International Journal of Scientific Research and Management (IJSRM)
||Volume||14||Issue||09||Pages||3132-3138||2026||
Website: https://ijsrm.net ISSN (e): 2321-3418
DOI: 10.18535/ijsrm/v14i09.ec08

Cybersecurity In The Tunisian Banking Sector Comprehensive assessment of cyber risk management, governance, resilience and digital transformation

Mme Houda Jendoubi

Abstract: The digital transformation of the Tunisian banking sector has profoundly altered the ways in which financial services are accessed, transactions are processed and data is managed. This development simultaneously increases the attack surface of banking institutions and the importance of cybersecurity for financial stability, customer protection and business continuity. This article builds on the framework of the original study, which initially focused on a single bank, but extends it to a sector-wide approach covering all Tunisian banks. The study proposes an assessment framework structured around eight key areas: cyber governance and strategy, data protection and compliance, risk management, systems and identity security, incident management, resilience and business continuity, the human factor, and supplier security. The analysis is contextualised against the NIST Cybersecurity Framework 2.0, ISO/IEC 27001:2022, international principles of operational resilience and the Tunisian regulatory framework, notably Decree-Law No. 2023-17 on cybersecurity. The results presented are a sector-based and documentary synthesis: they do not constitute a technical audit of the banks and should not be interpreted as official scores for individual banks. They highlight an overall maturity level ranging from intermediate to good, with likely variations between institutions and across different areas. Common priorities include, in particular, third-party risk governance, resilience to ransomware, the automation of identity management, the financial quantification of cyber risk, data protection by design, and the development of sector-wide threat intelligence capabilities.

Keywords: Banking cybersecurity, Tunisian banks, cyber risk, digital transformation, operational resilience, NIST CSF 2.0, ISO/IEC 27001, governance, data protection, incident management.

Introduction

With the proliferation of information technology, the banking system has undergone significant changes in terms of processes, transactions and operations. Tunisian banks are developing digital services, remote banking channels and interconnected infrastructures that enhance the customer experience but also increase dependence on technology, service providers and data exchanges.

This evolution is accompanied by a shift in risk: attacks no longer target just a single IT infrastructure, but can simultaneously affect digital identities, mobile applications, payment systems, suppliers, workstations, customer data and business continuity mechanisms. International literature shows that phishing, identity theft, malware and attacks targeting digital services constitute major risks to the adoption of digital banking (Wang, Nnaji & Jung, 2020; Cele & Kwenda, 2025).

In Tunisia, the institutional framework has been strengthened by Decree-Law No. 2023-17 of 11 March 2023 on cybersecurity, which, amongst other things, defines the concepts of cybersecurity, cyber-attack, vulnerability and cyber crisis, and reinforces the role of the competent national authority. The financial sector also has cooperation mechanisms in place, including the Tunisian Financial CERT, which is coordinated by the Banking and Financial Council.

Literature review

A great deal of theoretical and empirical research has focused on banking cybersecurity. Wang, Nnaji and Jung (2020), in the Nigerian context, demonstrated the evolution of banking cybercrime towards more sophisticated attacks and highlighted the combined importance of technology, training and the legal framework. This study is particularly useful for developing a sector-specific framework, as it links observed breaches to protective capabilities.

Recent literature also emphasises the interdependence between digital transformation, artificial intelligence and cybersecurity. Rodrigues et al. (2022) show that the introduction of new technologies in banking must be

accompanied by governance capable of simultaneously balancing innovation, security, compliance and stakeholder trust.

Research on data protection, for its part, emphasises that the cloud, analytics, AI and new digital architectures create new opportunities but also additional risks in terms of privacy and security. A study published in

Computers & Security in 2024 highlights these tensions in the context of digital transformation in banking.

The Tunisian context is also beginning to be the subject of specific academic research. Redissi (2025) examines cybersecurity governance and ISO/IEC 27001 certification in a sample of twelve Tunisian banks over the period 2016-2023. This research suggests that certification can be operationally significant without immediately producing a visible effect on profitability, which reinforces the idea that cybersecurity should be viewed as a resilience capability rather than merely a productive investment.

Reference frameworks

NIST Cybersecurity Framework 2.0: a flexible framework for identifying, prioritising, communicating and managing cybersecurity outcomes.

ISO/IEC 27001:2022: an information security management system based on risk management and continuous improvement.

Tunisian Decree-Law No. 2023-17: national cybersecurity framework and institutional mechanisms.

International principles of operational resilience: continuity of critical services, management of dependencies and response capability.

I. Background to the issue

The sector-based approach adopted recognises that the cybersecurity of Tunisian banks cannot be assessed solely on an institution-by-institution basis. Banks share infrastructure, payment systems, technology suppliers, service providers and a common regulatory environment. A weakness in one entity can therefore have knock-on effects across the ecosystem.

Objectives of the study

To assess the key dimensions of cyber maturity in the Tunisian banking sector.

To identify the priority risks associated with the digitalisation of banking services.

To compare sector practices with the NIST CSF 2.0 and ISO/IEC 27001 standards.

Highlight organisational, technological and human gaps.

Propose a common improvement plan applicable to Tunisian banks, adapted to their size and level of maturity.

Research hypotheses

H1: Cyber governance integrated into risk governance improves prevention and response capabilities.

H2: The maturity of identity, detection and resilience controls has a significant impact on the security of digital services.

H3: Risk associated with suppliers and technology chains is becoming a major determinant of collective resilience.

H4: Ongoing awareness-raising amongst staff and customers constitutes an essential complementary control to technical measures.

Scope

The study covers the Tunisian banking sector on a consolidated basis. It focuses on commercial banks and other banking institutions subject to the Tunisian prudential framework, without assigning individual scores to institutions due to the lack of standardised and publicly available audit data.

II. Selection of the Tunisian banking sector

Unlike the benchmark study, which focused on a specific bank, this study considers the entire Tunisian banking sector as its unit of analysis. This approach prevents a practice observed at a single institution from being unduly generalised to the whole market.

Scope	Justification	Cyber security
Economic significance	The banking sector provides a vital part of financial intermediation.	Availability and integrity of critical services.
Digital transformation	Mobile apps, online banking, electronic payments and automation.	Expansion of the attack surface.
Sensitive data	Identification, financial and transactional data.	Privacy, fraud and identity theft.
Interconnectivity	Payment systems, service providers and interbank transactions.	Risk of dependency and chain attacks.
Regulatory framework	Gradual tightening of national requirements.	Compliance and ability to provide evidence.

III. Data collection method: sector-specific questionnaire

To retain the structure of the original study, a questionnaire comprising 38 questions is proposed. In this version, it is designed as a sector-specific grid that can be administered to CISO, CIO, risk managers, compliance officers, DPOs and internal auditors at several banks. The results below are an analytical and documentary summary; they do not replace an actual survey.

Key areas of the questionnaire (8 areas)

1. Cybersecurity governance & strategy

2. Data protection & regulatory compliance

3. Cyber risk management

4. Systems, networks & identity security (IAM)

5. Incident management & security operations (SecOps)

6. Resilience & Business Continuity (BCP/RMA)

7. Staff, Awareness & Human Security

IV. Methods used

The approach is based on a compliance and maturity analysis inspired by the study provided, supplemented by international standards and Tunisian institutional sources. The NIST CSF 2.0 enables risk management to be structured around six functions -- Govern, Identify, Protect, Detect, Respond and Recover -- whilst ISO/IEC 27001 provides a framework for information security risk management.

1. Maturity matrix

Level	Interpretation	Characteristic
1 -- Initial	Low	Ad hoc checks, high dependence on individuals.
2 -- Developing	Medium	Defined but inconsistent or partially automated processes.
3 -- Established	Good	Structured governance, regular checks and indicators.
4 -- Advanced	Very good	Continuous monitoring, automation, frequent testing and improvement.
5 -- Optimised	Excellent	Adaptive approach, threat intelligence and data-driven improvement.

2. Compliance testing

The first test involves aligning expected practices with the functions of the NIST CSF 2.0. The second involves examining whether a management system is consistent with the principles of ISO/IEC 27001:2022: asset identification, risk assessment, selection of controls, monitoring, auditing and continuous improvement.

3. International benchmark

The benchmark compares the capabilities expected of the Tunisian sector with practices observed in highly mature banking ecosystems, notably in Canada, as well as with the recommendations of international organisations. The aim is not to rank Tunisian banks, but to identify transferable practices.

V. Presentation of the main sectoral findings

1. Governance and strategy

Cybersecurity is increasingly becoming a matter of governance and overall risk management.

The roles of CISO/CIO, risk, compliance and audit must be clearly separated and coordinated.

Cyber indicators must be presented to governance bodies.

The strategy must take into account the risk of dependence on technologies and suppliers. Indicative sector-specific assessment: Good -- Level 3, with variations between institutions.

2. Data protection and compliance

Customer and transactional data are critical assets.

Encryption, classification and access control are fundamental measures.

Data protection must be built in from the design stage of new services.

Compliance must be documented and tested regularly.

Indicative sector assessment: Good / under consolidation -- Level 3 to 4.

3. Cyber risk management

Risk assessments must incorporate scenarios involving fraud, ransomware, service disruption and the compromise of service providers.

Vulnerability and penetration tests must be supplemented by crisis exercises.

The financial quantification of cyber risk remains a key area for improvement. Indicative sectoral assessment: Good -- Level 3.

4. Security of systems, networks and identities (IAM)

Strong authentication and centralised identity management are priorities.

Network segmentation, EDR/XDR, PAM and patch management reduce the attack surface.

Automation of processes relating to staff onboarding, mobility and offboarding must be strengthened. Indicative sector assessment: Good / advanced -- Level 3 to 4.

VI Sector results (continued)

5. Incident management and security operations (SecOps)

Detection must be continuous and correlated with a response capability.

SOCs and SIEMs must be supplemented by orchestration and response procedures.

Simulation exercises must replicate realistic scenarios: ransomware, identity compromise, data breaches and service outages.

Indicative sectoral assessment: Advanced -- Level 4 for the most structured capabilities, with sectoral variation.

6. Resilience and business continuity

BCPs/DRPs must cover technological dependencies and critical suppliers.

Backups must be protected against tampering and the spread of ransomware.

Recovery tests must measure realistic RTO/RPO targets. Indicative sectoral assessment: Good -- Level 3 to 4.

7. Human security and awareness

Simulated phishing campaigns and regular training are essential.

Security must also extend to senior management, service providers and business functions.

Customer awareness of phishing, social engineering and fraud must be strengthened. Indicative sectoral assessment: Good -- Level 3.

8. Suppliers and supply chain

Cloud, software, maintenance and security service providers must be assessed according to their criticality.

Contracts must include requirements relating to security, incident notification, auditing and reversibility.

Continuous monitoring of supplier risk is a priority. Indicative sectoral assessment: Average to good -- Level 2 to 3.

9. Threat Intelligence

Banks benefit from sector-wide cooperation, but the structured sharing of indicators and scenarios could be further improved.

A more automated threat intelligence platform would improve the ability to anticipate threats. Indicative sectoral assessment: Good -- Level 3.

Updated statistics on the Tunisian cyberspace -- 2025 and the first half of 2026

To update this article, the national figures below replace the undated general data. They are taken directly from statistics published by the National Cybersecurity Agency (ANCS). They relate to the Tunisian cyberspace as a whole and do not, on their own, constitute statistics specific to banks.

Interpreting the data: the number of incidents reported nationally in the first half of 2026 already exceeds the total for the whole of 2025. However, this comparison should be interpreted with caution, as the 2026 period covers only six months and reporting methods and volumes may change.

For incidents handled in the first half of 2026, the ANCS notes in particular that intrusions and unauthorised access account for 38.95 per cent and phishing for 33.98 per cent of the reported categories. These figures reinforce the relevance of two priorities highlighted in the article: identity and access management (IAM/MFA) and awareness-raising against phishing.

Source: National Cybersecurity Agency (ANCS), 'Statistics on the Tunisian cyberspace - 2025' and 'Statistics on the Tunisian cyberspace - first half of 2026', published on 20 July 2026.

Overall maturity summary

Axis	Indicative level	Priority
Governance & strategy	3 -- Good	High
Data & compliance	3-4 -- Good to advanced	High
Risk management	3 -- Good	High
IAM, systems & networks	3-4 -- Good to advanced	Very high
SecOps & incidents	4 -- Advanced*	Very high
PCA/PRA & resilience	3-4 -- Good to advanced	Very high
Human factor	3 -- Good	High
Suppliers	2-3 -- Developing to good	Very high
Threat Intelligence	3 -- Good	High

* Indicative level of the most structured capabilities, not an audited average across all banks.

Key strengths

Strengthening of the institutional and regulatory framework.

Development of operational security capabilities.

Gradual roll-out of strong authentication mechanisms.

Existence of sector-wide cooperation and a banking CERT.

Increasing consideration of cyber risk in governance.

Priority areas for improvement

Ongoing monitoring of suppliers and subcontractors.

Recovery following ransomware attacks and multi-system crisis scenarios.

Automation of IAM and offboarding, and the principle of least privilege.

Financial quantification of cyber risk.

Privacy by Design and Security by Design.

Threat intelligence and automated sharing of indicators.

Ongoing awareness-raising for customers and staff.

VI International Comparison (Benchmark)

The international benchmark shows that the most mature banking ecosystems do not merely accumulate security tools. They organise cybersecurity as a business resilience capability, driven by governance, measured by indicators and tested through regular exercises.

International best practice	Target scenario for the Tunisian sector	Gap to be bridged
Cyber governance at board level	Cybersecurity indicators and scenarios integrated into decision-making	Medium

International best practice	Target scenario for the Tunisian sector	Gap to be bridged
Sector-specific threat intelligence	Automated sharing and utilisation of IOCs/TTPs	High
Crisis testing	Cross-functional exercises with business units and suppliers	High
Third-party risk	Continuous monitoring of critical suppliers	Very important
Ransomware resilience	Immutable backups, tested recovery, crisis procedures	Very important
Identities	Widespread MFA, PAM, least privilege, automation	High
Security/Privacy by Design	Controls integrated into the development cycle	High

The NIST CSF 2.0 is particularly well-suited to this benchmark as it does not prescribe a single technology: it defines cybersecurity outcomes and enables organisations to establish profiles tailored to their specific context. ISO/IEC 27001 complements this approach with a structured management system.

Lessons for Tunisian banks

Move from an ad hoc compliance approach to one based on measurable resilience.

Treat suppliers as an extension of the security perimeter.

Test recovery capabilities as rigorously as prevention capabilities.

Develop common indicators at sector level.

Invest in skills, simulation and behavioural analysis to complement the tools.

VII Strategic action plan for the Tunisian banking sectorShort term: 0-12 months

Update cyber-risk maps and crisis scenarios.

Harmonise minimum security requirements for critical suppliers.

Strengthen MFA, PAM, EDR/XDR and patch management.

Conduct ransomware and identity compromise exercises.

Roll out regular awareness campaigns and simulated phishing exercises.

Medium term: 12-24 months

Establish sector-specific maturity and resilience indicators.

Develop an advanced capability for threat intelligence and indicator sharing.

Automate IAM cycles, particularly offboarding.

Integrate Security by Design and Privacy by Design into digital projects.

Develop test scenarios involving key critical service providers.

Long term: 24-36 months

Advance maturity towards adaptive and predictive capabilities.

Develop sector-specific mechanisms for systemic crisis exercises.

Strengthen the controlled use of AI for fraud detection and prevention.

Implement an economic quantification of cyber risk to inform investment decisions.

Develop a shared culture of cyber resilience amongst banks, authorities, service providers and customers.

Proposed indicators (KPIs/KRIs)

Indicator	Measure	Target
MFA	% of critical accounts protected	Aim for 100 per cent
Critical patch	Median time to fix	Continuous reduction
MTTD	Mean time to detection	Continuous reduction
MTTR	Mean time to response/recovery	Continuous reduction
Phishing	Click-through rate in simulations	Continuous decline
Critical suppliers	% under continuous monitoring	100% target
Restoration	PRA test success rate	100% target

Conclusion

Cybersecurity in the Tunisian banking sector is now a central component of stability, trust and digital transformation. The approach proposed in this article follows the structure of the benchmark study, but replaces the analysis of a single bank with a sector-wide assessment applicable to all Tunisian banks.

The analysis highlights already significant capabilities in the areas of governance, infrastructure protection, incident management and business continuity, whilst also identifying areas requiring collective improvement: supplier risk, resilience to ransomware, identity automation, economic quantification of risk, data protection by design and threat intelligence.

The key lesson is that a bank can no longer regard cybersecurity as merely an IT function. It must be integrated into governance, operational risk, compliance, procurement, product development, business continuity and customer relations. At sector-wide level, cooperation between banks, authorities and incident response teams is also crucial.

Limitations of the study

This version does not constitute a technical audit and does not include a questionnaire that has actually been administered to all banks. The maturity levels are therefore indicative. Further academic research should collect anonymised responses from CISOs/CIOs, construct a representative sample, calculate statistical scores and test the hypotheses put forward.

References

1. National Cybersecurity Agency (ANCS). (2023). Decree-Law No. 2023-17 of 11 March 2023 on cybersecurity and institutional cybersecurity resources in Tunisia. 10.35467/cal/169298
2. Central Bank of Tunisia (BCT). (2024). Circular No. 2024-05 of 13 February 2024 on the rules governing the management of payment systems and securities settlement systems. 10.1596/41812
3. Central Bank of Tunisia (BCT). (2025). Circular No. 2025-06 of 28 February 2025 on the minimum rules governing the electronic onboarding of customers. 10.1787/97afc9f7-en
4. Benthabet, S. (2025). When ESG Meets Cybersecurity: The Moderating Effect of Digital Protection on Bank Performance in MENAT Countries. International Journal of Economics and Financial Issues, 15(6), 356-370. https://doi.org/ 10.32479/ijefi.21354
5. Bilodeau, et al. (2019). Work cited in the benchmark study on threats to banking cybersecurity. 10.55454/rcsas.3.11.2023.004
6. Banking and Financial Council (CBF). (2022). Annual Report -- cybersecurity measures and activities of the Tunisian Financial CERT. 10.1163/2210-7975_hrd-1957-2016002
7. Cele, N. N., & Kwenda, S. (2025). Do cybersecurity threats and risks have an impact on the adoption of digital banking? A systematic literature review. Journal of Financial Crime, 32(1), 31-48. https://doi.org/ 10.1108/JFC-10-2023-0263
8. International Organisation for Standardisation (ISO). (2022). ISO/IEC 27001:2022 -- Information security, cybersecurity and privacy protection -- Information security management systems -- Requirements. 10.3403/30285727u
9. Kesharwani, et al. (2019). Works cited in the benchmark study on cybercrime in the banking sector. 10.7591/9781501725333-016
10. Maharjan, & Chatterjee. (2019). Work cited in the benchmark study on protecting banks against cyber-attacks. 10.3030/735734
11. National Institute of Standards and Technology (NIST). (2024). The NIST Cybersecurity Framework (CSF) 2.0. NIST Cybersecurity White Paper 29. 10.6028/nist.cswp.29
12. Ravikumar, R. (2025). Strengthening Cybersecurity - Lessons from the Cybersecurity Survey. International Monetary Fund, Technical Notes and Manuals. 10.5089/9798400296864.005
13. Redissi, A. (2025). Cybersecurity Governance and Bank Performance in Tunisia: An Exploratory Mixed-Methods Analysis of ISO/IEC 27001 Certification. Arab Economic and Business Journal, 17(2), Article 7. https://doi.org/ 10.38039/2214-4625.1066
14. Rodrigues, A. R. D., Ferreira, F. A. F., Teixeira, F. J. C. S., & Zopounidis, C. (2022). Artificial intelligence, digital transformation and cybersecurity in the banking sector: A multi-stakeholder cognition-driven framework. Research in International Business and Finance, 60, 101616. https://doi.org/ 10.1016/j.ribaf.2022.101616
15. Soni. (2019). Works cited in the benchmark study on artificial intelligence and banking cybersecurity. 10.65470/resnova.9788169935449.20
16. Wang, V., Nnaji, H., & Jung, J. (2020). Internet banking in Nigeria: cyber security breaches, practices and capability. International Journal of Law, Crime and Justice, 62, 100415. https://doi.org/ 10.1016/j.ijlcj.2020.100415
17. Wang, Y., & Zhang, Q. (2020). Brief Introduction to Network Security Asset Management for Banks. In Cyber Security (CNCERT 2020), Communications in Computer and Information Science, 1299. Springer. 10.1007/978-981-33-4922-3_16
18. Basel Committee on Banking Supervision. (2021). Principles for operational resilience. Bank for International Settlements. 10.1596/16798
19. National Cybersecurity Agency (ANCS): publications, statistics on the Tunisian cyberspace and national resources. 10.1201/b15253-17
20. Central Bank of Tunisia (BCT): regulatory texts and institutional reports. 10.2139/ssrn.6847158
21. Banking and Financial Council (CBF): banking sector publications and activities of the Tunisian Financial CERT.
22. NIST: resources from the Cybersecurity Framework 2.0. 10.6028/nist.cswp.29.tha
23. ISO: official ISO/IEC 27001:2022 documentation. 10.1201/9781003744139-5

Appendix

Sector-specific questionnaire (38 questions)

The table below sets out the eight key areas of the reference document and adapts them to all Tunisian banks. It can be used with the following response scale: 1 = non-existent, 2 = partial, 3 = established, 4 = advanced, 5 = optimised.

No.	Area	Question
1	Governance & strategy	Does the bank have a formalised and approved cyber security strategy?
2	Governance & strategy	Are the responsibilities of the CISO, CIO, risk, compliance and audit functions clearly defined?
3	Governance & strategy	Are cyber metrics regularly reported to the governance body?
4	Governance & strategy	Are cyber scenarios integrated into overall risk management?
5	Governance & strategy	Is the cyber budget aligned with critical risks?

No.	Area	Question
6	Data & compliance	Is data classified according to its sensitivity?
7	Data & compliance	Is critical data encrypted at rest and in transit?
8	Data & compliance	Is data protection built in from the design stage?
9	Data & compliance	Are compliance controls audited regularly?
10	Data & compliance	Are data retention periods and access to data properly managed?
11	Risk management	Is the cyber-risk map updated regularly?
12	Risk management	Are internal and external penetration tests carried out?
13	Risk management	Are cyber risks addressed in risk management plans?
14	Risk management	Have potential financial losses been quantified?

15Risk managementHave fraud and ransomware scenarios been assessed?

17IAM & infrastructureAre administrator privileges managed via PAM?

19IAM & infrastructureAre critical patches tracked via an SLA?

21SecOpsIs there a capability for continuous monitoring?

23SecOpsIs there a formal incident response plan in place?

25SecOpsAre incidents analysed to improve controls?

27ResilienceAre backups kept separate and tested regularly?

29ResilienceIs recovery from ransomware attacks tested?

31	Human factor	Is compulsory cyber security
		training provided?
32	Human factor	Are phishing simulations organised?
33	Human factor	Are access rights promptly revoked when staff leave the organisation?
34	Human factor	Are customers regularly made aware of fraud?
35	Suppliers	Are suppliers categorised according to their cyber risk profile?
36	Suppliers	Do the contracts contain cybersecurity requirements?
37	Suppliers	Is supplier risk monitored on an ongoing basis?
38	Suppliers	Are there requirements for notification and reversibility?

Final note

This appendix may serve as a basis for a future quantitative survey of Tunisian banks. To develop the article into a full-scale empirical study, it would be necessary to collect the responses, calculate the means for each category, measure the standard deviations, compare the profiles of the institutions and statistically test the hypotheses.

Indicator	2025	First half of 2026
Reported incidents	557,793	657,540
DDoS attacks detected	25,300	35,000
Peak DDoS volume	638 Gbps	636 Gbps
Security advisories published by tunCERT	--	336