal basis of electronic auditing in Algerian legislation.
The third axis: The legal responsibility resulting from breaches of electronic auditing.

The First Axis: The Nature of Electronic Payment Means and Electronic Auditing in the Banking Sector

In this section, we discuss electronic payment means. These means include: (Ma'ta Allah & Bougmoum, 2004)

First: Electronic Money

Electronic money is the monetary value of a currency issued electronically by the public or private sector and stored in an electronic device. It can be considered one of the forms of digital financial instruments whose function is to perform some or all of the functions of money (Tawfiq Shanbour, 2005).

Electronic money includes two forms: (Moussa, 2007)

- The first form: a prepaid card intended for multiple purposes, also called a stored-value card;
- The second form: stored-value payment mechanisms that enable payments through the use of open computer networks.

Electronic money can also be divided into accountable systems, where exchanges between parties are monitored by a third party, and non-accountable systems that allow free transfer of value similar to physical cash movement. There are several applications of these systems (Tawfiq Shanbour, 2005):

- Online systems requiring connection to a third party such as the currency issuer to verify the validity and accuracy of the transaction, and offline systems that do not require a third party but rely on cards containing stored value, from which each amount is deducted after completing the cash withdrawal process (Al-Shoura, 2008);
- Systems based on electronic coins, each containing information including a serial number and a specified value digitally signed by the issuing institution, and systems based on ledger balances.

Second: Banking (Plastic) Cards

A plastic card (credit card) is defined as a card issued by a credit institution or a legally authorized entity, allowing its holder to withdraw or transfer money from his account (Al-Qalyoubi, 2007). These cards vary as follows:

Credit Cards

Origin of the Credit Card:

Credit cards first appeared in 1914 in the United States, when oil companies began issuing cards allowing their customers to purchase petroleum products from their stations, with settlement of transactions at the end of an agreed period. Since 1950, these cards appeared in the form of store cards, then travel cards, entertainment cards, and finally banking credit cards (Al-Shoura, 2008).

Definition of Credit Cards:

This card is known by several names, including charge card and plastic payment card. It is defined as a payment instrument similar to a check, granting its holder short-term bank credit. According to the Islamic Fiqh Academy of the Organization of Islamic Conference, it is: “A

document given by its issuer to a specific person based on a contract between them, enabling him to purchase goods and services from those who accept the document without immediate payment, as it includes the issuer's commitment to pay, and it may also enable cash withdrawal from banks" (Abdel Hadi Al-Najjar, 2007).

Types of Credit Cards:

Credit cards are divided into several categories according to classification basis (Al-Shoura, 2007):

- **According to usage:**
  - Debit or direct deduction cards: a payment instrument, not considered a credit instrument, as it does not grant a grace period for payment and requires the customer to have previously opened a current account with sufficient liquidity;
  - Monthly debit or deferred charge cards (debt card): both payment and credit instrument, where the account does not need to contain the transaction amount, and the customer may withdraw within the permitted limit, with settlement required within 25 to 40 days;
  - Installment credit cards: similar to deferred charge cards but differ in that the customer pays in periodic installments.
- **According to privileges granted:**
  - Silver card: grants a low credit limit;
  - Gold card: grants a high or unlimited credit ceiling, with additional privileges such as accident insurance and free consultations.
- **According to use:**
  - Regular credit card: used for withdrawal, purchase, and services;
  - Electronic cash withdrawal card: used only for ATM withdrawals;
  - Local cards: used only within the issuing bank's territory and currency.
- **According to issuing entity:**
  - Visa Card: issued by all participating member banks worldwide;
  - American Express: issued by a single financial institution supervising all operations;
  - Cards issued by commercial institutions such as hotels or gas stations;
  - Cheque Guarantee: bank guarantee for payment of a check drawn using the card within the guaranteed limit (Al-Qalyoubi, 2007).
- **According to type of guarantee:**

The issuer may require a guarantee in the form of a current or investment account.

Payment Cards

These are cards issued by banks or international finance companies based on the existence of actual balances in the customer's account. They do not grant credit but serve as a means of payment for goods and services instead of cash. Transactions are carried out within the customer's balance by inserting the card into a device connected to the issuing bank's card center, allowing immediate deduction and settlement.

Third: Electronic Checks

An electronic check contains all the information and elements of a traditional check (drawer's name, beneficiary, bank, amount, date of issuance) (Abu Al-Hayja, 2011). Electronic checks rely on the existence of an intermediary for clearing operations, represented by the bank, where both seller and buyer open accounts and register their electronic signatures in the bank's database (Ben Habib & Khaldi, 2005).

The electronic signature represents a number or secret code created by its owner using computer software, generating a digital encrypted function for an electronic message using key algorithms (Sharaf Al-Din, 2007). To ensure its credibility and legal recognition, it must be created within a secure framework and certified by neutral entities responsible for validating its authenticity (Alem, 2007).

Fourth: Smart Cards

Smart cards are a technological development consisting of a plastic card containing an electronic chip that stores all data related to its holder. This card allows the customer to choose between immediate or credit-based transactions, which has led to its widespread global use. It is characterized by high security and the ability to transfer value from and to another card, and even from a current account (Ben Habib & Khaldi, 2005).

The Second Axis: The Legal Basis of Electronic Auditing in Algerian Legislation

Although the term "electronic auditing" is not explicitly mentioned in Algerian legislative texts, its legal framework is derived from various laws and regulations that establish protection of information systems, ensure the security of electronic transactions, and impose effective internal control mechanisms within banking institutions. Electronic auditing is thus considered an executive mechanism to ensure compliance with these texts (Waked, 2001).

First: Penal Code as Amended by Law 04-15

Under Law No. 04-15 amending the Penal Code, the Algerian legislator introduced a special section titled: "Attacks on automated data processing systems," from Article 394 bis to Article 394 bis 7 (Law 04-15, 2004).

This section criminalizes:

- Unauthorized access or stay in an information system;
- Fraudulent deletion, modification, or insertion of data;
- Obstruction of automated data processing systems;
- Destruction or alteration of electronic data.

This regulation is particularly significant in the banking field due to reliance on centralized information systems. It implicitly requires banks to adopt periodic electronic auditing mechanisms to detect hacking or manipulation attempts, otherwise they may incur civil liability for negligence in securing their systems (Alem, 2007).

Second: Law 09-04 on Crimes Related to Information and Communication Technology

Law No. 09-04 strengthened the preventive and regulatory framework for combating cybercrime (Law 09-04, 2009). It defined several concepts, including information systems, data, service providers, traffic data, and electronic communications.

It also established a national authority responsible for cybercrime prevention, coordination, and judicial assistance.

In the banking context, this law obliges banks to:

- Retain digital records of operations;
- Enable tracking of suspicious transactions;
- Ensure integrity of data usable as judicial evidence.

All of this falls within the core functions of electronic auditing (Waked, 2001).

Third: Law 15-04 on Electronic Signature and Certification

Law No. 15-04 of 01 February 2015 regulated:

- The concept of electronic signature;
- Qualified electronic signature;
- Electronic certification certificate;
- Obligations of electronic certification service providers (Law 15-04, 2015).

The law established conditions for recognizing a qualified electronic signature and imposed strict obligations on certification service providers, including data confidentiality and system security.

It also provides criminal penalties, including imprisonment and fines, for any person entrusted with auditing who discloses confidential information during the performance of his duties, thereby establishing direct criminal liability for the electronic auditor (Law 15-04, 2015).

Fourth: Regulations of the Bank of Algeria Related to the Security of Payment Systems

The Bank of Algeria issued Internal Regulation No. 05-07 concerning the security of payment systems, in which it defined the interbank payment and settlement system and obligated its participants to adopt technical and organizational measures ensuring the security of operations (Waked, 2001).

Among the principles emphasized by these regulations:

• System readiness and continuity;
• Recording and documentation of exchanged information;
• Traceability of operations;
• Auditability of the system;
• Protection of technical infrastructure.

These elements constitute essential components of any effective electronic auditing system, as digital control cannot be conceived without traceable systems, preserved records, and clear internal controls.

Accordingly, electronic auditing in the Algerian banking sector is based on an integrated legal framework combining criminal rules, technical regulations, and electronic signature provisions, thereby establishing multidimensional legal liability in case of breach of those obligations.

Waked, Y. (2001). The legal system of electronic payment (Unpublished master's thesis). University of Tizi Ouzou, Algeria.

The Third Axis: Legal Responsibility Resulting from Breach of Electronic Auditing

The Third Axis: Legal Responsibility Related to Electronic Auditing

Electronic auditing in the banking sector is considered an essential control mechanism to ensure the integrity of information systems, the security of financial transactions, and the protection of customers' rights. However, breach of auditing duties may give rise to multiple legal liabilities, ranging from civil, criminal, administrative, and professional liability, depending on the nature of the committed fault and the resulting damage.

The specificity of liability in this field stems from the technical nature of banking systems, the complexity of their structure, and their complete reliance on automated data processing, which makes any technical malfunction or supervisory negligence capable of causing serious financial consequences (Hall, 2016).

First: Civil Liability

1- Legal Basis of Civil Liability

Civil liability in the field of electronic auditing is based on the general rules of contractual and tort liability stipulated in the Algerian Civil Code (Law 05-10 amending the Civil Code).

Civil liability generally rests on three elements:

1. Fault;
2. Damage;
3. Causal relationship between fault and damage.

2- Forms of Fault in Electronic Auditing

Fault may occur in several forms, including:

• The bank's negligence in establishing an effective internal control system for its information systems;

• Failure to conduct periodic audits of electronic payment systems;

• The electronic auditor's failure to detect substantial vulnerabilities that could have been discovered according to professional standards;

• Reliance on protection systems that do not comply with approved technical standards.

If it is established that the damage suffered by the customer (such as theft of data or transfer of funds from his account) resulted from negligence in auditing or weakness in control, liability of the bank or the auditor arises, as the case may be (Romney & Steinbart, 2018).

3- Contractual or Tort Liability?

• Contractual liability arises when there is a contract between the bank and the customer, or between the bank and the external auditor, and contractual obligations are breached, such as the bank's obligation to secure transactions.

• Tort liability arises when damage results from the breach of a general legal duty without a direct contractual relationship, such as hacking of a customer's data who is not directly contracted with the auditing entity.

It is noted that the modern doctrinal trend tends to tighten the liability of financial institutions as a "professional," who is presumed to exercise a high level of care and caution, especially in the digital environment (Singleton & Singleton, 2010).

Second: Criminal Liability

1- Legislative Basis

Criminal liability in the field of electronic auditing is based on several texts, most notably:

• The Penal Code as amended by Law 04-15 (2004) concerning attacks on automated data processing systems;

• Law 09-04 (2009) concerning crimes related to information and communication technology;

• Law 15-04 (2015) concerning electronic signature and certification.

2- Forms of Criminal Liability of the Electronic Auditor

Criminal liability may arise in the following cases:

A- Disclosure of Professional Secrecy

Law 15-04 explicitly provides for the punishment of any person entrusted with auditing who discloses confidential information obtained during the performance of his duties (Law 15-04, 2015).

This establishes the principle of professional confidentiality as a fundamental obligation in the electronic auditing profession.

B- Collusion or Participation in Cybercrimes

If it is proven that the auditor colluded in modifying data or intentionally facilitated system intrusion, he shall be considered an accomplice to the crime according to the rules of criminal participation stipulated in the Penal Code (Law 04-15, 2004).

C- Gross Negligence Leading to Facilitation of the Crime

In some cases, gross negligence may result in criminal liability, especially when it relates to a specific legal duty to protect data or report vulnerabilities.

3- Aggravated Nature of Liability in the Banking Environment

Due to the sensitivity of the banking sector, crimes related to it are often treated with strictness because of their direct impact on financial stability and public confidence in the banking system (Alem, 2007).

Third: Administrative and Professional Liability

1- Administrative Liability of Banking Institutions

Banks are subject to the supervision of the Bank of Algeria and regulatory authorities. In case of violation of information security standards or breach of compliance requirements, they may be subject to:

• Financial fines;
• Official warnings;
• Restriction of certain activities;
• Withdrawal of license in serious cases.

Electronic certification service providers may also be subject to license withdrawal if they violate obligations stipulated in Law 15-04 (2015).

2- Professional Liability of the Auditor

The electronic auditor is subject to professional obligations, including:

• Independence;
• Objectivity;
• Technical competence;
• Confidentiality.

In case of breach of these standards, he may be subject to:

• Disciplinary sanctions within the institution;
• Removal from the professional register;
• Prohibition from practicing the activity.

International standards for information systems auditing (ISACA, 2019) emphasize that the auditor's responsibility is not limited to detecting errors but includes evaluating the effectiveness of internal controls and digital risk management.

Final Analysis

It appears that the legal liability related to electronic auditing is composite and multidimensional:

• Civil when financial damage occurs to the customer;
• Criminal when legal obligations related to data security are breached;
• Administrative and professional when compliance and supervisory rules are violated.

This multiplicity reflects the specificity of the digital banking environment, which requires a high level of technical and legal caution, making electronic auditing not merely a technical procedure but a legal obligation whose breach entails serious consequences.
(4th ed.). Wiley.

Conclusion

In light of the rapid digital transformation witnessed by the banking sector, electronic auditing has become a pivotal tool to ensure the integrity of information systems, the security of financial transactions, and the protection of public trust in banking institutions. This study has shown that the legal liability associated with electronic auditing in the Algerian banking sector is characterized by a composite nature, combining civil, criminal, and administrative liability, depending on the nature of the committed breach and its consequences.

Through the analysis of Algerian legislative texts, particularly the Penal Code as amended by Law 04-15, Law 09-04 concerning crimes related to information and communication technology, and Law 15-04 concerning electronic signature and certification, it appears that the Algerian legislator has established an important legal framework to protect the digital banking environment, although there is no explicit and direct regulation of the concept of electronic auditing as an independent profession or specific legal regime. Thus, electronic auditing derives its legitimacy and legal basis from a dispersed legislative system that complements itself to ensure transaction security and data protection.

First: Results

The study reached several findings, most notably:

1. The absence of a specific legal text regulating the profession of electronic auditing in the banking sector despite its growing importance.
2. The existence of an indirect legal basis for electronic auditing derived from cybercrime and electronic signature laws.
3. The expansion of the scope of legal liability to include the bank, the auditor, and the electronic certification service provider according to the degree of fault and role in the process.
4. The legislator's strictness in criminalizing acts related to attacks on automated data processing systems, reflecting awareness of the seriousness of digital crimes.
5. The persistence of certain aspects, especially those related to civil liability for technical negligence or security vulnerabilities, requiring further legislative clarification.

Second: Recommendations

Based on the above findings, the study recommends the following:

1. Enacting a specific legal text regulating electronic auditing in the banking sector, defining conditions of practice, competence standards, and limits of liability.

2. Obliging banks to conduct periodic independent electronic audits, document their results, and subject them to regulatory supervision.
3. Establishing national standards derived from international information systems auditing standards to enhance professional uniformity.
4. Strengthening specialized training in electronic auditing and information security for judges, lawyers, auditors, and banking staff.
5. Developing early reporting mechanisms for technical vulnerabilities and hacking incidents to ensure rapid intervention and reduce damages.

Third: Future Prospects

The continuous development of financial technology (FinTech), the spread of digital banking services, and the use of artificial intelligence and blockchain require reconsideration of traditional concepts of legal liability. It is expected that future legal regulation will move toward:

• Establishing expanded digital liability based on risk management rather than merely traditional fault;
• Adopting smart control systems based on real-time data analysis;
• Strengthening international cooperation in combating electronic banking crimes;
• Integrating cybersecurity requirements within banking governance standards.

Accordingly, electronic auditing is no longer merely a technical function within the bank but has become a legal and security pillar for protecting the banking system in the digital age, which requires continuous legislative and institutional development to keep pace with rapid technological transformations.

List of References in Arabic:

Abu Al-Hayja, Muhammad Ibrahim. (2011). Electronic commerce contracts. Dar Al-Thaqafa for Publishing and Distribution.

Ben Habib, Abdel Razzaq, & Khaldi, Khadija. (2005). Fundamentals of banking work.

Khair Al-Din, Ma'ta Allah, & Bougmoum, Mohamed. (2004, December 14–15). Informatics and the banking system: The necessity of developing banking services (Paper presented). First National Conference on the Algerian Banking System and Economic Transformations: Reality and Challenges, Algeria.

Sharaf Al-Din, Ahmed. (2007). Electronic signature: Rules of proof and security requirements in electronic commerce (Paper presented). Annual Scientific Conference of the Faculty of Law, Beirut Arab University, Beirut.

Shanbour, Tawfiq. (2004). Electronic payment instruments: Payment cards – electronic money. Dar Al-Houda.

Al-Shoura, Jalal Aed. (2008). Electronic payment methods. Dar Al-Thaqafa for Publishing and Distribution.

Alem, Mohamed. (2007). Electronic banking operations: Problems raised by the use of the Internet in the banking field (Paper presented). Annual Scientific Conference of the Faculty of Law, Beirut Arab University, Beirut.

Law No. 04-15 of November 10, 2004, amending and supplementing Ordinance 66-156 containing the Penal Code, Official Gazette of the People's Democratic Republic of Algeria.

Law No. 09-04 of August 05, 2009, containing the specific rules for the prevention and combating of crimes related to information and communication technology, Official Gazette of the People's Democratic Republic of Algeria.

Law No. 15-04 of February 01, 2015, determining the general rules relating to electronic signature and certification, Official Gazette of the People's Democratic Republic of Algeria.

Moussa, Ahmed Jamal El-Din. (2007). Electronic money and its impact on the role of central banks in managing monetary policy (Paper presented). Annual Scientific Conference of the Faculty of Law, Beirut Arab University, Beirut.

Al-Najjar, Abdel Hadi. (2007). Credit cards and electronic banking operations (Paper presented). Annual Scientific Conference of the Faculty of Law, Beirut Arab University, Beirut.

Waked, Youssef. (2001). The legal system of electronic payment (Unpublished master's thesis). University of Tizi Ouzou, Algeria.

Foreign References

Hall, J. A. (2016). Information technology auditing (4th ed.). Cengage Learning.

ISACA. (2019). COBIT 2019 framework: Governance and management objectives. ISACA.

Romney, M. B., & Steinbart, P. J. (2018). Accounting information systems (14th ed.). Pearson.

Singleton, T. W., & Singleton, A. J. (2010). Fraud auditing and forensic accounting (4th ed.). Wiley.