الجمهورية الجزائرية الديمقراطية الشعبية
République Algérienne Démocratique et Populaire

Ministère de l'Enseignement Supérieur
et de la Recherche Scientifique

Ecole Nationale Supérieure de Management
Koléa

وزارة التعليم العالي و البحث العلمي

المدرسة الوطنية العليا للمناجمنت
القليعة

Mémoire de fin d'études

En vue de l'obtention d'un Master Académique

En « Entreprenariat et Management des Projets »

Évaluation de la conformité de la sécurité du SI selon la norme ISO/IEC 27001 :2022

Cas du SI SWIFT au niveau de la BEA

Élaboré par :

Khediri Esra

Chibane Amani

Encadré par :

Dr NACER Loubna

Année académique 2024/2025

RÉSUMÉ

La sécurité de l'information constitue un levier stratégique dans le secteur bancaire, notamment face à la multiplication des cybermenaces et à la digitalisation croissante des services. Ce travail porte sur l'évaluation de la conformité du dispositif SWIFT de la Banque Extérieure d'Algérie aux exigences de la norme ISO/IEC 27001 :2022, en articulation avec le référentiel SWIFT (CSP).

L'objectif de cette recherche est d'identifier les écarts entre les pratiques en vigueur au sein de la BEA et les exigences des référentiels internationaux, afin de proposer des mesures concrètes pour améliorer la posture de sécurité et accompagner la démarche de certification. La méthodologie adoptée est qualitative, fondée sur des entretiens semi-directifs avec les responsables sécurité et sur une analyse des contrôles de l'annexe A de la norme, en lien avec les exigences du CSP.

Les résultats de l'étude mettent en évidence une coordination efficace entre les différentes entités techniques de la banque, mais souligne le besoin d'une plus grande transversalité avec les directions métiers. L'analyse comparative avec des pratiques internationales montre que, malgré des avancées notables, la BEA doit renforcer certains aspects pour atteindre un niveau de conformité optimal.

Cette recherche propose un ensemble structuré de recommandations managériales et techniques visant à corriger les écarts identifiés, à renforcer la gouvernance de la sécurité de l'information et à poser les fondations nécessaires pour engager, de manière progressive et maîtrisée, la démarche de certification ISO/CEI 27001. Elle contribue ainsi à une meilleure valorisation des dispositifs de sécurité autour des systèmes critiques, notamment dans le secteur bancaire algérien, où les exigences de conformité deviennent un levier de résilience et de confiance.

Mots clés: Certification ISO/IEC 27001 :2022, Évaluation, Système d'information SWIFT, sécurité bancaire, Conformité.

Abstract

Information security has become a strategic lever in the banking sector, particularly in the face of increasing cyber threats and the growing digitalization of financial services. This study focuses on assessing the compliance of the SWIFT system at the External Bank of Algeria with the requirements of the ISO/IEC 27001:2022 standard, in alignment with the SWIFT (CSP).

The objective of this research is to identify the gaps between current practices at BEA and international standards, to propose concrete measures to enhance security posture and support the path toward certification. The methodology is qualitative, based on semi-structured interviews with security officers and an in-depth analysis of the Annex A controls of the standard, cross-referenced with CSP requirements.

The findings highlight effective coordination among the bank's technical entities, while underlining the need for greater integration with business units. A comparative analysis with international best practices reveals that, despite notable progress, BEA must reinforce several areas to achieve optimal compliance.

This research provides a structured set of managerial and technical recommendations to address identified gaps, strengthen information security governance, and lay the groundwork for a gradual and controlled move toward ISO/IEC 27001 certification. It contributes to enhancing the value of critical system security mechanisms, particularly in the Algerian banking sector, where compliance requirements are increasingly seen as a driver of resilience and trust.

Keywords: ISO/IEC 27001:2022 certification, Evaluation, SWIFT information system, Banking security, Compliance.

الملخص

أصبحت أمن المعلومات رافعة استراتيجية في القطاع المصرفي، لا سيما في ظل تزايد التهديدات السيبرانية والتوسع المتواصل في رقمنة الخدمات المالية. تركز هذه الدراسة على تقييم مدى امتثال نظام SWIFT لدى بنك الجزائر الخارجي (BEA) لمتطلبات معيار ISO/IEC 27001:2022، وذلك بما يتماشى مع إطار برنامج أمان عملاء SWIFT (CSP).

تهدف هذه الدراسة إلى تحديد الفجوات بين الممارسات الحالية المعتمدة داخل البنك والمعايير الدولية، بغرض اقتراح تدابير ملموسة من شأنها تعزيز الوضع الأمني ودعم مسار الحصول على شهادة المطابقة. وتعتمد المنهجية المستخدمة على مقاربة نوعية، ترتكز على مقابلات شبه موجهة مع مسؤولي الأمن، بالإضافة إلى تحليل معمق لعناصر الرقابة الواردة في الملحق "أ" من المعيار، بالمقارنة مع متطلبات CSP.

تُبرز النتائج وجود تنسيق فعّال بين مختلف الكيانات التقنية داخل البنك، لكنها في الوقت ذاته تؤكد الحاجة إلى تكامل أوسع مع الإدارات الوظيفية. كما تُظهر المقارنة مع الممارسات الدولية الرائدة أنه، على الرغم من التقدم الملحوظ، لا بد لـ BEA من تعزيز بعض الجوانب لتحقيق الامتثال الأمثل.

وتقترح هذه الدراسة مجموعة من التوصيات الإدارية والتقنية المنظمة لمعالجة أوجه القصور المكتشفة، وتعزيز حوكمة أمن المعلومات، وتمهيد الطريق نحو مسار تدريجي ومحكوم لنيل شهادة ISO/IEC 27001، كما تساهم في تعزيز قيمة آليات حماية الأنظمة الحرجة، لاسيما في القطاع المصرفي الجزائري، حيث بات الامتثال عاملًا محوريًا في تحقيق المرونة وبناء الثقة.

الكلمات المفتاحية: شهادة ISO/IEC 27001:2022، تقييم، نظام SWIFT، الأمن المصرفي، الامتثال.

REMERCIEMENTS

Avant toute chose, nous rendons grâce à Dieu, le Tout-Puissant, pour la force, la patience et la persévérance qu'Il nous a accordées tout au long de ce parcours. Sans Sa guidance invisible, ce travail n'aurait pu voir le jour. C'est à Lui que revient le premier mot, chargé de gratitude et de foi.

Nous exprimons notre plus sincère reconnaissance à notre encadrante, Dr NACER, pour son accompagnement rigoureux, ses conseils éclairés et sa confiance renouvelée. Son exigence bienveillante, son regard critique et sa constante disponibilité ont été des repères précieux dans l'approfondissement de notre réflexion et dans l'aboutissement de ce mémoire.

Nos remerciements vont également à Dr BELIMANE, pour son écoute attentive, sa patience et ses remarques toujours pertinentes, qui ont enrichi notre approche et affiné notre rigueur scientifique.

Nous remercions sincèrement les équipes de la DSSI, DSI et DCE pour leur accueil et leur soutien tout au long de cette étude. Une mention particulière revient à M. BARECHE, pour sa disponibilité et son appui technique précieux, ayant grandement contribué à la qualité du travail accompli. Et plus largement, nous remercions toute notre famille, pour son soutien moral, sa patience et ses encouragements inestimables.

Nous n'oublions pas non plus toutes les personnes qui, de près ou de loin, ont croisé notre chemin durant cette démarche, et qui, par un geste, un mot, un sourire, ont apporté leur pierre à cet édifice.

Enfin, et ce n'est pas le moindre des remerciements, nous nous remercions nous-mêmes : pour avoir persisté là où la fatigue voulait gagner ; pour avoir cru, douté, puis recommencé ; pour avoir affronté les exigences de ce travail avec résilience, lucidité et engagement. Car au-delà des pages rédigées, ce mémoire est aussi le témoignage d'un chemin personnel et intérieur, guidé par la rigueur, la passion et le sens du devoir accompli.

Table de matière

REMERCIEMENTS V
RÉSUMÉ II
INTRODUCTION 1
1. Contexte de la recherche 2
2. L'accroche et l'intérêt du thème 2
3. Problématique de la recherche 4
4. Les objectifs de la recherche 5
5. Apports conceptuels, méthodologiques et managériales 5
6. Structure du plan de recherche 6
CHAPITRE I : REVUE DE LITTÉRATURE ET CADRE CONCEPTUEL 7
Section 01 : Revue de la littérature 8
1. L'état de l'art des études de l'évaluation de conformité de SI à ISO 27001 8
2. Perspective historique et enjeux actuels de la sécurité des systèmes d'information 14
3. Évolution des systèmes d'information de l'outil opérationnel au pilier de la résilience organisationnelle 15
4. Positionnement de la recherche dans le champ de la sécurité de l'information 16
5. Approches d'évaluation de la conformité à ISO 27001 16
5.1 Méthodes d'évaluation 16
5.2 Intégration avec d'autres cadres de sécurité 17
6. Analyse critique des méthodes d'évaluation de la conformité 17
7. Défis et lacunes dans l'implémentation d'ISO 27001 18
7.1 Complexité opérationnelle et ressources 18
7.2 Équilibre entre sécurité et performance opérationnelle 19
7.3 Lacunes dans l'amélioration continue 19
8. Impact d'ISO 27001 sur le management des systèmes d'information et des projets 19
8.1. Renforcement de la gouvernance de la sécurité de l'information 19
8.2 Consolidation de la confiance des parties prenantes 19
8.3 Intégration dans les cycles de projet IT et de conformité 19
9. Perspectives internationales et études de cas 20
10. Positionnement et originalité de la recherche 23
Section 02 : Cadre conceptuel 25
1. système de management de la qualité 25

1.1 Notion de base du système de management de la qualité 25
1.1.1 La qualité 25
1.1.2 Système de Management de la qualité 26
1.2 La normalisation 26
1.2.1 La norme 26
1.2.2 L'Organisation Internationale de Normalisation (ISO) 27
1.3 Les normes et référentiels afférents à l'audit interne et à la sécurité de l'information 27
1.3.1 Les normes et référentiels applicables à l'audit interne 27
1.3.2 Les normes et référentiels applicables à la gestion de la sécurité de l'information: 28
1.4 Le référentiel 28
1.5 Cadre normatif ISO 27000 pour la gestion de la sécurité de l'information et de la cybersécurité 31
2. La sécurité du système d'information bancaire SWIFT 33
2.1 L'origine étymologique de la notion d'information 33
2.2 Informatique vs Numérique 34
2.2.1 Informatique 34
2.2.2 Numérique 35
2.3 Le système d'information (SI) 35
2.3.1 Les types de système d'information 37
2.4 Le système d'information SWIFT 37
2.4.1 Histoire 37
2.4.2 Le système SWIFT 38
2.4.3 Évolutions techniques et sécuritaires récentes 38
2.4.4 Rôle stratégique de l'administrateur SWIFT 39
2.5 Notion de sécurité du système d'information 39
2.5.1 La gouvernance de l'information 40
2.5.2 Importance de la gouvernance de l'information (IG) et de la sécurité de l'information (IS) dans la gestion de l'information 40
2.5.3 Principes fondamentaux de la sécurité du système d'information 41
2.5.4 L'importance de la sécurité de l'information consiste en les points suivants 43
3. ISO 27001 comme socle, complété par CSP SWIFT et PCI-DSS 43
3.1 la norme ISO 27001 43
3.2 Architecture de la norme ISO/IEC 27001 45
3.3 Mise en œuvre du PDCA et structure de l'Annexe A de la norme ISO/IEC 27001 47
3.3.1 Application du modèle PDCA dans la norme ISO/IEC 27001 47
3.3.2 Application 47
3.3.3 Les contrôles de l'annexe A de la norme ISO 27001 48
3.4 Programme de sécurité clientèle (CSP) de SWIFT 49

3.4.1 Enjeux du CSP SWIFT (Customer Security Programme) 49
3.4.2 Objectifs et principes de CSP SWIFT 50
3.4.3 Les mesures de CSP SWIFT 50
3.5 PCI-DSS : Un Standard Essentiel pour la Conformité en Matière de Paiement 51
CHAPITRE II : CADRE ORGANISATIONEL ET MÉTHODOLOGIQUE 53
Section 01 : Présentation de l'entreprise 54
1. A propos de la Banque extérieure d'Algérie BEA : 54
1.1 Historique de l'entreprise 55
1.2 Les missions de la BEA 56
1.3 Les valeurs de la BEA 57
1.4 Structure d'Accueil 57
1.4.1 Structure de la Banque 57
1.4.2 Structure du département d'Accueil 58
2. Etat de lieux de l'entreprise accueil : 60
2.1 Présentation du Système d'information de la (BEA) 60
2.2 Périmètre Prioritaire : Orientation Stratégique sur l'Environnement SWIFT et les Exigences de Contrôle ISO/CEI 27001 62
3. Architecture Applicative de la BEA : 63
4. Interactions Clés du Système d'Information 64
Section 02 : Cadre méthodologique 68
1 . Les techniques de recueil de données 68
1.1 La recherche qualitative 68
1.2 Le guide d'entretien 69
1.3 La collecte de données 69
1.4 Recherche documentaire 70
2. Approche de conception 71
2.1 Mode de raisonnement 71
2.1.1 Le choix épistémologique 71
2.1.2 Une posture constructiviste 72
2.2 Approche qualitative 73
2.3 Le choix de collecte Les données 74
2.3.1 Les entretiens semi-directifs 74
2.3.2 La checklist ISO 27001 77
2.4 Les techniques de recueil et analyse les données 77
2.4.1 l'approche sémantique 77
2.4.2 Analyse documentaire 78
2.4.3 Échelle d'évaluation 78

2.4.4 Détermination de la méthode d'analyse : 79
2.5 L'analyse des écarts 79
2.6 Plan d'action recommandé pour l'étude 80
CHAPITRE III : RESULTATS ET DISCUSSION 81
Section 01 : Présentation et analyse des résultats 82
1. Résultats de l'observation documentaire : 82
2. Résultats des entretiens 84
2.1 Analyse synthétique des entretiens 84
3. Mise en correspondance entre le Customer Security Controls Framework CSPSWIFT et ISO 27001 : 96
4. Application de la grille d'évaluation 100
4.1 Les résultats de la grille d'application appliquent à l'annexe A : 100
4.2 Représentation graphique des résultats et diagnostic : 102
4.3 Analyse des écarts des contrôles de l'annexe A de la norme ISO 27001 : 2022 104
4.4. Plan d'action de mise en conformité des contrôles Annexe A ISO27001 112
5. Choix des Exigences et Définition du Périmètre d'Évaluation dans le Contexte de l'ISO/IEC 27001 114
5.1 Diagnostic des écarts organisationnels par rapport aux exigences ISO/IEC 27001 :2022 ciblant le dispositif SWIFT 115
5.2 Représentation graphique des résultats et diagnostic 117
5.3 Plan d'action de mise en conformité contrôles Annexe A ISO27001 119
5.4 Analyse de la Maturité ISO/IEC 27001:2022 – Évaluation du Dispositif SWIFT 120
Section 02 : Discussion des résultats : 123
1. Discussion des résultats sur le positionnement initial de la BEA et l'engagement organisationnel dans la norme ISO/IEC 27001 123
2. Discussion des résultats sur le fonctionnement du système SWIFT au sein de la Banque Extérieure d'Algérie (BEA) 124
3. Discussion sur l'analyse comparative de l'engagement de la BEA au regard des pratiques internationales en matière de sécurité SWIFT 125
3.1 Hébergement local : entre contrôle et contraintes 126
3.2 Sécurité physique : un point de fragilité persistant 126
3.3 Gestion des risques : absence de scénarios MEHARI appliqués 127
3.4 Collaboration interfonctionnelle : progrès techniques mais cloisonnement métier 127

3.5 Renforcement des mécanismes de contrôle d'accès : vers une surveillance intelligente et adaptative _____ 127

4. Discussion sur l'alignement du SWIFT CSP avec les pratiques opérationnelles ___ 128

Conclusion générale _____ 130

Bibliographie _____ 135

ANNEXES _____ 144

LISTE DES TABLEAUX

Tableau 1 : Méthodes d'évolution de la conformité à ISO 27001 _____ 20
Tableau 2 : Intervalle de temps et recherches sur l'évaluation de la conformité à ISO 27001. _____ 21
Tableau 3 : Les clauses de la norme 27001. _____ 46
Tableau 4: Les mesure de sécurité de CSP SWIFT _____ 50
Tableau 5: Récapitulatif sur la présentation de la Banque extérieure d'Alger. _____ 55
Tableau 6 : Synthèse de l'architecture technologique globale. _____ 65
Tableau 7 : Liste des personnes interviews. _____ 74
Tableau 8: Le Guide d'entretiens _____ 75
Tableau 9 : Echelle SAMI _____ 79
Tableau 10 : Les documents consultés dans le cadre de l'évaluation de la conformité du SI SWIFT (ISO 27001). _____ 82
Tableau 11: Analyse synthétique des entretiens. _____ 84
Tableau 12 : La gestion des accès au système SWIFT. _____ 92
Tableau 13 : Mise en correspondance des normes de l'industrie. _____ 96
Tableau 14: Résultats de l'application par contrôle de l'annexe A de la norme ISO 27001:2022. _____ 101
Tableau 15 : Analyse des écarts des contrôles de l'annexe A de la norme ISO 27001 :2022. _____ 104
Tableau 16 : Plan d'action de mise en conformité des contrôles Annexe A ISO 27001 _ 112
Tableau 17 : Analyse des écarts organisationnels de la DSI par rapport aux exigences de la norme ISO 27001 :2022, dans le cadre du système SWIFT. _____ 115
Tableau 18 : Plan d'action de mise en conformité - système SWIFT (ISO 27001 :2022).119

LISTE DES FIGURES

Figure 1: La famille de la norme ISO 27000 _____ 32
Figure 2: Organigramme de la Banque extérieur d'Alger. _____ 58
Figure 3 : Organigramme de la direction des systèmes d'information. _____ 60
Figure 4 : Hiérarchie du Système d'information Bancaire. _____ 64
Figure 5 : Interaction Clés du Système d'Information _____ 66
Figure 6 : Cartographie applicative. _____ 67
Figure 7 :Rader des contrôles techniques (Annexe A_ISO/IEC27001). _____ 103
Figure 8 Rader des écarts organisationnels identifiés dans le système SWIFT (chapitre clés de la norme ISO/IEC 27001). _____ 117
Figure 9 Rader des conformités organisationnels identifiés dans le système SWIFT (chapitre clés de la norme ISO/IEC 27001). _____ 118
Figure 10 : Maturité ISO/IEC 27001 :2022-Evalution du dispositif SWIFT _____ 121

LISTE DES ABRÉVIATIONS

Acronyme	Signification
A.10.1.1, A.13.1.1, A.9.1.1	Références aux exigences spécifiques dans la norme ISO 27001 (contrôles de sécurité)
AEBS	Algerian E-Banking System
AES	Advanced Encryption Standard
AES-256	Advanced Encryption Standard avec clé 256 bits
AFNOR	Association Française de Normalisation
AGP	Système Automatisé de Gestion des Profils
AI	Intelligence Artificielle
AML	Anti-Money Laundering (Lutte contre le blanchiment d'argent)
APT	Advanced Persistent Threat (Menace persistante avancée)
API	Application Programming Interface
AWS	Amazon Web Services
BALE III	Basel III (Cadre réglementaire international pour les banques)
BCE	Banque Centrale Européenne
BEA	Banque Extérieure d'Algérie
B.I.A.M	Banque Industrielle de l'Algérie et de Méditerranée
BIC	Bank Identifier Code (Code SWIFT)
BS 7799	British Standard 7799
BSI	British Standards Institution
CEI	Commission Électrotechnique Internationale (IEC en anglais)
CIGREF	Club Informatique des Grandes Entreprises Françaises
CNIL	Commission Nationale de l'Informatique et des Libertés
CO4.1 / CO4.2	Contrôles du SWIFT CSP (politique de mots de passe et authentification multifacteur)
COBIT	Control Objectives for Information and Related Technologies
CORISI	(Système de gestion des risques ou garanties – non détaillé)
CORONA	Moteur de filtrage de messages SWIFT (SmartStream)
COSO	Committee of Sponsoring Organizations of the Treadway Commission
CSP	Customer Security Programme (Programme de sécurité client SWIFT)
CSP-C01, CSP-C02, CSP-C04	Références des contrôles SWIFT CSP
CSCF	Customer Security Controls Framework
CRIPP	Cadre de Référence International des Pratiques Professionnelles
DCE	Direction du Commerce Extérieur
DELTA	(Système financier non détaillé)
DRCI	Directeur de la Remédiation et de la Conformité Interne
DRS	Direction des Risques et de la Sécurité
DSS	Decision Support System
DSSI	Direction de la Sécurité des Systèmes d'Information
DSI	Direction des Systèmes d'Information
EBIOS	Expression des Besoins et Identification des Objectifs de Sécurité
EC2	Elastic Compute Cloud (AWS)
e-Payment Platform	Plateforme de paiement électronique
ENISA	European Union Agency for Cybersecurity

ERP	Enterprise Resource Planning (Progiciel de Gestion Intégré)
FATCA	Foreign Account Tax Compliance Act
FICO	Fair Isaac Corporation
FINASTRA	Société de logiciels financiers
FINASTRA KTP	Finastra's Key Treasury Platform
FLEXCUBE	Core Banking System (Oracle)
GLPI	Gestionnaire libre de parc informatique
GPI	Global Payments Innovation
HSM	Hardware Security Module
IA	Intelligence Artificielle
IAF	Independent Assessment Framework
ICT	Information and Communication Technology
IEC / CEI	International Electrotechnical Commission
IFACI	Institut Français de l'Audit et du Contrôle Interne
IFRS	International Financial Reporting Standards
IIA	Institute of Internal Auditors
IG	Information Governance
IRS	Internal Revenue Service (États-Unis)
ISMS	Information Security Management System
ISMS-CORAS	Information Security Management System - Constructive Risk Analysis System
ISO	International Organization for Standardization
ISO/CEI 27001	Norme internationale pour la gestion de la sécurité de l'information
ISO/IEC 27002	Lignes directrices pour les contrôles de sécurité de l'information
ITIL	Information Technology Infrastructure Library
KAMI	Indicateur de maturité de la sécurité de l'information (Indonésie)
KPI	Key Performance Indicator
KRI	Key Risk Indicator
KYC	Know Your Customer
KYC-SA	Know Your Customer – Security Attestation
LMS	Learning Management System
MEHARI	Méthodologie d'évaluation des risques en sécurité de l'information
MFA	Multi-Factor Authentication
MQ	Message Queue (IBM MQ)
MT103	Message Type 103 (virement international SWIFT)
MT300	Message Type 300 (contrats à terme sur devises)
MT700	Message Type 700 (crédit documentaire)
MT940	Message Type 940 (relevé de compte fin de journée)
MT950	Message Type 950 (relevé de compte consolidé)
NACLs	Network Access Control Lists
NIST	National Institute of Standards and Technology
NIST CSF	NIST Cybersecurity Framework
OFAC	Office of Foreign Assets Control
OneTrust	Logiciel de gestion de la confidentialité et des risques
PAM	Privileged Access Management
PCA	Plan de Continuité d'Activité
PCI-DSS	Payment Card Industry - Data Security Standard
PCI SSC	Payment Card Industry Security Standards Council

PDCA	Plan – Do – Check – Act (Planifier – Faire – Vérifier – Agir)
PDP Law	Personal Data Protection Law
PDP	Personal Data Protection
PME	Petites et Moyennes Entreprises
PoC	Proof of Concept
PwC	PricewaterhouseCoopers
QSE	Qualité, Sécurité, Environnement
RBAC	Role-Based Access Control
RDS	Relational Database Service
RHEA LAROS	Bibliothèque canadienne en gestion des risques cyber
RGPD	Règlement Général sur la Protection des Données
RMA	Relationship Management Application (SWIFT)
RSSI	Responsable de la Sécurité des Systèmes d'Information
SAA	SWIFT Alliance Access
SAGP	Système Automatisé de Gestion des Profils
SAM	Standard Assessment Maturity / Security Assurance Maturity
SAMI	Security Awareness Maturity Index
SAP	Systems, Applications, and Products in Data Processing
SI	Système d'Information
SIEM	Security Information and Event Management
SIG	Système d'Information de Gestion
SIRON AML	Logiciel de lutte contre le blanchiment d'argent
SIS	Système d'Information Stratégique
SMSI	Système de Management de la Sécurité de l'Information
SMQ	Système de Management de la Qualité
SOC 2	Service Organization Control Type 2
SOX	Sarbanes-Oxley Act
SPSS	Statistical Package for the Social Sciences
SSI	Sécurité des Systèmes d'Information
STP	Straight Through Processing
SWIFT	Society for Worldwide Interbank Financial Telecommunication
SWIFT CSP	SWIFT Customer Security Programme
Tbk	Terbuka
Temenos	Logiciel de Core Banking
TI	Technologies de l'Information
TLS	Transport Layer Security
TLM	Transaction Lifecycle Management
VLAN	Virtual Local Area Network
VPC	Virtual Private Cloud
WORM	Write Once, Read Many
XML	eXtensible Markup Language

INTRODUCTION

1. Contexte de la recherche

L'information constitue l'un des actifs stratégiques les plus critiques pour les entreprises ; sa protection apparaît comme un impératif incontournable, particulièrement dans le secteur bancaire. Ce dernier, gardien de données sensibles liées aux transactions, aux identités clients et à la stabilité financière, se trouve en effet au cœur d'enjeux sécuritaires sans précédent. Alors que la digitalisation a permis de démocratiser l'accès aux informations et d'optimiser leur gestion, elle a également exposé les institutions financières à des risques accrus de cybermenaces et de fuites de données. Comme le souligne (Autorité de contrôle prudentiel et de résolution, 2022), « Avec l'accroissement de la surface d'exposition au risque et la sophistication des cyberattaques, la sécurité est l'un des soucis majeurs des établissements interrogés ».

L'exposition aux cybermenaces des systèmes bancaires suscite une inquiétude croissante, exacerbée par une hausse exponentielle des attaques ciblées au cours de la dernière décennie. Comme le souligne (Guggenberger, 2023) , le secteur financier concentre 25 % des cibles privilégiées des cybercriminels. Ces menaces, bien que techniques dans leur exécution, génèrent des externalités systémiques en érodant la confiance institutionnelle, un *asset* fondamental pour les établissements bancaires. Selon PwC (2024) , «une violation de données entraîne une probabilité de 67 % de résiliation client, un chiffre qui illustre l'alignement croissant entre conformité réglementaire et impératifs de confiance numérique ».

Le paysage de la sécurité de l'information dans le secteur bancaire reflète l'état actuel et les tendances des défis et solutions cyber auxquels les banques sont confrontées.il évolue constamment, sous l'effet de nouvelles technologies, réglementations et cyberattaques, qui redéfinissent les enjeux et opportunités pour les institutions financières. Parmi les facteurs clés qui façonnent ce paysage :la digitalisation et l'innovation croissante des services bancaires, tels que la banque en ligne, la banque mobile, le cloud computing, l'intelligence artificielle, la blockchain et la biométrie. Ces technologies offrent des avantages en termes de commodité, d'efficacité et de compétitivité, mais introduisent également de nouveaux vecteurs d'attaque et des complexités pour les équipes de sécurité.

2. L'accroche et l'intérêt du thème

Le système d'information (SI) est aujourd'hui au cœur de l'activité bancaire, jouant un rôle déterminant dans la transformation de volumes massifs de données en connaissances

fiables et disponibles en temps réel, indispensables à la prise de décision stratégique. Il assure également la fluidité des transactions financières internationales, ce qui le rend d'autant plus exposé aux menaces cybernétiques, de plus en plus ciblées, complexes et fréquentes dans le secteur financier. Dans ce contexte, la Banque Extérieure d'Algérie (BEA), comme d'autres institutions bancaires, s'appuie sur le réseau SWIFT, une plateforme mondiale de messagerie sécurisée, pour garantir la fiabilité de ses échanges interbancaires. À la suite d'incidents majeurs comme l'attaque contre la Banque centrale du Bangladesh en 2016, SWIFT a instauré le Customer Security Programme (CSP) en 2017, exigeant de ses membres l'application rigoureuse de 7 principes fondamentaux de sécurité, structurés autour de 32 contrôles spécifiques. Bien que ce programme renforce considérablement la sécurité des échanges, il reste insuffisant s'il n'est pas intégré dans un cadre plus global de gouvernance de la sécurité.

En effet, seule l'adoption et la certification complète selon la norme ISO/CEI 27001 :2022 permettent d'assurer une gestion cohérente, continue et systémique de la sécurité de l'information à l'échelle de toute l'organisation. Cette norme internationale établit un cadre méthodologique rigoureux pour évaluer les risques, définir les politiques de sécurité, mettre en œuvre des contrôles adaptés et garantir l'amélioration continue au sein d'un Système de Management de la Sécurité de l'Information . Dans ce sens, la conformité au CSP SWIFT ne doit être envisagée que comme une composante technique sectorielle, alors que l'implémentation du SMSI ISO 27001 constitue le socle fondamental sur lequel la BEA doit bâtir une stratégie de cybersécurité globale, intégrée et résiliente. Ainsi, dans un environnement bancaire de plus en plus réglementer et exposé, il devient impératif pour la BEA de viser la certification ISO/CEI 27001 pour aligner ses pratiques avec les standards internationaux, renforcer la confiance des parties prenantes et préserver durablement l'intégrité de ses actifs informationnels critiques.

Parallèlement, la BEA adopte une approche globale de la sécurité de l'information. En s'engageant dans la démarche d'alignement sur la norme ISO/CEI 27001 :2022, elle structure progressivement sa gestion des risques à travers un système de management de la sécurité de l'information (SMSI) intégrant technologie, régulation et sensibilisation. Cette approche vise à renforcer sa résilience opérationnelle, garantir la confidentialité des données sensibles et maintenir la confiance des clients et des régulateurs, tout en assurant une amélioration continue de sa posture de cybersécurité.

3. Problématique de la recherche

Dans le cadre de notre recherche de fin d'études, nous avons eu l'opportunité d'intégrer la Banque Extérieure d'Algérie, au sein de la Direction de la Sécurité des Systèmes d'information (DSSI). Ce département joue un rôle stratégique dans la protection des actifs informationnels de la banque, notamment à travers la mise en œuvre de pratiques alignées sur la norme ISO/27001 :2022, référence internationale en matière de management de la sécurité de l'information. L'analyse a porté sur l'environnement technique du système SWIFT, identifié comme une zone de risque majeur dans le dispositif de sécurité de la BEA, en raison de la sensibilité des opérations qu'il supporte et de son exposition directe aux menaces cyber.

Bien que la DSSI affiche une volonté affirmée d'alignement avec les exigences de la norme ISO/ 27001 :2022, notre immersion a révélé des besoins spécifiques en matière d'évaluation, de formalisation et de suivi des contrôles techniques appliqués à ce périmètre particulier.

Dès lors, la question centrale de notre recherche s'énonce comme suit :

Comment évaluer la conformité de la sécurité du système d'information SWIFT de la BEA selon les exigences des contrôles techniques de la norme ISO/CEI 27001 :2022, en lien avec les exigences du référentiel CSP SWIFT ?

Pour élucider cette problématique, plusieurs questions doivent être éclaircis, qui sont comme suit :

1. Comment cette conformité se compare-t-elle aux contrôles définis par le référentiel CSP SWIFT ?
2. Quelles sont les modalités concrètes de mise en œuvre des exigences de sécurité de l'Annexe A de la norme ISO/IEC 27001:2022 au sein du système d'information SWIFT de la BEA, et comment cette conformité est-elle perçue et assurée par les acteurs concernés ?
3. Comment les bonnes pratiques du référentiel CSP SWIFT peuvent-elles être exploitées pour favoriser l'alignement progressif du système d'information de la BEA avec la norme ISO 27001 ?
4. Comment les acteurs internes de la BEA, responsables du système SWIFT, coordonnent-ils leurs actions pour assurer la sécurité et la conformité du système ?

4. Les objectifs de la recherche

La présente étude a pour objectif principal d'évaluer le niveau de conformité du système d'information SWIFT de la BEA aux exigences de la norme ISO 27001:2022. Plus spécifiquement, elle vise à :

- ✓ Analyser la gouvernance technique et fonctionnelle du système SWIFT,
- ✓ Identifier les vulnérabilités, les écarts ou les insuffisances dans le dispositif de sécurité actuel, au regard des exigences de l'Annexe A de la norme ISO 27001:2022 et du cadre CSP SWIFT
- ✓ Étudier l'intégration des bonnes pratiques du référentiel CSP SWIFT et leur contribution potentielle à un alignement progressif avec la norme ISO 27001. Formuler des recommandations stratégiques et opérationnelles visant à renforcer la posture de sécurité,

5. Apports conceptuels, méthodologiques et managériales

Cette recherche s'inscrit dans le champ de la gestion des risques liés à la sécurité des systèmes d'information, en mettant l'accent sur la conformité aux standards internationaux dans le secteur bancaire. Elle mobilise les apports théoriques relatifs à la gouvernance de la sécurité, aux normes ISO 27001 :2022 et au référentiel CSP SWIFT, ce dernier étant directement applicable au périmètre critique des échanges interbancaires. L'analyse permet d'évaluer la pertinence de ces référentiels pour renforcer la résilience organisationnelle et la gestion des risques cyber.

Sur le plan méthodologique, l'étude adopte une approche qualitative appliquée spécifiquement au Système d'Information SWIFT de la Banque Extérieure d'Algérie (BEA). Elle repose sur des entretiens semi-structurés menés avec des acteurs clés du dispositif de sécurité (responsable SI SWIFT, informaticien, auditeur), afin de recueillir des données sur la mise en œuvre concrète des contrôles de sécurité. L'analyse repose sur une grille d'évaluation construite à partir des exigences du CSP SWIFT, en correspondance directe avec l'Annexe A de la norme ISO 27001. Les pratiques observées ont été évaluées à travers des indicateurs de maturité permettant d'identifier les écarts de conformité, d'apprécier l'efficacité des mesures techniques et de formuler des recommandations ciblées, tout en respectant les exigences de confidentialité propres au secteur bancaire .Les résultats offrent des retombées managériales concrètes, notamment

en matière d'optimisation des processus de sécurité, renforcer la justification budgétaire des investissements en cybersécurité et orienter la banque vers une démarche structurée de préparation à la certification ISO 27001. En particulier, cette étude contribue à améliorer le pilotage stratégique de la posture de cybersécurité de la BEA sur le périmètre sensible du SI SWIFT, en alignant ses pratiques avec les meilleures normes internationales en vigueur.

6. Structure du plan de recherche

Premier chapitre : Nous y présentons une revue de la littérature portant sur la sécurité des systèmes d'information, en particulier dans le secteur bancaire. Ce chapitre couvre également le cadre conceptuel de la sécurité de SI, tout en explorant en profondeur le système d'information SWIFT et la norme ISO 27001 :2022, en lien avec les contrôles de la référentiel CSP SWIFT qui sont au cœur de notre recherche. Nous analysons les spécificités de chaque référentiel et leur rôle dans la sécurisation des échanges interbancaires, en mettant en évidence leur complémentarité et leur importance dans la mise en conformité des SI bancaires.

Deuxième chapitre : Ce chapitre est consacré à la méthodologie de recherche adoptée pour répondre à la question centrale de notre étude. Nous détaillons la démarche qualitative, les outils et techniques utilisés, notamment les entretiens semi-structurés avec les acteurs clés de la (BEA) et l'évaluation de la conformité du système SWIFT avec les exigences des référentiels CSP SWIFT et ISO 27001.

Troisième chapitre : Ce chapitre porte sur l'évaluation de la conformité du système d'information SWIFT de la (BEA) par rapport aux exigences du référentiel CSP SWIFT, en lien avec l'Annexe A de la norme ISO 27001 :2022. À travers des entretiens semi-structurés avec les acteurs clés de la DSSI, nous analysons la mise en œuvre des contrôles de sécurité, identifions les écarts critiques et évaluons le niveau de maturité des pratiques. Cette évaluation, fondée sur des indicateurs précis, permet de proposer un plan d'action réaliste pour renforcer les dispositifs existants, améliorer l'alignement avec les standards internationaux et soutenir la transition de la BEA vers la certification ISO 27001, tout en sécurisant durablement le périmètre stratégique SWIFT.

CHAPITRE I: REVUE DE LITTÉRATURE ET CADRE CONCEPTUEL

Le présent chapitre synthétise la revue de la littérature relative à l'application de la norme ISO/CEI 27001 :2022 dans l'évaluation de la sécurité des systèmes d'information. Puis il précise également les concepts fondamentaux mobilisés dans le cadre de cette recherche.

Section 01 : Revue de la littérature

Cette première section s'intéresse à retracer l'état de l'art concernant l'évaluation de la conformité des systèmes de sécurité de l'information (SI) à la norme ISO 27001. Nous allons essayer de démontrer que notre travail de recherche se réfère à des bases scientifiques et de déterminer les différents concepts clés de notre thématique.

1. L'état de l'art des études de l'évaluation de conformité de SI à ISO 27001

1/ Selon Albarrán Trujillo, (2024), les auteurs analysent l'intégration d'un Système de Gestion de la Sécurité de l'Information (SGSI) reposant sur la norme ISO/IEC 27001, en se concentrant sur les petites et moyennes entreprises (PME) au Mexique. Leur objectif est de proposer un guide pratique pour déployer un SGSI aligné sur cette norme, tout en mettant en avant l'importance croissante de la sécurité de l'information pour les PME, notamment face à l'essor des menaces cybernétiques et aux obligations réglementaires, comme la législation mexicaine sur la protection des données personnelles. Ils décrivent les phases essentielles du déploiement d'un SGSI, structurées autour du cycle PDCA (Plan-Do-Check-Act), et illustrent comment l'adoption d'ISO/IEC 27001 peut renforcer de manière significative la protection des informations dans les PME. Toutefois, les auteurs relèvent des obstacles majeurs, tels que l'insuffisance de ressources et de compétences techniques, ainsi que l'exigence d'une documentation approfondie.

2/ une étude menée en Algérie par (Mekimah, 2022) s'intéresse à la gouvernance de la sécurité de l'information et à la conformité aux normes internationales, en particulier la norme ISO 27001, qui établit un cadre pour la mise en œuvre, la maintenance et l'amélioration continue d'un système de management de la sécurité de l'information (SMSI). À travers une approche mixte (questionnaire structuré, analyse SPSS), les auteurs évaluent les bonnes pratiques, les faiblesses opérationnelles et les perspectives d'amélioration. Les résultats révèlent un taux de conformité global de 67,14 %, avec des points forts dans la revue de direction et les exigences générales, mais des lacunes notables en amélioration continue et en compréhension des définitions normatives. L'étude souligne

l'importance d'une culture de sécurité renforcée et d'une documentation claire pour accompagner la démarche de certification.

3/ Selon Allisha Apriany et Antoni Wibowo (2023), les auteurs examinent la mise en œuvre de la norme ISO 27001 :2022 dans une société de conseil en Indonésie. En utilisant une méthodologie mixte, comprenant des observations directes, des entretiens et une analyse documentaire, pour évaluer la conformité à la norme ISO 27001 :2022 et à l'indice KAMI. Les premiers résultats ont révélé des lacunes dans la mise en œuvre du système de gestion de la sécurité de l'information (SGSI), en particulier dans les contrôles technologiques et physiques, ainsi qu'un manque de politiques et de procédures formalisées. Les auteurs ont proposé des recommandations, y compris l'élaboration de politiques et de procédures, qui ont conduit à des améliorations significatives lors de la réévaluation. L'étude souligne l'importance d'une approche intégrée de l'évaluation de la conformité, combinant les normes internationales et les outils locaux, et met l'accent sur la nécessité de politiques formalisées et de mesures correctives pour améliorer la maturité du SMSI. Toutefois, les conclusions présentent des limites en raison du contexte spécifique d'une seule société de conseil en Indonésie. D'autres recherches sont nécessaires pour étudier la mise en œuvre de la norme ISO 27001 dans différents contextes organisationnels. Dans l'ensemble, l'étude contribue à la littérature sur l'évaluation de la conformité et suggère des pistes de recherche futures sur l'intégration des normes internationales et l'impact des politiques formalisées sur l'amélioration du SMSI.

4/ Selon Ta-Seen Junaid (2023), l'auteur analyse en profondeur la norme ISO 27001, en soulignant son rôle dans la mise en œuvre d'un système de management de la sécurité de l'information (SMSI). Junaid explique que cette norme offre un cadre structuré et rentable pour protéger les informations des organisations, adaptable à tous les secteurs et tailles d'entreprises. L'article détaille les objectifs de sécurité (confidentialité, intégrité, disponibilité), la structure (10 clauses obligatoires et 93 contrôles de l'Annexe A), ainsi que son évolution depuis 2005 jusqu'à la version 2022. La conformité à l'ISO 27001 est motivée par des facteurs internes (réduction des risques, amélioration de la gouvernance, culture de sécurité), et externes (exigences réglementaires comme le RGPD, pressions concurrentielles, avantages économiques et réputationnels). Les méthodes d'évaluation incluent l'évaluation par grilles, les audits internes et externes, et le cycle PDCA pour structurer la mise en œuvre et l'amélioration continue du SMSI. Cependant, l'article

présente des limites, notamment un manque de détails pratiques sur la mise en œuvre des contrôles, une approche trop théorique sans exploration des défis opérationnels, et une absence de comparaison avec d'autres cadres de sécurité comme le NIST CSF ou le COBIT. En conclusion, bien que l'article de Junaid constitue une ressource précieuse pour comprendre les principes fondamentaux de l'ISO 27001, il présente des lacunes en termes de profondeur d'analyse et de rigueur méthodologique. Pour enrichir cette revue de littérature, il serait pertinent d'explorer des études de cas et des comparaisons avec d'autres cadres de sécurité, afin de mieux comprendre les défis et les opportunités liés à l'implémentation de l'ISO 27001, tout en offrant des recommandations pratiques pour les organisations cherchant à améliorer leur sécurité de l'information.

5/ Selon Aditya Dyan Permadi et Laura Lahindah (2025), les auteurs examinent l'impact de l'implémentation de l'ISO 27001, de la gestion des risques et de la confiance des clients sur les décisions de location de centres de données. À travers une méthodologie quantitative basée sur des questionnaires distribués à des clients, les résultats révèlent que l'ISO 27001 et une gestion proactive des risques influencent significativement les décisions de location, tandis que la confiance des clients joue un rôle central dans la fidélisation et l'attraction de nouveaux clients. La conformité à l'ISO 27001 est motivée par des facteurs internes (réduction des risques, amélioration de la gouvernance des SI, création d'une culture de sécurité) et externes (exigences réglementaires comme le RGPD, pressions concurrentielles, et avantages économiques et réputationnels). Les méthodes d'évaluation incluent l'évaluation par grilles (93 contrôles de l'Annexe A), les audits internes et externes, et le cycle PDCA pour structurer la mise en œuvre et l'amélioration continue du système de management de la sécurité de l'information (SMSI). Cependant, l'article présente des limites, notamment un manque de détails pratiques sur la mise en œuvre des contrôles, une approche trop théorique sans exploration des défis opérationnels, et une absence de comparaison avec d'autres cadres de sécurité comme le NIST CSF ou le COBIT. En conclusion, bien que l'article constitue une ressource précieuse pour comprendre l'impact de l'ISO 27001 sur les décisions de location, il serait pertinent d'explorer des études de cas et des comparaisons avec d'autres cadres de sécurité pour mieux comprendre les défis et les opportunités liés à l'implémentation de l'ISO 27001, tout en offrant des recommandations pratiques pour améliorer la sécurité de l'information et renforcer la confiance des clients, éléments clés dans un marché de plus en plus compétitif et réglementé.

6/ Selon Roger Sant Gonzalez (2023), chercheur indépendant et expert en sécurité de l'information, son analyse des normes ISO 27001 :2022 et ISO 27002 :2022 met en lumière leurs évolutions pour répondre aux défis actuels en matière de cybersécurité et de confidentialité. Les résultats principaux montrent que ces normes offrent un cadre plus flexible et intégré pour la gestion de la sécurité de l'information, nécessitant une adaptation des SGSI pour intégrer les nouveaux contrôles.

7/ Selon Arya Adhi Nugraha et Asyahri Hadi Nasyuha (2024), Les auteurs soulignent que l'ISO 27001 :2022 et la PDP Law sont complémentaires, bien que des lacunes subsistent, notamment en matière de gestion du consentement et de droits des sujets des données.En mettant l'accent sur la création d'un cadre unifié pour la protection des données et la sécurité de l'information. L'intégration de ces deux cadres permet aux organisations de se conformer à la fois aux normes internationales et aux réglementations locales, renforçant ainsi leur posture de sécurité.

8/Selon Manar Abu Talib, May El Barachi, Adel Khelifi et Olga Ormandjieva (2012), les auteurs illustrent comment les organisations peuvent mettre en œuvre cette norme. En mettant l'accent sur les avantages, les défis et les méthodes d'évaluation de la conformité. À travers trois études de cas détaillées, Les principales résultats révèlent que l'ISO 27001 est largement utilisée aux EAU pour renforcer la sécurité de l'information et répondre aux exigences réglementaires. Les grandes organisations et les entités gouvernementales sont les plus susceptibles d'obtenir la certification, Elles disposent des ressources nécessaires pour gérer les coûts et la complexité de la mise en œuvre. Les méthodes d'évaluation, telles que les grilles et les audits, sont essentielles pour identifier les écarts et assurer une conformité complète. Cette étude souligne l'importance de l'ISO 27001 pour améliorer la gestion des risques informationnels tout en répondant aux besoins réglementaires dans un contexte de cybermenaces croissantes.

9/ Selon Kristian Beckers, Maritta Heisel, Bjørnar Solhaug et Ketil Stølen (2015), les auteurs proposent ISMS-CORAS comme une extension de la méthodologie CORAS pour soutenir la conformité à ISO 27001. L'objectif principal est de combler les lacunes dans la mise en œuvre de la norme en fournissant une méthode structurée pour l'analyse des risques et la documentation des exigences de la norme. Les résultats montrent qu'ISMS-CORAS permet de générer les artefacts nécessaires pour la documentation d'un système de management de la sécurité de l'information (SMSI) conforme à ISO 27001, Cela s'appuie sur des modèles, des diagrammes et des outils spécifiques. La méthode a été validée sur un

scénario de réseau électrique intelligent (smart grid), démontrant son applicabilité dans un contexte industriel.

10/ L'étude de (Akindote, 2023), examine l'implémentation et l'efficacité de la norme ISO 27001 dans le secteur bancaire, un domaine confronté à des cybermenaces sophistiquées et à des exigences réglementaires strictes. Les auteurs soulignent l'importance d'un Système de Management de la Sécurité de l'Information (SMSI) pour protéger les données sensibles (clients, transactions) et répondre à des régulations comme le RGPD ou l'Accord de Bâle III. La méthodologie repose sur une approche mixte combinant audits internes, entretiens avec des responsables bancaires, analyses documentaires et simulations de crises, structurée autour du cycle PDCA (Plan-Do-Check-Act) de l'ISO 27001. Les résultats révèlent un taux de conformité global de 67,14 %, avec des disparités marquées : des performances élevées en gestion des risques (83,33 %) et en revue de direction (87,5 %), mais des lacunes critiques dans les contrôles technologiques (18,3 %) et physiques (22,9 %). Les auteurs identifient des défis majeurs, tels que la résistance culturelle, le manque de ressources techniques, et la complexité d'aligner la norme avec des réglementations locales (Loi 09-04 en Algérie). Ils insistent sur l'importance d'une stratégie d'amélioration continue, incluant la formation des employés, l'intégration d'outils comme le SIEM ou l'IA, et la collaboration avec des tiers pour renforcer la résilience. L'étude propose des recommandations pragmatiques, comme la priorisation des contrôles clés (chiffrement, gestion des accès) et le développement de politiques adaptées aux spécificités bancaires. Enfin, elle souligne l'originalité d'une approche hybride, associant normes internationales (ISO 27001) et outils locaux (indice KAMI en Indonésie), pour certifier la conformité et anticiper les menaces futures (ransomwares, 5G). Une contribution essentielle pour les banques cherchant à concilier rigueur normative, agilité opérationnelle et éthique dans un paysage cyber en mutation.

11/ Selon Cipriani, Goldberg et La Spada (2023), l'objectif de l'étude est d'analyser le rôle croissant des sanctions financières dans les relations internationales, en mettant l'accent sur leur mise en œuvre via les infrastructures critiques du système de paiement international, notamment le réseau SWIFT, afin de comprendre comment l'accès ou l'exclusion de ce dernier peut amplifier ou limiter l'efficacité de ces sanctions. Pour cela, les auteurs adoptent une approche historique et descriptive, s'appuyant sur des données quantitatives issues de la Global Sanctions Data base et sur des études de cas emblématiques (Iran,

Russie, Corée du Nord, Afrique du Sud, Myanmar) pour retracer l'évolution des sanctions financières depuis la Seconde Guerre mondiale et leur lien avec les réseaux de paiement transfrontaliers. Les résultats montrent une augmentation significative du nombre et de la complexité des sanctions financières au fil du temps, avec un recours accru à l'exclusion de SWIFT comme outil de pression économique, tout en soulignant que cette centralité de SWIFT incite certains pays à développer des systèmes alternatifs (comme le SPFS russe ou le CIPS chinois), risquant à long terme de fragmenter le système financier mondial et de réduire l'efficacité des sanctions occidentales.

12/ Selon Kitsios, Chatzidimitriou et Kamariotou (2023), les auteurs explorent la mise en œuvre de la norme ISO/IEC 27001 dans une entreprise du secteur des technologies de l'information (IT), identifiée sous le pseudonyme « XYZ ». L'objectif de l'étude est de démontrer comment l'adoption de cette norme permet aux entreprises de renforcer la sécurité de l'information, d'optimiser la gestion des risques et de répondre aux exigences réglementaires, tout en améliorant leur réputation et leur compétitivité. Les auteurs s'appuient sur une étude de cas approfondie de l'entreprise XYZ, spécialisée dans les services de conseil IT et le développement logiciel. La démarche inclut : Diagnostic initial : Évaluation des pratiques existantes en matière de sécurité, révélant des lacunes documentaires et des risques non identifiés. Alignement avec ISO 27001 : Déploiement d'un cadre de gestion des risques conforme à la norme, incluant l'identification des actifs, l'analyse des vulnérabilités, et la sélection de contrôles de sécurité. Processus d'implémentation : Structuration en quatre étapes : établissement des politiques, mise en œuvre des contrôles, évaluation continue, et amélioration proactive. Évaluation des risques : Utilisation combinée de la norme ISO 31000 pour la gestion des risques et de la méthodologie NIST SP 800-30 pour quantifier les impacts. Pour les résultats, L'entreprise a amélioré sa capacité à identifier et traiter les risques (réduction des erreurs humaines, automatisation de la gestion des accès). La certification a renforcé la confiance des clients et aligné les pratiques avec le RGPD. Cet article souligne que l'ISO 27001 est un levier stratégique pour les entreprises IT, malgré des défis logistiques et financiers. Il offre des insights précieux pour les praticiens, tout en appelant à des recherches futures pour élargir la validation empirique et adapter le standard aux contextes dynamiques (évolution des cybermenaces, adoption du télétravail).

13/ Dans son étude, (MOHAMED, 2021) se fixe pour objectif de proposer un processus optimisé de mise en œuvre des contrôles de la mesure 4 du SWIFT CSP, afin d'améliorer l'efficacité et la productivité du contrôleur DSSI dans la prévention des vols d'identifiants. Il mobilise une approche qualitative de type recherche-action, entretiens semi-directifs, analyse documentaire et observation participante lors d'audits internes, pour confronter les prescriptions aux pratiques de terrain . Ses résultats montrent que le contrôle CO4.2 (authentification multifactorielle) atteint un niveau de maturité maximal (niveau 5), tandis que le contrôle CO4.1 (politique mots de passe) se situe au niveau 4, partiellement aligné avec les bonnes pratiques du CSP . Fort de ce diagnostic, il élabore un workflow automatisé pour extraire les bonnes pratiques, piloter le processus de conformité et générer des rapports et recommandations, offrant ainsi à Al'Salam Bank Algeria un outil concret pour renforcer la résilience de son SI et préparer une future certification ISO 27001.

2. Perspective historique et enjeux actuels de la sécurité des systèmes d'information

Pour appréhender la sécurité des systèmes d'information, il convient d'abord de préciser ce qu'est un système d'information ; la littérature le définit tantôt par ses attributs, tantôt par ses fonctions (Ein-Dor, Segev, & Shani, 1978). Dans une perspective fonctionnelle, il s'agit d'un ensemble organisé de ressources, matériel, logiciel, personnel, données et procédures conçu pour collecter, traiter, stocker et diffuser l'information sous toutes ses formes (Reix R. , 2002) (Aldosa & Boudriga, 2003). Plus généralement, un système d'information regroupe des composants interconnectés dont l'objectif est de soutenir la prise de décision, la coordination, le contrôle et l'analyse au sein d'une organisation.

La seule performance de ces processus est insuffisante ; pour contribuer véritablement à l'efficacité et à la résilience organisationnelle, ils doivent être entièrement sécurisés. La sécurité du système d'information se définit par la garantie des quatre critères fondamentaux de la valeur de l'information : disponibilité, intégrité, confidentialité et preuve/contrôle (non-répudiation), auxquels s'ajoutent souvent l'authentification, l'autorisation et la journalisation (Godart, 2002). Ces objectifs varient en fonction des enjeux propres à chaque organisation ; dans le secteur bancaire, où le SI représente un investissement majeur et un levier de performance commerciale (Traoré & Zeroual, 2023) (Zeroual, 2021), la perception qu'ont les acteurs de son rôle stratégique conditionne la mise en œuvre effective de ces garanties de sécurité.

- Quelles perceptions les acteurs des entreprises ont-ils de la sécurité du système d'information (SSI) ?

Selon la théorie de la contingence de Mintzberg (1982), la configuration organisationnelle module la responsabilité et la perception de la sécurité des systèmes d'information :

appliquée au contexte (SWIFT, Society for Worldwide Interbank Financial Telecommunication, 2022) et à l'évaluation ISO 27001 (ISO, 2013), elle montre que le Directeur Général voit avant tout dans la protection du réseau SWIFT une garantie de continuité des paiements transfrontaliers et de préservation de la réputation, la DSI, épaulée par le RSSI, traduit ces enjeux en politique ISO 27001 et contrôles CSP SWIFT, les managers intermédiaires en assurent la déclinaison opérationnelle et l'audit interne, tandis que les opérateurs, confrontés quotidiennement au traitement des messages MT, perçoivent la sécurité comme un ensemble de procédures à appliquer (MFA, chiffrement, journalisation) et nécessitent un accompagnement pédagogique. Cette pluralité de regards souligne que la conformité ISO 27001 du SI SWIFT ne peut reposer sur une vision technico-légale isolée : elle exige un engagement et une compréhension partagée à tous les niveaux de l'organisation pour transformer les bonnes pratiques en réflexes collectifs.

3. Évolution des systèmes d'information de l'outil opérationnel au pilier de la résilience organisationnelle

Le système d'information jusqu'ici considéré comme simple moyen d'informer l'ensemble des acteurs impliqués dans le fonctionnement de l'entreprise, grâce à des procédures de collecte, de traitement, de stockage et de diffusion des données bien établies, ne permet pas d'avoir une connaissance précise des capacités internes de l'entreprise et de l'environnement en mutation permanente. Une insuffisance qui trouve une réponse d'abord avec les travaux de recherches de Charles Wiseman qui donne une vision stratégique au système d'information (Rackoff, 1985) (Wiseman, 1988). Plus tard Hubert Tardieu et Bernard Guthmann abordent dans la même approche le système d'information comme support à la stratégie de l'entreprise ou levier de l'avantage concurrentiel de l'entreprise (Tardieu, 1991). Si le système d'information présente un avantage concurrentiel, la maîtrise d'une information de qualité est aussi d'un intérêt stratégique et donc la question quant aux enjeux de sa sécurité reste préoccupante. En effet, les organisations devraient réfléchir aux conséquences financières sur leurs activités, leurs ventes de produits et services, d'une interruption totale de tous leurs systèmes, voire de la simple perte de données sensibles (données clients). Des conséquences qui sans doute affecteraient la

résilience de l'organisation en termes de capacité à se développer bien, à continuer à se projeter dans l'avenir en dépit d'évènements déstabilisants, de conditions de vie difficiles, de traumatismes parfois sévères. Fort est de savoir que la contribution du système d'information à la résilience aux autres actifs de l'entreprise dépend de l'apport de l'utilisation d'une application ou d'un service informatique en termes de : la réduction de temps de travail, la diminution de litiges et de pertes d'affaires grâce à des informations plus fiables, l'obtention de chiffres d'affaires, l'amélioration d'une image de marque.

4. Positionnement de la recherche dans le champ de la sécurité de l'information

La norme ISO 27001 (ISO, 2013) s'est imposée comme le référentiel international incontournable pour concevoir et gouverner un Système de Management de la Sécurité de l'Information (SMSI), structuré selon le cycle Plan–Do–Check–Act et articulant un ensemble de politiques, de processus et de mesures techniques pour garantir la confidentialité, l'intégrité et la disponibilité des actifs informationnels, quels que soient le secteur et la taille de l'organisation. Cependant, sa mise en œuvre engendre des contraintes significatives : un investissement financier et en ressources humaines substantiel pour déployer et maintenir le SMSI, l'acquisition de compétences spécialisées (cryptographie, audit, gestion des incidents) et l'intégration complexe de ces exigences au sein des méthodologies de gestion de projet existantes, afin de préserver budgets et délais (Albarrán-Trujillo). Dans le contexte de la BEA, l'évaluation de la conformité du système SWIFT composante stratégique du traitement des paiements transfrontaliers nécessite une approche à la fois rigoureuse et pragmatique, combinant un pilotage de la sécurité aligné sur les processus opérationnels, un leadership fort de la direction et une formation continue des équipes pour assurer la robustesse et la pérennité du SMSI.

5. Approches d'évaluation de la conformité à ISO 27001

5.1 Méthodes d'évaluation

Plusieurs méthodes sont largement utilisées dans la littérature pour évaluer la conformité à la norme ISO/CEI 27001, et elles constituent également le socle méthodologique de notre étude appliquée au système SWIFT dans un contexte bancaire. Le cycle PDCA (Plan–Do–Check–Act), fréquemment cité comme un cadre fondamental pour le pilotage de la sécurité de l'information, permet de structurer la mise en œuvre et l'amélioration continue du SMSI, comme l'a souligné Junaid (Iqbal, 2023). En parallèle, l'utilisation de grilles

d'évaluation basées sur les 93 contrôles de l'annexe A de la norme ISO 27001 est courante pour réaliser une analyse des écarts, mesurer la maturité des dispositifs de sécurité et identifier les zones de non-conformité. (Apriany D. e., 2022) Mettent en avant l'importance de ces grilles pour formaliser l'évaluation, orienter les actions correctives et renforcer la résilience du système. À ces pratiques s'ajoutent les audits internes et externes qui, dans plusieurs études empiriques, sont décrits comme des leviers clés pour valider les pratiques en place et assurer un alignement effectif avec les exigences normatives. Notre recherche s'inscrit dans cette lignée méthodologique en combinant ces approches avec des outils complémentaires comme l'échelle de maturité SAMI et une checklist personnalisée, dans le but de produire un diagnostic approfondi et contextualisé du niveau de conformité du système SWIFT aux exigences de l'ISO 27001 dans le secteur bancaire algérien.

5.2 Intégration avec d'autres cadres de sécurité

L'intégration de la norme ISO 27001 avec d'autres cadres réglementaires et méthodologiques, tels que l'indice KAMI en Indonésie (Apriany A. e., 2023) ou la loi sur la protection des données personnelles (PDP Law) (Nugroho, 2025), illustre la nécessité d'une approche hybride combinant standards internationaux et exigences locales. Une telle démarche permet non seulement de renforcer globalement la posture de sécurité de l'information, mais également de faciliter l'alignement avec les obligations réglementaires spécifiques à chaque contexte national. Ce couplage stratégique optimise la résilience organisationnelle face aux risques cyber et démontre la flexibilité du cadre ISO 27001 dans des environnements réglementaires variés.

6. Analyse critique des méthodes d'évaluation de la conformité

Les méthodes d'évaluation de la conformité à la norme ISO 27001, bien que fondamentales pour assurer l'intégrité des systèmes de gestion de la sécurité de l'information (SMSI), ne sont pas exemptes de limites. L'évaluation par grilles, bien que systématique et permettant une cartographie précise des écarts, se heurte à une rigidité structurelle qui limite son adaptabilité aux contextes organisationnels spécifiques, en particulier dans les petites et moyennes entreprises (PME) où les ressources et les besoins diffèrent considérablement (Rianto, 2024). Par ailleurs, les audits internes et externes, bien que indispensables pour valider la conformité et identifier les non-conformités, s'avèrent souvent onéreux et tributaires de l'expertise des auditeurs, ce qui peut compromettre leur accessibilité et leur efficacité, notamment pour les organisations aux budgets restreints (Akindote, 2023). Enfin, le cycle PDCA (Plan-Do-Check-Act), bien que reconnu pour son

approche systématique et son orientation vers l'amélioration continue, présente une complexité opérationnelle non négligeable. Sa mise en œuvre requiert une culture de sécurité mature et une expertise approfondie, ce qui peut constituer un obstacle majeur pour les organisations en phase de transition ou disposant de capacités techniques limitées (Albarrán Trujillo, 2024).

- **Critiques du langage et des exigences d'ISO 27001 entre complexité technique et charge administrative**

La norme ISO 27001, bien que reconnue pour son cadre structuré et son adaptabilité, fait l'objet de critiques concernant son langage et ses exigences. D'une part, le langage employé dans la norme est souvent perçu comme technique et difficile à interpréter pour les non-experts, ce qui peut entraîner des incompréhensions et des erreurs d'application, notamment dans les organisations où les compétences en sécurité de l'information sont limitées (Junaid, 2023). Bien que cette technicité assure une précision nécessaire, elle peut également constituer une barrière à l'adoption pour certaines entreprises. D'autre part, la flexibilité de la norme, bien qu'étant un atout pour s'adapter à divers secteurs d'activité, peut conduire à des interprétations variées, voire contradictoires, ce qui complexifie sa mise en œuvre uniforme (Sant Gonzalez, 2023) . En ce qui concerne les exigences, l'Annexe A, qui liste 93 contrôles, est souvent jugée exhaustive mais complexe à appliquer, en particulier pour les petites et moyennes entreprises (PME) qui peuvent manquer de ressources pour les mettre en œuvre de manière complète (Albarrán Trujillo, 2024) . Enfin, la déclaration d'applicabilité, qui oblige les organisations à justifier l'exclusion de certains contrôles, est perçue comme une charge administrative supplémentaire, pouvant décourager les entreprises, notamment celles disposant de capacités limitées en gestion de projet (Rianto, 2024) .

7. Défis et lacunes dans l'implémentation d'ISO 27001

7.1 Complexité opérationnelle et ressources

La mise en œuvre d'ISO 27001 exige des ressources conséquentes, notamment en termes de compétences techniques et de documentation approfondie (Albarrán Trujillo, 2024). Par exemple, dans l'étude de (Rianto, 2024), la Banque Victoria International Tbk a rencontré des difficultés majeures dans la prévention des fuites de données et la gestion des menaces externes, en raison d'un manque d'outils spécialisés et de politiques formalisées.

7.2 Équilibre entre sécurité et performance opérationnelle

Un défi récurrent est de parvenir à un équilibre entre la sécurité des SI et la performance opérationnelle. (Akindote, 2023) Soulignent que les banques certifiées ISO 27001 doivent souvent réajuster leurs processus pour intégrer les exigences de la norme, ce qui peut entraîner des coûts supplémentaires et des perturbations opérationnelles.

7.3 Lacunes dans l'amélioration continue

L'étude de (Mekimah, 2022) révèle que de nombreuses organisations, comme l'entreprise portuaire de Skikda, peinent à mettre en place des mécanismes d'amélioration continue. Un taux de conformité global de 67,14 % indique des lacunes significatives dans des domaines clés, tels que la gestion des risques et la culture de sécurité.

8. Impact d'ISO 27001 sur le management des systèmes d'information et des projets

8.1. Renforcement de la gouvernance de la sécurité de l'information

L'adoption de la norme ISO/CEI 27001 constitue un levier stratégique pour la gouvernance des systèmes d'information, en offrant un cadre structuré pour la gestion des risques, la définition des responsabilités, et la mise en œuvre de contrôles adaptés. (Akindote, 2023) Soulignent que cette norme favorise une meilleure articulation entre les objectifs organisationnels et les dispositifs de sécurité, en professionnalisant la gestion de la cybersécurité au sein des institutions financières.

8.2 Consolidation de la confiance des parties prenantes

Selon Permadi et Lahindah (2025) , la conformité à la norme ISO/CEI 27001 influence de manière significative la perception des clients et partenaires en matière de fiabilité et de sérieux. Dans des environnements sensibles comme les banques, cette conformité devient un critère décisif pour la compétitivité, en rassurant les parties prenantes sur la protection des données et la résilience des infrastructures critiques.

8.3 Intégration dans les cycles de projet IT et de conformité

(Kristian Beckers, 2014) Proposent une approche méthodologique baptisée ISMS-CORAS, permettant d'intégrer ISO 27001 dans la planification et l'exécution des projets informatiques. Cette démarche facilite la génération automatique des livrables nécessaires à la documentation du SMSI, tout en assurant une cohérence entre les exigences de sécurité et les objectifs du projet. Dans le contexte de la BEA, cela se traduit par une meilleure

intégration des exigences normatives dans le pilotage des périmètres critiques, tels que le système SWIFT.

9. Perspectives internationales et études de cas

- **Contexte indonésien**

L'étude de (Rianto, 2024) sur la Banque Victoria International Tbk illustre les progrès réalisés en matière de sensibilisation à la sécurité, mais souligne également des lacunes dans la prévention des fuites de données et la gestion des menaces externes.

- **Contexte mexicain**

(Albarrán Trujillo, 2024) Mettent en avant les défis spécifiques aux PME mexicaines, notamment l'insuffisance de ressources et de compétences techniques, tout en proposant un guide pratique pour déployer un SMSI aligné sur ISO 27001.

- **Contexte algérien**

A travers l'étude de (Mekimah, 2022) , un taux de conformité moyen est de 67,14 % dans l'entreprise portuaire de Skikda, avec des lacunes significatives dans la gestion des risques et l'amélioration continue.

Tableau 1 Méthodes d'évolution de la conformité à ISO 27001

Méthode	Avantages	Critiques
Évaluation par grilles	Structuration claire, identification des écarts spécifiques aux risques bancaires	Manque de flexibilité, complexité pour les PME.
Audits internes/externes	Validation indépendante, identification des non-conformités critiques (Art. 6 de la Loi 09-04).	Coûts élevés, dépendance à l'expertise des auditeurs. Nécessité d'un engagement fort de la DSSI et des audits internes
Cycle PDCA	Approche systématique adaptée aux changements technologiques rapides (mobile banking, cloud), promotion d'une culture de sécurité mature.	Complexité de mise en œuvre, nécessite une culture de sécurité mature

Source : élaboré par nous-mêmes (données inspirées des articles).

Le tableau compare trois méthodes d'évaluation de la conformité à l'ISO 27001, chacune reflétant des compromis entre rigueur normative et adaptabilité organisationnelle. L'évaluation par grilles, bien que structurante pour identifier les écarts techniques (contrôles de chiffrement, gestion des accès), manque de flexibilité pour les PME, comme le souligne (Mekimah, 2022) : ces entreprises, souvent confrontées à des ressources limitées, peinent à aligner des checklists rigides sur leurs pratiques informelles. Les audits internes/externes, quant à eux, offrent une validation indépendante cruciale pour les institutions régulées (secteur bancaire), mais leur coût élevé et leur dépendance à l'expertise des auditeurs—souvent détachés des réalités terrain, les rendent inaccessibles pour de nombreuses PME (Akindote, 2023) . Enfin, le cycle PDCA (Plan-Do-Check-Act), bien que promouvant une amélioration continue et une réponse dynamique aux menaces (phishing, ransomware), exige une culture de sécurité mature, rare dans les contextes où la résistance au changement domine (Albarrán Trujillo, 2024). Ces limites expliquent pourquoi, malgré une conformité technique moyenne de 67,14 % en Afrique (Akindote, 2023) , les organisations oscillent entre rigidité normative et pragmatisme. Une approche hybride, combinant checklists prioritaires (Apriany A. e., 2023) et analyse qualitative des pratiques informelles (Lincoln, 2018), semble donc essentielle pour concilier exigences ISO et réalités opérationnelles, en particulier dans les secteurs régulés comme la banque, où les cybermenaces coûtent en moyenne 4,7 millions de dollars par incident (Khan, 2024) .

Tableau 2 : Intervalle de temps et recherches sur l'évaluation de la conformité à ISO 27001

Période	Thème principale	Détails et Contributions Clés
2000/ 2013	Émergence des méthodes d'évaluation et des premiers défis	Importance des grilles d'évaluation : Les premières grilles basées sur l'Annexe A d'ISO 27001 permettent d'identifier les écarts de conformité, mais leur rigidité limite leur adaptabilité aux contextes organisationnels spécifiques. (Albarrán Trujillo, 2024) Nécessité des audits internes/externes : Les audits sont essentiels pour valider la conformité, mais leur coût élevé et leur dépendance à l'expertise des auditeurs peuvent limiter leur accessibilité, en particulier pour les PME (Rianto, 2024). Adoption du cycle PDCA : Le cycle Plan-Do-Check-Act est reconnu pour son approche systématique et son orientation vers l'amélioration continue, mais sa mise en œuvre nécessite une culture de sécurité mature (Junaid, 2023) .
2014/ 2024	Intégration avec d'autres	Intégration avec des cadres locaux : La combinaison d'ISO 27001

	cadres et réglementations locales	avec des cadres locaux, comme l'indice KAMI en Indonésie, démontre l'importance d'une approche combinée pour répondre à la fois aux normes internationales et aux réglementations locales (Apriany A. e., 2023). Alignement sécurité-performance : Les recherches soulignent la nécessité d'aligner les objectifs de sécurité avec les priorités opérationnelles, en particulier dans les secteurs critiques comme la banque et la santé (Akindote, 2023). Complexité opérationnelle : Les études mettent en avant les coûts élevés et la complexité de mise en œuvre, notamment dans les PME, avec des propositions pour simplifier les processus et réduire les barrières à l'adoption (Albarrán Trujillo, 2024).
2017/2020	Perspectives internationales et études de cas	Contexte mexicain : Les PME mexicaines rencontrent des défis spécifiques, notamment l'insuffisance de ressources et de compétences techniques, ce qui complique la mise en œuvre d'ISO 27001 (Albarrán Trujillo, 2024). Contexte algérien : Dans l'entreprise portuaire de Skikda, un taux de conformité moyen de 67,14 % révèle des lacunes significatives dans la gestion des risques et l'amélioration continue (Mekimah, 2022). Contexte indonésien : La Banque Victoria International Tbk a réalisé des progrès en matière de sensibilisation à la sécurité, mais des lacunes persistent dans la prévention des fuites de données et la gestion des menaces externes (Rianto, 2024).
2020/ 2023	Critiques, solutions et équilibre sécurité-performance	Critiques du langage technique : Le langage technique d'ISO 27001 est souvent perçu comme difficile à interpréter pour les non-experts, ce qui peut entraîner des erreurs d'application et des incompréhensions (Junaid, 2023). Solutions proposées : L'utilisation du cycle PDCA et l'intégration avec des cadres locaux sont recommandées pour réduire la complexité opérationnelle et améliorer l'accessibilité de la norme pour les PME (Apriany A. e., 2023). Équilibre sécurité-performance : Les recherches soulignent la nécessité de trouver un équilibre entre les exigences de sécurité et les priorités opérationnelles, en particulier dans les secteurs où la performance est critique (Akindote, 2023). Amélioration continue : La mise en place de mécanismes d'évaluation et de révision réguliers est essentielle pour assurer une conformité durable et une gestion proactive des risques (Mekimah, 2022).

Source : élaboré par nous-mêmes (données inspirées des articles).

La mise en œuvre de la norme ISO/IEC 27001 a connu une progression notable depuis les années 2000, passant d'une approche centrée sur des audits standardisés basés sur

l'Annexe A à des stratégies plus souples et contextualisées. Si ces premiers outils ont permis d'identifier les écarts de conformité, leur manque d'adaptabilité a rapidement été souligné. Dès 2014, l'intégration de la norme dans des cadres réglementaires locaux, comme l'indice KAMI en Indonésie, a renforcé sa pertinence en conciliant exigences sécuritaires et réalités opérationnelles. Entre 2017 et 2020, des études menées au Mexique, en Algérie et en Indonésie ont mis en évidence les obstacles rencontrés par les PME, notamment en matière de ressources et de compétences techniques. Plus récemment, les travaux menés entre 2020 et 2023 ont remis en cause le langage complexe de la norme, encourageant des approches plus pragmatiques, comme l'adoption du cycle PDCA et l'hybridation avec des référentiels locaux. L'ensemble de ces évolutions souligne la nécessité d'une démarche adaptable, continue et ancrée dans le contexte organisationnel pour assurer une conformité pérenne et efficace à la norme ISO 27001.

10. Positionnement et originalité de la recherche

Cette étude se positionne à l'intersection de deux axes encore peu explorés dans la littérature académique : d'une part, l'évaluation de la conformité à la norme ISO 27001 dans le contexte bancaire algérien, et d'autre part, l'analyse ciblée d'un système d'information interbancaire aussi critique que SWIFT. Si les recherches existantes portent souvent sur des environnements industriels ou hospitaliers, rares sont celles qui abordent la conformité normative dans les institutions financières d'Afrique du Nord, en particulier au sein des services sensibles tels que la Direction de la Sécurité des Systèmes d'Information (DSSI). L'originalité de cette démarche repose sur un double ancrage :

- Pratique, par l'analyse fine des contrôles CSP SWIFT et leur correspondance avec l'annexe A de la norme ISO 27001, à travers une grille d'audit hiérarchisée, un modèle d'écart (gap analyses) et un plan d'action structuré.
- Empirique et humain, par la conduite d'entretiens semi-directifs auprès des acteurs clés (DSI, RSSI, auditeurs internes, responsables TI), permettant d'explorer les dynamiques réelles de mise en conformité, au-delà des prescriptions formelles.

En conclusion, cette revue de la littérature permet d'identifier les principaux enjeux, méthodes et défis relatifs à l'évaluation de la conformité à la norme ISO 27001, tout en soulignant les limites notables des approches actuelles, notamment dans des environnements critiques comme ceux intégrant le système de messagerie interbancaire SWIFT. Elle met en évidence le besoin urgent de méthodes d'évaluation plus souples,

contextualisées et adaptées aux exigences spécifiques du secteur financier, où la sécurité de l'information est directement liée à la confiance des partenaires et à la stabilité des transactions.

Les outils classiques d'évaluation tels que le cycle PDCA, les audits (internes/externes) ou les grilles associées aux contrôles de l'annexe A demeurent essentiels, mais se révèlent parfois inadaptés aux contraintes de systèmes complexes comme SWIFT, en raison de leur lourdeur administrative, de leurs coûts élevés et de leur faible agilité face à l'évolution rapide des menaces. Ces limitations sont particulièrement ressenties dans les établissements bancaires de taille moyenne, souvent confrontés à un manque de ressources humaines spécialisées, à une faible maturité des processus SSI et à des difficultés d'alignement entre sécurité, conformité réglementaire (comme les exigences de la BCE ou de CSP) et performance opérationnelle.

Cette étude se distingue par une analyse critique des méthodes d'évaluation existantes à la lumière du contexte spécifique de l'intégration de la norme ISO 27001 dans les infrastructures utilisant le système SWIFT. Elle vise à combler une lacune dans la littérature en abordant les défis pratiques rencontrés dans les environnements financiers, tout en proposant des pistes d'amélioration comme l'harmonisation des référentiels, la simplification des procédures de conformité, le renforcement de la formation continue des acteurs impliqués (DSI, RSSI, auditeurs), et la mise en œuvre de mécanismes agiles d'amélioration continue. En offrant ces recommandations concrètes, cette étude contribue à une meilleure compréhension des pratiques d'évaluation de la sécurité de l'information dans les systèmes critiques et à une consolidation de la résilience organisationnelle dans le secteur bancaire.

Dans un environnement économique de plus en plus complexe soumis à de nombreuses règles, la qualité et la normalisation semblent être deux notions inséparables pour assurer une performance et une pérennité à long terme des organisations.

Section 02 : Cadre conceptuel

L'analyse de la littérature existante nous a permis d'extraire des éléments pertinents pour l'évaluation de la conformité de la sécurité des systèmes d'information, en particulier dans le contexte bancaire. Cette section vise à clarifier les notions fondamentales mobilisées dans notre étude. Dans un premier temps, nous définirons le cadre de la norme ISO/CEI 27001 :2022 ainsi que les exigences du référentiel CSP SWIFT, afin de mieux cerner leur portée et leur complémentarité. Nous aborderons ensuite les concepts de sécurité de l'information, de contrôle technique et de conformité, qui constituent le socle conceptuel de cette recherche.

1. Système de management de la qualité

1.1 Notion de base du système de management de la qualité

1.1.1 La qualité

La qualité est un concept multidimensionnel qui repose avant tout sur la satisfaction des besoins des clients.

L'AFNOR définit la qualité comme « *un produit ou service de qualité dont les caractéristiques lui permettent de satisfaire les besoins exprimés ou implicites des consommateurs* ». (AFNOR, 2024)

Selon la norme ISO (2015) étend cette vision en affirmant que la qualité est « *la capacité d'un produit ou d'un service à satisfaire les besoins et attentes des clients et autres parties intéressées pertinentes, tout en répondant aux exigences légales et réglementaires applicables* ». Ces définitions mettent en évidence que la qualité ne se limite pas aux seules performances techniques d'un produit ou service. Elle dépend aussi de la perception du client et de la valeur concrète qu'il en retire. Une démarche qualité efficace repose donc sur une culture organisationnelle forte, ancrée dans les comportements, les processus et les actions, avec une attention constante à l'écoute du client, condition essentielle pour identifier ses besoins réels et y répondre de manière appropriée. (Pinet, Management de la qualité : vers un management durable, 2015, pp. 19-23)

1.1.2 Système de Management de la qualité

Selon ISO (2015) le système de management de la qualité est : « *Ensemble d'éléments corrélés ou en interaction d'un organisme, utilisés pour établir des politiques, des objectifs et des processus de façon à atteindre lesdits objectifs* ».

Selon ISO (2015). « *Partie d'un système de management relatif à la qualité* ». Le système de management de la qualité (SMQ) vise à optimiser les processus et ressources pour créer de la valeur durable. Il doit s'adapter aux enjeux internes et externes, s'appuyant sur l'engagement de la direction, la mobilisation des ressources et l'implication du personnel. Fondé sur l'amélioration continue, le SMQ évolue pour répondre aux attentes des parties prenantes, selon huit principes fondamentaux :L'organisme à l'écoute du client ; le leadership ; l'implication du personnel ; l'approche processus ; le management par approche système ; l'amélioration continue ; l'approche factuelle pour la prise de décision ; les relations mutuellement bénéfiques avec les fournisseurs. (Pinet, Découverte de la qualité : Conforme à la NF EN ISO 9001:2015, 2017, pp. 18-19)

1.2 La normalisation

Selon France (2009) définit la normalisation comme « *une activité d'intérêt général qui a pour objet de fournir des documents de référence élaborés de manière consensuelle par toutes les parties intéressées, portant sur des règles, des caractéristiques, des recommandations ou des exemples de bonnes pratiques, relatives à des produits, à des services, à des méthodes, à des processus ou à des organisations. Elle vise à encourager le développement économique et l'innovation tout en prenant en compte des objectifs de développement durable* ». La normalisation, qui repose sur des documents élaborés en collaboration avec diverses parties prenantes (producteurs, consommateurs, experts, régulateurs, société civile), encadre produits, services, méthodes, processus organisationnels et fonctionnement des entreprises. Supervisée par des organismes spécialisés, tels que l'Organisation internationale de normalisation (ISO), elle vise à établir des normes de haute qualité, contribuant ainsi au bien-être collectif. (Lachaud, Certifier la conformitéaux Autorisations uniquesde la CNIL:Un projet à portée de main, 2010, p. 16).

1.2.1 La norme

Selon le guide ISO/CEI (2004) définit la norme comme « *un document établi par19consensus par une institution reconnue qui fournit un ensemble de règles, de guides et de caractéristiques pour un usage régulier dans le but d'atteindre un degré d'ordre optimal dans un contexte donné* ».

Madame Agnès Grenard a mené une étude approfondie sur le processus de normalisation. Selon elle, une norme se définit comme *« une spécification technique présentée sous la forme d'un document qui détermine les caractéristiques des biens, des services ou des processus* » (Grenard, 2004). Une norme est un document officiel accessible à tous, élaboré par consensus entre toutes les parties prenantes. Elle sert de référence commune pour résoudre de façon répétée des problèmes techniques ou commerciaux rencontrés entre partenaires économiques, scientifiques, techniques et sociaux. (Lachaud, Certifier la conformitéaux Autorisations uniquesde la CNIL:Un projet à portée de main, 2010, p. 18)

1.2.2 L'Organisation Internationale de Normalisation (ISO)

L'Organisation internationale de normalisation (ISO), fondée le 23 février 1947 à Genève, trouve ses origines dans la Fédération ISA créée dans les années 1920. Suspendue pendant la Seconde Guerre mondiale, l'initiative fut relancée par l'ONU, menant à la création de l'ISO. Présente dans 167 pays, elle regroupe un seul organisme de normalisation par nation. Bien que les particuliers et entreprises ne soient pas membres, des experts peuvent y collaborer. L'assemblée générale annuelle fixe les orientations stratégiques, tandis qu'un conseil d'administration assure la gouvernance. Le terme « ISO » est parfois utilisé pour désigner un produit conforme à ses normes. (Robin, 2023)

1.3 Les normes et référentiels afférents à l'audit interne et à la sécurité de l'information

Le domaine des audits de systèmes d'information est complexe et nécessite des compétences pointues basées sur des normes et des référentiels faisant autorité. Ces cadres ont été conçus par des organismes spécialisés en collaboration avec des experts locaux afin de définir des exigences minimales garantissant la qualité et l'éthique des auditeurs, tout en guidant les parties prenantes vers les meilleures pratiques. (Lachaud, Certifier la conformitéaux Autorisations uniquesde la CNIL:Un projet à portée de main, 2010)

1.3.1 Les normes et référentiels applicables à l'audit interne

Les normes internationales de l'IIA constituent le principal référentiel encadrant la mission d'audit interne, complété par un code de déontologie définissant les principes et valeurs professionnels. Selon l'IFACI (2013), elles visent à : établir les principes fondamentaux de l'audit interne, offrir un cadre pour des missions à forte valeur ajoutée, définir des critères d'évaluation de son fonctionnement et encourager l'amélioration continue des

processus et opérations. Ces normes sont regroupées en trois catégories dans le cadre des CRIPP :

- **Les normes de qualification**, qui précisent les exigences relatives aux auditeurs et à leur organisation ;
- **Les normes de fonctionnement**, qui décrivent la nature des missions et les critères de qualité ;
- **Les normes de mise en œuvre**, qui détaillent les précédentes selon qu'il s'agit d'activités d'assurance ou de conseil.

La norme 1210.A3 précise : « *Les auditeurs internes doivent posséder des connaissances suffisantes des principaux risques et contrôles relatifs aux technologies de l'information, et des techniques d'audit informatisées susceptibles d'être mises en œuvre dans le cadre des travaux qui leur sont confiés* » (The Institute of Internal Auditors (IIA), 2017). Les normes s'appliquent tant aux individus qu'à la fonction d'audit interne. Tous les auditeurs doivent respecter les règles liées à l'objectivité, aux compétences et à la diligence professionnelle, tandis que les responsables de l'audit doivent veiller à la conformité globale du service avec ces exigences. (Lachaud, Certifier la conformitéaux Autorisations uniquesde la CNIL:Un projet à portée de main, 2010)

1.3.2 Les normes et référentiels applicables à la gestion de la sécurité de l'information

Plusieurs normes, méthodes et référentiels de bonnes pratiques en matière de sécurité des systèmes d'information sont disponibles. Ils sont constitués de guides méthodologiques ainsi que de moyens de garantir une démarche de sécurité cohérente. La sécurité de l'information évolue dans un cadre défini par les normes ISO 2700x et le CobiT. (Lachaud, Certifier la conformitéaux Autorisations uniquesde la CNIL:Un projet à portée de main, 2010)

1.4 Le référentiel

Un référentiel, selon CIGREF (2009), est « *une collection de bonnes pratiques sur un sujet donné* ». Lorsqu'il est largement diffusé et reconnu, il devient un standard. Dans le domaine des systèmes d'information (SI), un référentiel regroupe des données cohérentes, partagées par une communauté d'acteurs, et se caractérise par la centralité, la stabilité, la qualité, l'unité de sens et l'interopérabilité. Il joue un rôle centralisateur et confère une

validité reconnue à ceux qui s'y conforment, étant généralement établi par des experts. Dans le cadre de ce travail, seuls les référentiels pertinents pour la gestion des risques informatiques seront abordés.

Un référentiel normatif efficace doit clairement énoncer des règles simples et vérifiables, permettant une évaluation objective de la conformité. Cela implique l'existence de règles standardisées, d'une structure logique, ainsi que de méthodes d'audit externe fondées sur des critères mesurables. Pour illustrer ces exigences, trois référentiels technologiques seront étudiés. (CIGREF, 2009, p. 9)

A/ COSO (Committee of Sponsoring Organizations of the Treadway Commission)

Le COSO a été mis en place pour évaluer l'efficacité du contrôle interne dans les entreprises. Son adoption s'est largement répandue, notamment en réponse à la Loi sur la Sécurité Financière et à la loi Sarbanes-Oxley.

Ce cadre définit cinq piliers fondamentaux du contrôle interne, mis en œuvre par le conseil d'administration, les dirigeants et les employés, afin d'assurer le bon fonctionnement des opérations, la fiabilité des informations financières, et le respect des exigences légales. Ces cinq composantes sont :

- L'environnement de contrôle,
- L'évaluation des risques,
- Les activités de contrôle,
- L'information et la communication, à optimiser pour une meilleure circulation des données,
- La supervision, c'est-à-dire le contrôle du système de contrôle interne lui-même.

Le COSO II, qui constitue l'évolution de ce cadre, introduit la notion d'appétence au risque (Risk Appetite), définissant le niveau de risque que l'organisation est prête à accepter pour atteindre ses objectifs stratégiques. (CIGREF, 2009, p. 53)

B/ CobiT (Control Objectives for Information and related Technology)

Publié en 1996, le CobiT (Control Objectives for Information and Related Technologies) est une méthodologie d'évaluation et de gouvernance des services informatiques en entreprise. Il propose un ensemble de bonnes pratiques destinées à maîtriser et contrôler

l'environnement informatique, applicables à un système existant ou en cours d'implémentation.

Le CobiT couvre 34 processus répartis en quatre domaines :

- Planification et organisation
- Acquisition et mise en place
- Distribution et support
- Surveillance et évaluation

Ces processus permettent de répondre à 318 objectifs de contrôle, contribuant à :

- L'alignement des SI avec les objectifs métiers,
- Une meilleure gestion des ressources et des risques,
- L'optimisation de la valeur ajoutée par l'IT.

En matière de sécurité de l'information, CobiT insiste sur :

- L'alignement stratégique de la sécurité,
- La gestion des risques à un niveau acceptable,
- La protection des actifs et la gestion des ressources,
- La mesure des performances en sécurité,
- L'intégration de la sécurité dans les processus métiers.

Plus de 20 processus sur 34 intègrent la dimension sécurité, avec une importance particulière pour :

- **PO6** : Communication des objectifs du management
- **PO9** : Évaluation et gestion des risques
- **DS4** : Assurance de la continuité de service
- **DS5** : Sécurité des systèmes

Le CobiT est un outil central pour la gouvernance informatique, apportant un cadre structuré et des outils concrets pour la gestion des risques, la conformité et la création de valeur. (MERIYEM, 2017, pp. 14-16)

C/ IT Infrastructure Library – ITIL

Au début des années 1990, le gouvernement britannique a lancé une étude qui a conduit à la création de la bibliothèque ITIL (Information Technology Infrastructure Library), visant à établir les meilleures pratiques de gestion des services informatiques. En 2004, la version 2, composée de neuf livres, a mis l'accent sur l'alignement entre technologie et besoins métier, en décrivant les processus essentiels à la fourniture de services adaptés.

Adoptée mondialement, ITIL est reconnue pour améliorer le contrôle des services TI, notamment ceux externalisés, en apportant des résultats mesurables aux entreprises. En 2007, la version 3, structurée autour de cinq ouvrages, propose un cadre basé sur une amélioration continue des services :

- Stratégie de service : alignement stratégique et gouvernance,
- Conception de service : procédures et architectures pour concevoir les services,
- Transition de service : intégration entre métiers et opérations,
- Exploitation de service : efficacité opérationnelle,
- Amélioration continue : amélioration progressive des processus via le cycle PDCA.

Contrairement à la version précédente, ITIL v3 n'est pas centrée sur la certification, mais sur l'optimisation continue des services informatiques fournis. (MERIYEM, 2017, p. 14).

1.5 Cadre normatif ISO 27000 pour la gestion de la sécurité de l'information et de la cybersécurité

- **Historique de la série ISO/IEC 27000 :**

À la fin des années 1990, la BSI a publié la norme BS 7799 sur la sécurité de l'information. En 1998, une seconde partie a introduit les exigences pour un système de management de la sécurité de l'information (SMSI). Cette norme a été adoptée par l'ISO en 2000 sous le nom ISO 17799, comme référentiel de bonnes pratiques.

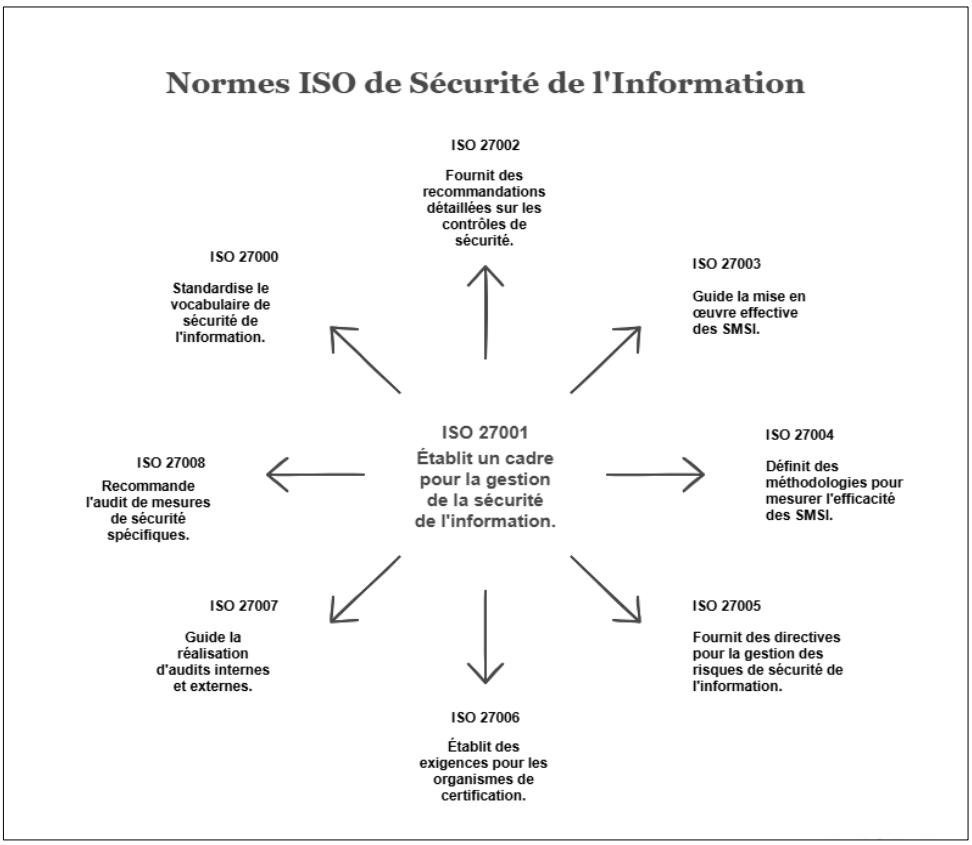
En 2002, la BSI publie BS 7799-2, que l'ISO adopte en 2005 sous la forme de la norme certifiable ISO/IEC 27001 :2005. ISO 17799 devient ISO 27002 en 2007. Ces deux normes

sont révisées en 2013 puis en 2022, afin de suivre l'évolution des risques numériques. (Adarsh, 2023, p. 13)

La série ISO/CEI 27000, Publiée par l'ISO en 2014 et adoptée par l'AFNOR en 2015, cette norme sur les systèmes de gestion de la sécurité de l'information a permis d'unifier les pratiques en Europe. Une révision majeure a eu lieu en 2018 pour intégrer les évolutions technologiques, tout en conservant l'esprit initial de protection des données et de cybersécurité. Bien que technique, elle constitue un référentiel utile pour renforcer la résilience numérique, à condition de l'adapter aux réalités propres à chaque organisation. (Pinet, 10 clés pour la sécurité de l'information ISO/IEC 27001:2022, 2023, p. 17)

La norme, regroupe plus d'une douzaine de normes visant à aider les organisations à renforcer la sécurité de l'information par la mise en place d'un système de management de la sécurité de l'information (SMSI). Ces normes visent à réduire les risques liés au personnel, aux processus et à la technologie. Au centre de cette série se trouve la norme ISO 27001, qui définit les exigences pour un SMSI efficace. (Adarsh, 2023, p. 13)

Figure 1: La famille de la norme ISO 27000



Source : élabore par nous-mêmes à partir de (MERIYEM, 2017, p. 12).

2. La sécurité du système d'information bancaire SWIFT

2.1 L'origine étymologique de la notion d'information

Au sens étymologique, le terme information trouve son origine dans le verbe latin *informare*, qui signifie *« donner forme à »* ou «s*e former une idée de* ». Ainsi, l'information est ce qui donne une forme à un concept ou à une idée. En fait, l'information désigne à la fois le message à communiquer et les symboles utilisés pour l'écrire, comme les lettres de l'alphabet, les chiffres, des dessins, des idéogrammes ou des pictogrammes.

Le concept « *information* » a eu bien des définitions différentes au cours de ces quarante dernières années de recherche en management des systèmes d'information. L'information est un concept polysémique. (McKinney, 2023) affirme à ce sujet que « *l'information est un caméléon sémantique*». Certains vont même jusqu'à affirmer que l'information ne peut pas être décrite par une définition. Pour (Cleveland, 1985), «*l'information est humaine*»: elle n'existe qu'au travers de l'observation de l'homme. Pourtant, l'information est souvent présentée par rapport à la « *donnée* ». Ainsi, l'information serait une «*donnée traitée* » douée de sens. La question sous-jacente : quel type de traitement permet de passer de la donnée à l'information ? Qui plus est, selon le contexte, l'information n'a pas forcément le même sens d'un individu à un autre, voire d'un contexte à l'autre. La connaissance est un état résultant d'une transmission d'information.

Pour synthétiser ces différentes acceptions, la conceptualisation la plus souvent citée dans la littérature est celle de (Ackoff, 1989). Il propose la hiérarchie « *données-information-connaissance* **»** qui va parfois jusqu'à la **«** sagesse **».** Cette hiérarchie, souvent abrégée « DIKW » (pour Data, Information, Knowledge, Wisdom), part des données, qui, par structuration et classement, produisent de l'information, qui, à son tour, conduit à la connaissance et, enfin, à la sagesse. Cette progression entre les différents niveaux de la hiérarchie DIKW est associée à une augmentation des niveaux de compréhension. Ainsi, dans une acception plus générique et dans le contexte d'entreprise, nous proposons la définition suivante : :« *L'information constitue l'ensemble des données et des connaissances créées, acquises, modifiées, gérées et détenues par l'entreprise. Elle représente son histoire, son patrimoine, ses savoir-faire, ses compétences. »* (DEIXONNE, 2012)

Une fois le concept d'information défini, examinons les outils dédiés à son traitement, à savoir l'informatique et le numérique.

2.2 Informatique vs Numérique

2.2.1 Informatique

Le terme informatique apparaît pour la première fois en 1957 dans un article du scientifique allemand (Steinbuch, 1957) intitulé « *Informatik: Automatische Informations verarbeitung*», soit « *Informatique: traitement automatique de l'information*».

En 1962, le terme est utilisé conjointement en France et aux États-Unis pour la dénomination de deux entreprises : la Société d'informatique appliquée (SIA), créée par Philippe Dreyfus, ancien directeur du Centre national de calcul électronique de Bull, et Informatics Inc., fondée par Walter Bauer. Contrairement à la France ou à l'Allemagne, le terme informatics n'est pas devenu la référence aux États-Unis. La raison est peu connue, mais réside probablement dans un dépôt de marque. En effet, lorsque l'Association for Computing Machinery (ACM), la plus grande association d'informaticiens au monde, sollicite la société Informatics Inc. afin de pouvoir utiliser le mot informatics en remplacement de l'expression computer machinery, l'entreprise éponyme décline la proposition. Cela ne lui a pas porté chance par la suite : rachetée par Sterling Software, la société Informatics a cessé ses activités en 1986. Formé de l'association des termes information et automatique, le néologisme est officialisé en France par le général de Gaulle, en conseil des ministres, qui l'aurait préféré à ordinatique. On notera que ce choix marque clairement la prédominance de l'information sur la machine ; on pressent l'enjeu majeur qu'elle représente pour les années à venir. En 1968, le mot Informatica fait son apparition en Italie et en Espagne, de même qu'informatics au Royaume-Uni.

Pour nous, et toujours dans un contexte professionnel, « *l'informatique représente la fonction ou le métier qui a pour but de concevoir, développer, intégrer, exploiter et maintenir les solutions matérielles et logicielles, ainsi que de fournir l'ensemble des services connexes* ». En cela, l'informatique se positionne clairement du côté du « producteur » vs le « consommateur ». Elle caractérise bien le métier qui œuvre autour des outils matériels, logiciels et services associés du « traitement automatique » de l'information. (DEIXONNE, 2012)

2.2.2 Numérique

Le terme numérique est de plus en plus usité dans notre vocabulaire. Il a même tendance à se substituer à l'informatique, induisant à la fois ambiguïté et confusion. Pour preuve, en 2013, le syndicat professionnel du secteur informatique et télécoms Syntec Numérique a décidé de rebaptiser les « *SSII* » (Sociétés de services et d'ingénierie en informatique) en « *ESN* » (Entreprises de services du numérique).

En fait, le terme numérique vient du latin numerus (« *nombre* », « *multitude* ») et signifie « *représentation par nombres* ». On oppose ainsi le calcul numérique (l'arithmétique) au calcul algébrique ou littéral (algèbre ou par lettres).

Le terme anglais digital vient lui aussi du latin (digitus signifie « *doigt* ») et, en anglais, digit désigne un chiffre (0 à 9). Les autres langues romanes (espagnol, italien) gardent le terme digital. Vraisemblablement, la notion de digital en anglais se rapportait à l'idée de compter avec ses doigts... Le rapport avec les chiffres traduit clairement la conversion du réel analogique vers le numérique. Exprimé autrement, numérique qualifie une représentation de l'information par un nombre fini de valeurs discrètes, s'opposant à analogique.

Dans le contexte économique, « *le numérique représente à la fois les informations, ainsi que l'ensemble des usages et traitements de ces informations, s'appuyant sur un outil informatique en vue d'une finalité métier* ». Aussi, le numérique est claire- ment objectiver. Il se positionne donc clairement du côté (des « *usages* » et des « *consommateurs* » vs le « *producteur* »). (DEIXONNE, 2012)

2.3 Le système d'information (SI)

Selon Salzman, Claude (2025), président du Club européen de la gouvernance des systèmes d'information :« *Trop souvent, on confond les termes système d'information et système informatique . Bien qu'ils soient voisins, ils ne sont pas synonymes. Le système d'information n'est pas le système informatique. C'est la source de conséquences non plus* ».

Ces définitions, proches de celle de l'informatique, soulèvent une question : système d'information et informatique sont-ils synonymes ? Si l'on prend cette fois-ci une référence plus internationale comme (Encyclopædia Britannica, n.d.) décrit le SI comme :« *Un ensemble intégré de composants pour collecter, stocker, traiter et communiquer de l'information. Les entreprises, organisations et individus en société contemporaine*

s'appuient sur les systèmes d'information pour gérer leurs opérations, concurrencer sur le marché, fournir des services et enrichir les vies personnelles. Par exemple, les corporations modernes utilisent des systèmes informatisés pour traiter les comptes financiers et gérer les ressources humaines ; les gouvernements locaux les utilisent pour offrir des services essentiels aux citoyens ; les individus les exploitent pour étudier, acheter, banker ou investir ».

On peut observer qu'elle reste dans une logique équivalente tout en étant récurrente, preuve, s'il en est, de la difficulté à donner une définition claire et précise. Passons à présent à (Encyclopædia Britannica, n.d.) précise :« *Un système d'information est un ensemble de ressources (personnel, logiciels, processus, données, matériels, équipements informatiques et de télécommunication) permettant la collecte, le stockage, la structuration, la modélisation, la gestion, la manipulation, l'analyse, le transport, l'échange et la diffusion d'informations (textes, images, sons, vidéos) au sein d'une organisation. Parmi les ressources informatiques figurent les bases de données, les ERP (Enterprise Resource Planning), les CRM (Customer Relationship Management), les SCM (Supply Chain Management) et les ERM (Employee Relationship Management)* » (Universalis, n.d.)

(Rowe, 2004, pp. 15-34) Ajoutent :« *Un système d'information est un ensemble d'acteurs sociaux qui mémorisent et transforment des représentations via des technologies de l'information et des modes opératoires.* »

Enfin, selon Reix, Robert (2004), propose : « *Un système d'information est un ensemble organisé de ressources (matériel, logiciel, personnel, données, procédures) permettant d'acquérir, de traiter, de stocker des informations (sous forme de données, textes, images, sons, etc.) dans et entre des organisations.* » (Monaco, 2012/2013)

Le système d'information a pour premier objectif, donc, de réduire l'incertitude face à la complexité et aux changements environnementaux

À cet effet, trois rôles sont attribués aux SI au sein des organisations :

- **Support aux opérations (le niveau fonctionnel)**

Ce rôle correspond à l'utilisation des SI dans les grands domaines de gestion de l'entreprise (gestion commerciale, gestion de production, gestion comptable et financière, gestion du personnel, gestion du stock). Ces derniers se matérialisent au niveau de

l'entreprise par des outils de reporting représentés sous forme d'ERP. Dans cette logique, on peut dire que l'existence même du SI est encore plus liée à son utilisation aux niveaux opérationnels qui doivent alimenter ce dernier en données, et donc aux outils de gestion associés. Le SI est donc le support informationnel des outils de gestion permettant les échanges de flux d'informations entre les entités.

- **Support à la gestion et à la prise de décision (niveau tactique)**

Le SI fournit aux opérationnels, managers et dirigeants des indicateurs pertinents (tableaux de bord, rapports analytiques) pour éclairer leurs décisions. Il transforme les données brutes en informations exploitables, permettant une gestion proactive des ressources et des risques. (Monaco, 2012/2013)

2.3.1 Les types de système d'information

Les systèmes d'information (SI) se divisent en plusieurs types selon leurs fonctions : les systèmes d'exploitation gèrent les opérations courantes, les systèmes transactionnels enregistrent les activités commerciales, et les systèmes d'information de gestion (SIG) soutiennent la prise de décision à différents niveaux. Les systèmes d'information stratégiques (SIS), en particulier, contribuent à créer un avantage concurrentiel en automatisant des fonctions clés ou en analysant des données externes, comme le précisent Tardieu et Guthmann (1991). Dès lors, le SI devient un levier stratégique majeur. Toutefois, cette centralité rend indispensable une sécurité rigoureuse, notamment pour les systèmes traitant des données sensibles comme SWIFT, afin de préserver la performance et la pérennité de l'entreprise. (Monaco, 2012/2013)

2.4 Le système d'information SWIFT

2.4.1 Histoire

Le réseau SWIFT (Society for Worldwide Interbank Financial Télécommunication) a été créé en 1973 à Bruxelles par un groupement de 239 banques issues de 15 pays. Il répondait à un besoin pressant de modernisation des communications interbancaires internationales, jusqu'alors assurées par le système Telex, jugé peu fiable en raison de ses failles en matière de sécurité et de manque de standardisation, ce qui augmentait les risques d'erreurs et de fraudes.

Le système SWIFT est devenu opérationnel en 1977, connectant dès le départ 518 institutions financières réparties dans 22 pays. Sa mission était de fournir une plateforme de messagerie interbancaire fiable, rapide et sécurisée.

SWIFT est structuré en tant que société coopérative de droit belge (SCRL), avec son siège social situé à l'adresse suivante : Avenue Adèle 1, 1310 La Hulpe, en Belgique, à proximité de Bruxelles. (SWIFT)

2.4.2 Le système SWIFT

Contrairement à une idée répandue, SWIFT n'est pas un système de transfert de fonds à proprement parler, mais un réseau de messagerie hautement sécurisé. Il permet aux banques et institutions financières d'échanger des instructions relatives aux paiements, aux transactions sur titres ou aux opérations de change. Ces échanges reposent sur des formats de messages normalisés, principalement :

- Les messages de type MT (Message Type),
- Ainsi que la norme ISO 20022, basée sur le langage XML, dont l'adoption est en cours de généralisation. Chaque entité participante est identifiée par un code BIC (Bank Identifier Code), également appelé code SWIFT, assurant la traçabilité et l'unicité des communications. (SWIFT)

2.4.3 Évolutions techniques et sécuritaires récentes

A. Infrastructure technique actuelle

Le réseau repose désormais sur SWIFT Net, une plateforme hautement sécurisée assurant la fiabilité des échanges financiers.

B. Norme ISO 20022

Progressivement mise en place pour remplacer les anciens messages MT, cette norme basée sur le format XML améliore la clarté des données échangées et renforce l'interopérabilité entre systèmes. Sa généralisation, notamment dans les paiements transfrontaliers, est prévue d'ici 2025.

C. SWIFT GPI (Global Payments Innovation)

Introduit en 2017, ce service optimise les paiements internationaux en offrant une visibilité en temps réel, tout en garantissant rapidité, transparence et traçabilité.

D. SWIFT CSP (Customer Security Programme)

Suite à plusieurs cyberattaques importantes, dont celle subie par la Banque centrale du Bangladesh en 2016, SWIFT a instauré un programme de sécurité obligeant ses utilisateurs à respecter des normes strictes en matière de cybersécurité, incluant des contrôles réguliers, des audits et une gouvernance renforcée. (SWIFT)

2.4.4 Rôle stratégique de l'administrateur SWIFT

L'administrateur SWIFT, également appelé Security Officer, occupe une fonction clé dans la gestion sécurisée du système d'information connecté au réseau SWIFT. Il assure la conformité réglementaire, la sécurité opérationnelle et la continuité du fonctionnement de l'infrastructure locale. Parmi ses responsabilités principales, on retrouve :

- Gestion des accès : définition des profils utilisateurs et attribution des droits d'accès selon le modèle RBAC (Role-Based Access Control).
- Surveillance de la sécurité : supervision continue des dispositifs de protection tels que les pare-feu, mise en œuvre de l'authentification forte, et analyse régulière des journaux d'activité.
- Mise en œuvre du SWIFT CSP : veille à l'application rigoureuse des exigences de sécurité définies par l'organisation centrale de SWIFT.
- Maintenance des systèmes : assure les mises à jour logicielles et l'installation des correctifs de sécurité nécessaires.
- Gestion des audits : organise l'archivage et la documentation des journaux pour répondre aux contrôles internes et externes.
- Coordination avec SWIFT : agit comme point de contact avec les équipes de support technique et de conformité de SWIFT. (SWIFT)

2.5 Notion de sécurité du système d'information

La sécurité de l'information a pour objectif de protéger à la fois les données confidentielles et les données publiques. Par ailleurs, elle contribue à garantir l'intégrité et la disponibilité des informations pour la communauté. En assurant la confidentialité, elle offre également le niveau de secret nécessaire. Les informations confidentielles incluent notamment les données personnelles, commerciales, expertes, officielles et les secrets d'État. (Monaco, 2012/2013)

2.5.1 La gouvernance de l'information

La gouvernance de l'information (IG) englobe l'ensemble des méthodes de gestion et de partage approprié des données ou des informations. Elle concerne notamment les données clients collectés numériquement (Mikalef, 2020). (Smallwood, 2014) Définit la gouvernance de l'information comme « *une caractéristique distinctive des organisations bien gérées, qui améliore l'efficacité opérationnelle et renforce les capacités de conformité en exploitant l'information comme une ressource stratégique essentielle, tout en utilisant largement ces informations pour créer de la valeur pour l'organisation* ». Cette définition se révèle précise, car la gestion de l'information inclut la création, l'utilisation, l'évaluation, le stockage, l'archivage et la suppression des données. Elle reflète également la manière dont l'information est utilisée et gérée. Il s'agit d'une pratique nécessaire visant à limiter les risques liés à la gestion des données tout en garantissant la conformité réglementaire. Les activités clés de la gouvernance de l'information comprend la gestion des métadonnées, les opérations de données, la gestion des données, l'architecture des données, la qualité des données et les données primaires. (Monaco, 2012/2013)

2.5.2 Importance de la gouvernance de l'information (IG) et de la sécurité de l'information (IS) dans la gestion de l'information

La gouvernance de l'information joue un rôle essentiel dans la protection des données et la réduction des risques juridiques, notamment en cas de litiges ou d'enquêtes gouvernementales (Adams, 2020). Elle permet aussi aux entreprises de classer les données selon leur niveau de risque, facilitant ainsi leur gestion. Parallèlement, la gestion de la sécurité de l'information concerne l'ensemble des politiques et des mesures mises en œuvre pour protéger les actifs informationnels contre les menaces et vulnérabilités. Elle vise à garantir la continuité des activités, réduire les risques, optimiser les opportunités d'affaires et le retour sur investissement. La sécurité repose sur des éléments variés : procédures, politiques, structures organisationnelles, moyens techniques et humains. Ces mesures doivent être régulièrement mises à jour pour répondre aux objectifs fixés. L'adoption d'un Système de Management de la Sécurité de l'Information (SMSI), tel que défini par la norme ISO/CEI 27001, est donc indispensable. Cette norme met l'accent sur la confidentialité, intégrité et disponibilité des informations tout au long de leur cycle de vie. La sécurité implique aussi une classification rigoureuse des actifs et des politiques de contrôle d'accès strictes. Enfin, la sécurité de l'information n'est plus uniquement une responsabilité technique ; elle est devenue un enjeu stratégique pour les entreprises. À

court terme, elle garantit un accès approprié à l'information, à moyen terme elle assure la cohérence du système, et à long terme, elle renforce la confiance des utilisateurs et partenaires (Deyrieux, 2003).

2.5.3 Principes fondamentaux de la sécurité du système d'information

La sécurité des systèmes d'information (SSI) repose sur cinq piliers :

- **L'intégrité** : qui assure que la donnée reçue est la même que celle qui a été émise, c'est-à-dire qu'elle n'a pas été corrompue. L'altération des données (le manque d'intégrité) peut conduire à la prise de mauvaises décisions ;
- **La confidentialité** : qui assure que la donnée reste privée durant la transmission pour que seules les personnes concernées aient la possibilité de la traiter. Il faudrait pour cela un message crypté ou une clé d'accès détenue uniquement par le(s) destinataire(s) concerné(s). La divulgation d'informations privées (perte de la confidentialité) ou le transfert d'informations privées à un destinataire autre que celui concerné peut affecter la crédibilité de l'entreprise et surtout favoriser la concurrence ;
- **La disponibilité** : qui assure que la donnée est présente et accessible à tout moment. L'indisponibilité des informations en temps réel pourrait entraîner un retard considérable dans les tâches à accomplir et occasionner par la suite la perte de clients et donc des pertes financières ;
- **La non-répudiation** : qui permet de s'assurer de l'identité réciproque à la fois de l'émetteur et du destinataire. Ce qui permet de garantir qu'une transaction ne peut être niée par aucun des correspondants. Déroger au principe de non répudiation entraîne une non-traçabilité des conversations ou des messages entre l'émetteur et le destinataire et donc un non-suivi quant au respect de la confidentialité des informations.
- **L'authentification** : qui permet de s'assurer de la véracité de l'identité de l'utilisateur qui souhaite accéder à des données à accès restreint. Missions et Objectifs de la sécurité du système d'information Selon le site Eduscol (2015), « *la SSI, c'est donc la sécurité du système informatique ». « Le système informatique est le support technique du SI et sa partie croissante*. » Il comprend : « *les technologies de*

l'information, les ordinateurs, les applications, les réseaux et les autres systèmes qui permettent à tous d'accéder à l'information, de l'analyser, de la créer, de l'échanger et de l'utiliser ».

Le besoin de maintenir l'intégrité de l'information et de protéger les actifs informatiques exige un processus de gestion de la sécurité. Ce processus comprend la mise en place et maintenance de rôles et responsabilités, de politiques, de plans et de procédures informatiques. (Ghernaouti-Hélie, Sécurité Internet : Stratégies et technologies, 2000)

La gestion de la sécurité implique également une surveillance, des tests et des actions correctives en cas d'incidents ou de découvertes de failles. Une gestion efficace protège tous les actifs informatiques pour minimiser les conséquences des vulnérabilités et des incidents de sécurité.

La protection de l'information est : « *Une démarche consciente visant à protéger, au sein de l'entreprise étendue, ce qui mérite de l'être, tant au niveau des données que des supports d'information ». Cette démarche implique un système de gestion, une identification des informations sensibles, une analyse des risques, des acteurs avec des rôles et responsabilités définis, et un programme de réduction des risques.* » (Claude, 2012) .

Ainsi, mettre en place la sécurité de l'information dans le système d'information permet à l'entreprise de prévenir des incidents majeurs et de limiter leur impact néfaste sur son environnement. (MEDROMI, 2013)

Selon Ghernaouti-Hélie, S. (2000), l'objectif de la sécurité des systèmes d'information est « *de garantir qu'aucun préjudice ne puisse menacer la pérennité de l'entreprise* ». Cela consiste à réduire la probabilité de concrétisation des menaces, à en limiter les dommages ou dysfonctionnements, et à permettre un retour à un fonctionnement normal à des coûts et délais acceptables en cas de sinistre. La sécurité ne génère pas directement de profits, mais évite des pertes. Elle s'inscrit dans une stratégie préventive liée à l'intelligence économique.

Pour atteindre l'objectif de sécurité de l'information, les données et les informations doivent être protégées contre toute modification non autorisée en spécifiant des pouvoirs dans le système de contrôle interne ou par la direction de l'entreprise. (Ebondo Wa Mandzala, 2006)

2.5.4 L'importance de la sécurité de l'information consiste en les points suivants

Les éléments cités dans notre texte sont extraits du livre (Linlaud, 2003, pp. 55-80)

- Les secteurs de la sécurité militaire et économique dépendent de l'exactitude et de la pertinence des informations.
- Les pays doivent disposer de mesures de sécurité viables couvrant les risques qui peuvent survenir en traitant avec d'autres parties.
- La nécessité croissante de créer un environnement électronique sécurisé au service des secteurs privé et public.
- La croissance rapide des utilisations des applications électroniques qui nécessitent un environnement sécurisé.
- La nécessité de protéger l'infrastructure du réseau de l'information afin de maintenir la continuité des activités.
- À mesure que la technologie de l'information se développe et prospère, des possibilités de cybercriminalité se sont multipliées.

3. ISO 27001 comme socle, complété par CSP SWIFT et PCI-DSS

Dans cette partie, nous présentons donc en priorité la norme ISO 27001, tout en élargissant l'analyse aux deux cadres sectoriels étroitement liés à la sécurité bancaire et financière : le SWIFT Customer Security Programme (CSP), développé spécifiquement pour les institutions utilisant le réseau SWIFT, et la norme PCI-DSS, centrée sur la protection des données de cartes bancaires. L'objectif est d'offrir une lecture comparative entre ces référentiels, tant en termes de structure que d'approche de la conformité et des contrôles de sécurité.

3.1 la norme ISO 27001

La norme ISO/IEC 27001, intitulée "Sécurité de l'information, cybersécurité et protection de la vie privée – Systèmes de management de la sécurité de l'information – Exigences", La norme constitue la référence internationale en matière de système de management de la sécurité de l'information. Publiée initialement en 2005 par l'Organisation internationale de normalisation, elle définit les exigences pour établir, mettre en œuvre, maintenir et améliorer continuellement un SMSI. Elle est conçue pour aider les organisations à protéger leurs actifs informationnels critiques, à identifier les risques de cybersécurité et à se

conformer aux exigences réglementaires relatives à la confidentialité, l'intégrité et la disponibilité des données. (Adarsh, 2023)

Conçue selon une approche générique et adaptable, la norme ISO 27001 est applicable à tout type d'organisation, quel que soit son secteur d'activité. Elle repose sur une structure commune à d'autres normes de management telles que l'ISO 9001 (qualité) ou l'ISO 14001 (environnement), facilitant ainsi l'intégration de systèmes de gestion multiples au sein d'un cadre cohérent. (FERNANDEZ-TORO)

L'ISO 27001 spécifie des processus permettant à une entreprise de construire, gérer et entretenir un système de gestion de la sécurité de l'information robuste fondé sur le cycle PDCA (Planifier-Déployer-Contrôler-Agir) d'amélioration continue.

- **Planifier (établissement du SMSI) :** définir la politique, les objectifs, les processus et les procédures du SMSI liés à la gestion du risque et à l'amélioration de la sécurité de l'information afin de fournir des résultats conformes aux politiques et aux objectifs globaux de l'organisation.
- **Déployer (mise en œuvre et fonctionnement du SMSI) :** mettre en œuvre et exploiter la politique, les mesures, les processus et les procédures du SMSI.
- **Contrôler (surveillance et réexamen du SMSI) :** évaluer et, le cas échéant, mesurer les performances des processus par rapport à la politique, aux objectifs et à l'expérience pratique, puis en rendre compte aux dirigeants pour réexamen.
- **Agir (mise à jour et amélioration du SMSI) :** entreprendre les actions correctives et préventives sur la base des résultats de l'audit interne du SMSI, de la revue de direction ou d'autres informations pertinentes, afin d'améliorer continuellement le système.
- Vérifier que toutes les tâches relatives à la sécurité sont vraiment exécutées, que ce soit par des humains ou des automatismes ;
- Identifier les actions à réaliser pour corriger les non-conformités aux règles de sécurité.

Le suivi du système de gestion de la sécurité de l'information doit s'appuyer sur des audits réguliers, des rapports d'incidents et les retours des parties prenantes afin d'évaluer son efficacité. La norme ISO/IEC 27001 impose ainsi des mécanismes formels d'évaluation

des risques, d'audits internes et de gestion des non-conformités. Toutefois, malgré ce cadre rigoureux, elle présente une limite notable : l'absence de métriques normalisées, ce qui complique la comparaison entre organisations certifiées (MEDROMI, 2013).

3.2 Architecture de la norme ISO/IEC 27001

La norme NF ISO/IEC 27001 définit les exigences pour établir, mettre en œuvre, gérer et améliorer continuellement un système de gestion de la sécurité de l'information. Elle constitue la référence de base pour la certification en matière de sécurité des données.

Sa structure s'aligne sur celles des autres grandes normes de gestion comme :

- NF ISO 9001 (système de management de la qualité).
- NF ISO 14001 (système de gestion environnemental).
- ISO/IEC 20000-1 (gestion des services informatiques).

Cette harmonisation, basée sur une structure de haut niveau, facilite l'intégration des systèmes de gestion au sein d'une organisation. Elle permet également de mutualiser les efforts en termes de conformité, de pilotage et d'audit.

Par conséquent, lorsqu'une entreprise est concernée par plusieurs référentiels, il est conseillé d'opter pour une certification multiple (par exemple, ISO 9001 et ISO 27001, ou ISO 20000-1 et ISO 27001). Cette approche favorise des économies d'échelle, améliore la cohérence des processus et renforce la gouvernance globale du système de gestion.

Sur le plan structurel, la norme ISO 27001 est composée de dix clauses principales. Les clauses 4 à 10 définissent les exigences pour mettre en place, exploiter et améliorer continuellement un système de management de la sécurité de l'information. Ces exigences couvrent :

- L'analyse du contexte organisationnel (clause 4),
- L'engagement du leadership (clause 5),
- La planification des risques (clause 6),
- La mobilisation des ressources et supports (clause 7),
- La mise en œuvre des activités opérationnelles (clause 8),
- L'évaluation de la performance (clause 9),

- L’amélioration continue du système (clause 10). (Pinet, 10 clés pour la sécurité de l'information ISO/IEC 27001:2022, 2023)

Tableau 3 : Les clauses de la norme 27001.

Clauses	**Exigences**
Clause 4 : Contexte de l’organisation	1.La compréhension de l’organisme et de son contexte. 2. La compréhension des besoins et des attentes des parties prenantes/intéressées. 3. La détermination du domaine d’application du SMSI 4. Le système de management de la sécurité de l’information
Clause 5 : Le leadership	1.Leadership et engagement de la direction 2. La politique sécurité 3. Rôles, responsabilités et autorités au sein de l’organisation
Clause 6 : Planification	1. Actions à mettre en œuvre face aux risques et opportunités 2. Appréciation des risques de sécurité de l’information 3. Traitement des risques de sécurité de l’information 4. Objectifs de sécurité de l’information et plans pour les atteindre 5. Planification des modifications
Clause 7 : Supports	1. Ressources 2. Compétences 3. Sensibilisation 4. Communication 5. Informations documentées
Clause 8 : Fonctionnement	1. Planification et contrôle opérationnels 2. Appréciation des risques de sécurité de l’information 3. Traitement des risques de sécurité de l’information
Clause 9 : Évaluation de la performance	1.Surveillance, mesurage, analyse et évaluation 2. Audit interne 3. Revue de direction

Clause 10 : Amélioration	1. Amélioration continue 2. Non-conformité et action corrective

Source : élaboré par nous-mêmes selon (Pinet, 10 clés pour la sécurité de l'information ISO/IEC 27001:2022, 2023).

Remarque : Bien que la norme ISO 27001 offre une certaine flexibilité dans le choix des contrôles de l'annexe A, il est impératif de traiter tous les risques identifiés. Certains contrôles peuvent être mis de côté s'ils ne sont pas pertinents pour votre organisation, mais chaque exception doit être justifiée et documentée dans la Déclaration d'Applicabilité (SoA).

3.3 Mise en œuvre du PDCA et structure de l'Annexe A de la norme ISO/IEC 27001

3.3.1 Application du modèle PDCA dans la norme ISO/IEC 27001

Le cycle PDCA (Plan-Do-Check-Act), également appelé roue de Deming, constitue le socle méthodologique de nombreuses normes de management, dont l'ISO/IEC 27001. Développé initialement par Walter A. Shewhart puis formalisé et diffusé par W. Edwards Deming dans les années 1950 au Japon, ce modèle vise l'amélioration continue des processus, produits et services. Intégré dans des démarches qualité comme Kaizen, Lean ou les référentiels ISO 9001, ISO 14001 et ITIL, le PDCA s'est imposé comme un cadre de pilotage structuré et universel. Dans le contexte de la gestion de la sécurité de l'information, ce cycle permet à l'organisation de planifier sa stratégie de sécurité (Plan), de la déployer (Do), d'en vérifier l'efficacité (Check), puis de l'ajuster en fonction des écarts identifiés (Act). L'ISO 27001 en fait une application directe dans la construction et le suivi du SMSI, assurant une dynamique d'amélioration continue essentielle à la résilience organisationnelle face aux menaces cybernétiques en constante évolution (Ahanda, 2009, p. 263).

3.3.2 Application

La mise en œuvre de la méthode PDCA est souvent représentée par la roue de Deming qui comporte quatre étapes :

- **Le P (plan) pour planifier:**

  - Utiliser les données existantes pour faire des prévisions.

  - Définir les conditions d'un essai ou d'un changement.

  - Définir les conditions de mesure et d'analyses des résultats.

- **Le D (do) pour réaliser :**

- Faire l’essai ou le changement dans les conditions prévues.

- Enregistrer les résultats.

- **Le C (chek) pour vérifier :**

  - Analyser et mesurer les résultats.

  - Évaluer ce qui a été appris.

- **L'A (act) pour (réagir, corriger, exécuter) :**

  - Mettre en application le changement envisagé ou recommencer un nouveau cycle (Ahanda, 2009).

3.3.3 Les contrôles de l’annexe A de la norme ISO 27001

L'annexe A de la norme ISO 27001 :2022 comprend 93 contrôles, répartis en quatre catégories :

Article 5 : Contrôles organisationnels (37 contrôles)

Article 6 : Contrôles des personnes (8 contrôles)

Article 7 : Contrôles physiques (14 contrôles)

Article 8 : Contrôles technologiques (34 contrôles)

Lors de la mise à jour de la norme ISO 27001 :2013 en 2022, l'Organisation internationale de normalisation a ajouté 11 nouveaux contrôles. Il s'agit de :

A.5.7 : Renseignements sur les menaces

A.5.23 : Sécurité des informations pour l'utilisation des services cloud

A.5.30 : Préparation des TIC pour la continuité des activités

A.7.4 : Surveillance de la sécurité physique

A.8.9 : Gestion de la configuration

A.8.10 : Suppression des informations

A.8.11 : Masquage des données

A.8.12 : Prévention des fuites de données

A.8.16 : Activités de surveillance

A.8.23 : Filtrage Web

A.8.28 : Codage sécurisé. (Adarsh, 2023)

Selon Adarsh, Nair et Greeshma M. R. (2023), « *l'application des contrôles de l'Annexe A de la norme ISO/IEC 27001 doit être adaptée au contexte propre de chaque organisation. La sélection des mesures repose sur une évaluation interne des risques, et les contrôles exclus doivent être dûment justifiés dans la Déclaration d'applicabilité (SoA). Cette flexibilité permet à chaque entité de répondre aux exigences réglementaires et contractuelles tout en maintenant une pertinence opérationnelle du SMSI* ».

3.4 Programme de sécurité clientèle (CSP) de SWIFT

Depuis 2016, le Programme de sécurité clientèle (CSP) de SWIFT renforce la cybersécurité de ses utilisateurs face à des cybermenaces croissantes. Il repose sur le Cadre de Contrôle de la Sécurité des Clients (CSCF), composé de contrôles obligatoires et recommandés, alignés sur des normes internationales telles qu'ISO/IEC 27000, NIST et PCI-DSS. Ces contrôles visent trois objectifs clés : sécuriser l'environnement local, restreindre les accès, et détecter/réagir aux menaces.

Chaque année, les utilisateurs doivent attester leur conformité via l'application KYC-SA, selon la version actualisée du CSCF publiée en juillet. Ce processus favorise la transparence et l'évaluation des risques entre institutions. L'évolution du CSCF repose sur une concertation communautaire, soutenue par un groupe de travail dédié et le Comité de surveillance SWIFT, pour garantir sa pertinence face aux menaces émergentes (SWIFT, 2021).

3.4.1 Enjeux du CSP SWIFT (Customer Security Programme)

Le Programme de sécurité clientèle (CSP) de SWIFT impose aux institutions financières une auto-évaluation annuelle de leurs dispositifs de sécurité, pouvant être accompagnée d'un audit par un prestataire externe qualifié. Dans une banque, la zone SWIFT constitue le lien entre le back-office et les réseaux externes, protégée par un cadre de sécurité local articulé autour de trois objectifs fondamentaux et huit principes directeurs.

Depuis fin 2021, le cadre d'évaluation indépendante (IAF) rend obligatoire une validation externe. Celle-ci peut être réalisée soit par une entité de contrôle interne indépendante des opérations SWIFT (comme l'audit interne), soit par un auditeur externe compétent en cybersécurité et en gestion des risques informationnels (SWIFT, 2021).

3.4.2 Objectifs et principes de CSP SWIFT

- **Diversifier les défenses et réduire les vulnérabilités :** il est essentiel d'établir des partitions réseau solides, de restreindre strictement le trafic Internet entrant et sortant, de maintenir régulièrement les systèmes à jour et renforcés, et de séparer les processus d'authentification des utilisateurs de ceux du réseau.

- **Gérer avec précaution les identités et les autorisations :** Le réseau SWIFT de l'établissement requiert une gestion méticuleuse des accès au système et des privilèges accordés aux opérateurs, ainsi que le recours à des mécanismes d'authentification renforcés.

- **Surveiller en permanence les activités sur les systèmes :** La traçabilité de toutes les actions, qu'il s'agisse des systèmes ou des processus métier, constitue le point de départ essentiel au dispositif de surveillance exigé. Il est également nécessaire de mettre en place des mesures pour garantir l'intégrité constante des bases de données. Les procédures à suivre en cas d'incident doivent être clairement définies à l'avance (SWIFT, 2021).

3.4.3 Les mesures de CSP SWIFT

Le programme CSP de SWIFT établit sept grandes mesures de sécurité que tous les membres du réseau doivent respecter. Chacune de ces mesures comprend un ou plusieurs contrôles de sécurité. Les contrôles recommandés, mais non obligatoires, sont signalés par la lettre « A », indiquant leur caractère facultatif (SWIFT, 2021).

Tableau 4: Les mesure de sécurité de CSP SWIFT

Mesure de sécurité	Contrôle associe à la mesure
1. Limiter l'accès à Internet et séparer les systèmes critiques de l'environnement TI général	1.1 Protection de l'environnement SWIFT 1.2 Contrôle des comptes à privilèges dans le système d'exploitation 1.3 Protection de la plateforme de virtualisation 1.4 Restriction de l'accès à Internet 1.5A Protection de l'environnement client
2. Réduire la surface d'attaque et les vulnérabilités	2.1 Sécurité des flux de données internes 2.2 Mises à jour de sécurité 2.3 Sécurisation des systèmes 2.4A Sécurité du flux de données d'application métier : 2.5A Protection des données transmises en externe 2.6 Confidentialité et intégrité de la session opérateur 2.7 Analyse des vulnérabilités

	2.8A Externalisation des activités critiques 2.9A Contrôles opérationnels des transactions 2.10 Sécurisation des applications 2.11A Mesures opérationnelles RMA
3 Sécuriser physiquement l'environnement	3.1 Sécurité physique
4 Prévenir les vols d'identifiants	4.1 Politique en matière de mots de passe 4.2 Authentification à facteurs multiples
5 Gérer les identités et séparer les privilèges	5.1 Contrôle d'accès logique 5.2 Gestion des jetons 5.3A Processus Ressources humaines de validation du personnel 5.4 Stockage physique et logique des mots de passe
6 Détecter les activités anormales dans les systèmes ou les relevés d'opérations	6.1 Protection contre les logiciels malveillants 6.2 Intégrité des logiciels 6.3 Intégrité des bases de données 6.4 Journalisation et surveillance 6.5A Détection des intrusions
7 Plan d'intervention en cas d'incident et partage d'informations	7.1 Planification de l'intervention en cas de cyber-incident 7.2 Formation et sensibilisation à la sécurité 7.3A Tests d'intrusion 7.4A Évaluation des risques fondée sur des scénarios

Source : élaboré par nous-mêmes selon (SWIFT, 2021).

3.5 PCI-DSS : Un Standard Essentiel pour la Conformité en Matière de Paiement

La norme PCI-DSS a été créée en 2005 par le groupe américain Payment Card Industry Security Standards Council (PCI SSC) regroupant des entreprises telles que Visa, Mastercard, American Express, JCB et Discover Financial Services. Son objectif est d'établir de bonnes pratiques en matière de protection des données bancaires stockées sur les cartes de paiement pour les différents acteurs comme les banques, commerçants, entreprises de commerce électronique et hébergeurs de solutions bancaires. PCI-DSS comporte douze exigences, notamment :

- Installer et gérer une configuration de pare-feu pour protéger les données du titulaire de la carte,
- Chiffrer la transmission des données du titulaire sur les réseaux publics ouverts,
- Utiliser des logiciels antivirus et les mettre à jour régulièrement,
- Restreindre l'accès physique aux données du titulaire de la carte,
- Tester régulièrement les processus et les systèmes de sécurité.

Ces exigences illustrent le pragmatisme de la PCI-DSS et couvrent bien les principaux aspects liés à la sécurité d'un processus de paiement au sein d'un système d'information. Une fois ces critères respectés, le commerçant (entreprise gestionnaire des données bancaires) peut demander à une société agréée de procéder à un audit afin d'obtenir la certification PCI-DSS, valable un an. De manière évidente, les actions requises pour l'obtention de la certification PCI-DSS ne sont pas les mêmes selon les profils des organisations. Quatre niveaux ont été définis par le PCI en fonction du type d'activité. La norme PCI-DSS n'est donc pas acquise une fois pour toute car il est nécessaire de manière générale d'auditer le site web chaque année et d'effectuer un scan de vulnérabilité tous les trimestres (FERNANDEZ-TORO, pp. 28-31).

CHAPITRE II : CADRE ORGANISATIONEL ET MÉTHODOLOGIQUE

Ce chapitre présente le cadre méthodologique et organisationnel de notre recherche. Il se compose de deux sections principales. La première est consacrée à la présentation de l'organisme d'accueil, la Banque Extérieure d'Algérie (BEA). Elle aborde ses repères historiques, son rôle dans l'économie nationale, ses missions, ses valeurs, ainsi que la structure d'accueil, à savoir la Direction des Systèmes d'Information. La seconde section détaille la méthodologie adoptée et les outils mobilisés pour la réalisation de l'étude pratique.

Section 01 : Présentation de l'entreprise

Dans cette section, nous présentons l'organisme d'accueil de l'étude, en l'occurrence la Banque Extérieure d'Algérie. Nous commencerons par une brève présentation générale de l'institution, avant de détailler son organigramme fonctionnel, puis la structure du département concerné par l'étude, notamment la Direction du Systèmes d'Information (DSI).

1. A propos de la Banque extérieure d'Algérie BEA

La banque est une institution financière habilitée à recevoir des fonds du public et à les employer pour accorder des crédits.

La Banque Extérieure d'Algérie est une banque algérienne fondée en 1967, dont le siège social est situé à Alger. Elle est considérée comme la plus grande banque commerciale en Algérie en termes d'actifs et de réseau, avec plus de 200 agences à travers le pays.

La BEA propose une gamme complète de produits et de services financiers, tels que des comptes courants, des comptes d'épargne, des prêts personnels et professionnels, des cartes bancaires, des transferts d'argent, des services de change, et bien plus encore. Elle s'adresse à une clientèle diversifiée, comprenant des particuliers, des entreprises locales et internationales, ainsi que des organismes gouvernementaux. En tant que banque commerciale, la BEA joue un rôle important dans le développement économique de l'Algérie en offrant des services financiers qui soutiennent les entreprises locales et étrangères. Elle a également une forte présence à l'étranger, avec des filiales en Europe, en Afrique et au Moyen-Orient, qui offrent des services de financement et de conseil aux entreprises qui cherchent à faire des affaires en Algérie. La BEA est réputée pour son engagement en faveur de la responsabilité sociale des entreprises, notamment à travers des initiatives en faveur de l'éducation, de la culture, de la santé et de l'environnement. Elle a

également mis en place des programmes de formation pour ses employés afin de maintenir un niveau élevé de compétences et de professionnalisme.

Tableau 5: Récapitulatif sur la présentation de la Banque extérieure d'Alger

Nom	La Banque extérieure d'Algérie
Logo	
Slongo	BEA, la banque à la hauteur de vos aspirations.
Forme juridique et économique	SPA
Siège	42 rue des Frères Bouadou, 16005 Bir Mourad Raïs, Alger
Objet social	Activités bancaires
Date de création	1er octobre 1967
Capital	24 milliards 500 mille dinars algériens.
Site internet	www.bea.dz
Fax	+213 23 54 23 35

Source : élaboré par nous-mêmes à partir des documents internes de l'entreprise.

1.1 Historique de l'entreprise

Le 1er octobre 1967, par ordonnance N° 67-204, le processus de nationalisation du système

bancaire s'achève avec la création de la BEA. Date à partir de laquelle elle prend les activités

en Algérie du Crédit lyonnais.

Aux termes de ses statuts, la BEA a la qualité de banque de dépôts. Elle a pour but de simplifier les rapports économiques de l'Algérie avec les autres pays dans le cadre de la planification nationale. Dans le cadre des mesures gouvernementales favorisant la concentration chez les banques nationales des activités des banques étrangères, la BEA reprend par la suite les établissements suivants :

- La Société Générale dans sa situation au 31 décembre 1967.
- La Barclays Bank limitée au 30 avril 1968.
- Le Crédit du Nord.
- La Banque industrielle de l'Algérie et de Méditerranée (B.I.A.M.) au 31 mai 1968.

- La structure définitive de la BEA est achevée à partir du 1er juin 1968.

L'étude de l'évolution historique de la formation du système bancaire algérien permet de constater que les intermédiaires financiers, en Algérie, sont constitués de 3 catégories d'institutions :

- Le Trésor public.
- Les institutions financières bancaires.
- Les institutions financières non bancaires.

Initialement, le capital de la BEA était fixé à 20 millions de dinars, constitué d'une dotation
entièrement souscrite par l'État. Le capital ne pouvait être augmenté que par incorporation des réserves sur délibération du Conseil de Direction approuvé par arrêté du Ministère des Finances et du Plan. Actuellement, le capital de la BEA a atteint 24 milliards 500 mille dinars algériens.

1.2 Les missions de la BEA

La Banque extérieure d'Algérie a pour mission de :

- **Fournir des services bancaires de qualité :** la BEA doit offrir des produits et des services bancaires fiables et de qualité supérieure, tels que des comptes courants, des comptes d'épargne, des cartes de crédit, des prêts et des services de change. Ses services doivent être adaptés aux besoins de ses clients, qu'ils soient des particuliers, des entreprises ou des organismes gouvernementaux.
- **Soutenir le développement économique :** la BEA joue un rôle important dans le développement économique de l'Algérie en offrant des services financiers qui soutiennent les entreprises locales et étrangères. Elle doit aider à financer les projets d'investissement et les activités commerciales des clients, contribuant ainsi à la création d'emplois et à la croissance économique.
- **Maintenir la stabilité financière :** la BEA doit assurer la stabilité financière en gérant de manière prudente les risques financiers, en respectant les réglementations financières et en maintenant une solide base de capital. Cela permet de garantir la sécurité des dépôts de ses clients et de maintenir la confiance du public dans la banque.
- **Soutenir les relations internationales de l'Algérie :** La BEA a une forte présence l'étranger avec des filiales en Europe, en Afrique et au Moyen-Orient. Elle doit aider

les entreprises algériennes à s'implanter sur les marchés internationaux en offrant des services de financement et de conseil adaptés à leurs besoins.

- **Contribuer à la responsabilité sociale des entreprises :** La BEA s'engage à être une entreprise socialement responsable en menant des initiatives en faveur de l'éducation, de la culture, de la santé et de l'environnement. Elle doit contribuer à l'amélioration du bien-être de la communauté et à la préservation de l'environnement dans le cadre de sa mission globale.

1.3 Les valeurs de la BEA

La BEA s'est engagée à respecter des valeurs clés qui reflètent sa mission, son engagement envers la société et sa vision pour l'avenir. Voici quelques-unes des valeurs les plus importantes de la BEA :

- **L'engagement envers l'éthique et l'intégrité :** la BEA est engagée à respecter les normes les plus élevées d'éthique et d'intégrité dans toutes ses activités, pour maintenir la confiance et la loyauté de ses clients et de la société en général.
- **La satisfaction client :** la BEA met l'accent sur la satisfaction de ses clients en fournissant des services de qualité, en écoutant leurs besoins et en répondant rapidement à leurs demandes.
- **L'innovation :** la BEA est déterminée à être une entreprise innovante en utilisant les dernières technologies pour offrir des services bancaires modernes et efficaces à ses clients.
- **L'excellence opérationnelle :** la BEA vise à atteindre l'excellence opérationnelle en établissant des processus efficaces et en optimisant ses opérations pour améliorer la qualité de ses services et sa compétitivité.
- **La responsabilité sociale des entreprises :** la BEA est consciente de son rôle de la société et s'engage à avoir un impact positif sur la communauté, en soutenant L'éducation, la culture, la santé et l'environnement.
- **La transparence :** la BEA s'engage à être transparente dans ses opérations, en fournissant des informations claires et précises sur ses produits et services, ainsi que sur ses résultats financiers.

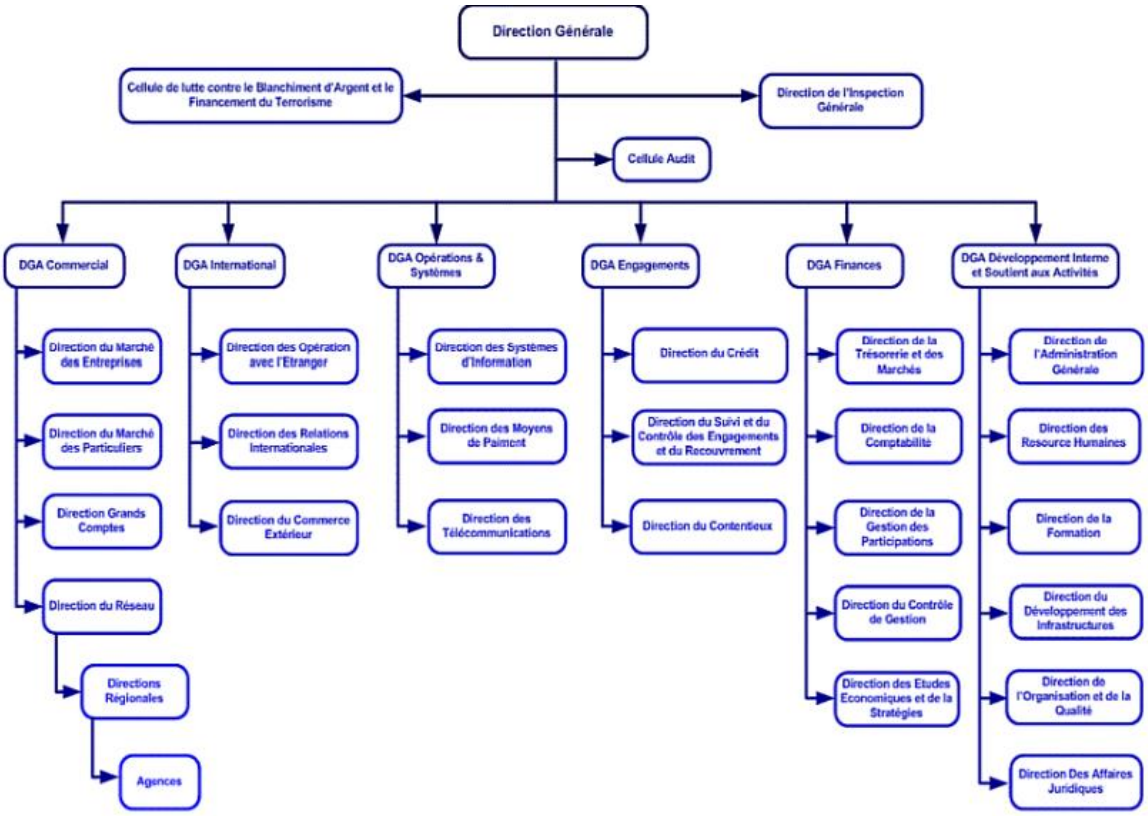
1.4 Structure d'Accueil

1.4.1 Structure de la Banque

La BEA a un effectif de 3.800 employés répartis sur une Direction Générale, plusieurs

Directions Générales Adjointes, des Directions et des Agences. Nous illustrons par la figure de l'organigramme de la BEA.

Figure 2: Organigramme de la Banque extérieur d'Alger



Source : Documents interne de l'entrepris.

1.4.2 Structure du département d'Accueil

- **La Direction des Systèmes d'Information (DSI)**

L'informatique étant le cœur de tout système bancaire, la Direction des Systèmes d'Information (DSI) travaille en étroite collaboration avec la Direction Générale afin de fournir un système d'information performant et une infrastructure IT des plus fiables. La DSI assure un support technique aux différents utilisateurs du système. Elle a pour missions d'assurer la sécurité des données et du système et un service continu 24H/24H. Elle a également un rôle d'innovateur, car elle propose toujours de nouveaux outils (soft ou hard) pour automatiser et accélérer les différents processus métiers.

Pour assurer ses différentes missions, la DSI est composée de cinq départements :

- **Le Département Architectures et standards :** étude et proposition de nouvelles procédures et méthodologies de fonctionnement de la DSI.

- **Le Département de Sécurité :** son rôle principal est d'assurer la disponibilité. La sécurité des systèmes d'information et l'intégrité des données. Il a pour mission de défini une politique de sécurité performante et de veiller à son application. Ce département procède régulièrement à des audits afin d'évaluer le niveau de vulnérabilités et de proposer des solutions en conséquence.

- **Le Département Gestion des Environnements :** cette structure prend en charge la maintenance des appareils, assiste les différents utilisateurs (help desk), gère le réseau, assure le suivi des licences et des systèmes d'exploitation.

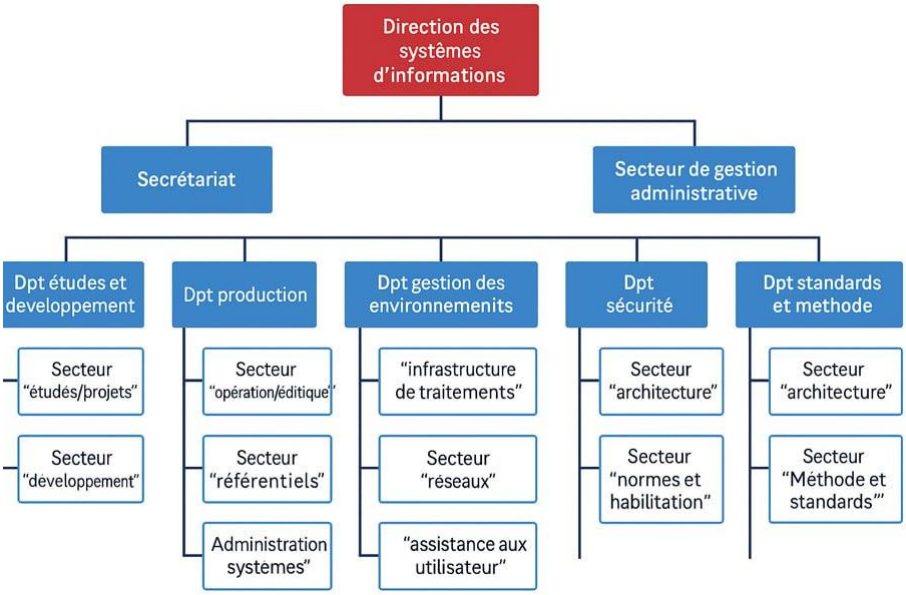
- **Le Département de Production :** son rôle principal est la gestion de la base de données et l'exploitation des moyens informatiques de la banque.

- **Le Département Etude et développement :** c'est dans ce département que nous avons effectué notre stage. Composé de plus d'une dizaine d'ingénieurs, ce dernier a pour fonction d'aider les différentes structures à formuler une expression de besoins claire et bien définie. L'étude et l'analyse des besoins exprimés, la conception et le développement de logiciels.

- Notre stage a débuté au sein du Département Architectures et Standards (DSI), pilier stratégique de la gouvernance technique de l'organisation. Ce département supervise la conception des architectures système, garantit l'alignement des solutions technologiques avec les normes internes et externes, et définit les standards de sécurité et d'interopérabilité. Durant cette phase, nous avons approfondi les enjeux de structuration des systèmes critiques, notamment en étudiant les processus d'intégration de solutions SWIFT, dont la fiabilité et la conformité sont essentielles pour les opérations financières internationales. En parallèle, Une partie de notre stage s'est également déroulée à la Direction des Opérations Commerciales Extérieures (DCE), où nous avons observé la mise en œuvre pratique des normes SWIFT dans les flux transactionnels. Cette étape a renforcé notre compréhension des interactions entre les systèmes backend et les besoins métier, notamment en matière de traçabilité et de rapidité des transactions. Enfin, notre passage à la Direction de Conformité a achevé cette formation transversale. Nous y avons étudié les processus de validation des habilitations utilisateurs, les audits réglementaires, et les exigences légales liées aux systèmes financiers.

- La Direction de la Sécurité des Systèmes d'information répond aux besoins et exigences de la Banque en termes de sécurité et de conformité du système d'information. Elle s'aligne sur les normes internationales (IFRS, CSCF, SWIFT, IS027001, 27005, 27015, PCI DSS, Accord BALE III, SOX, COBIT & COSO).

Figure 3 : Organigramme de la direction des systèmes d'information



Source : Documents interne de l'entreprise.

2. Etat de lieux de l'entreprise accueil

2.1 Présentation du Système d'information de la Banque Extérieure d'Algérie (BEA)

La Banque Extérieure d'Algérie, acteur majeur du secteur bancaire national, s'appuie sur un Système d'Information complexe, modulaire et interconnecté, intégrant des solutions critiques couvrant l'ensemble de ses processus métiers. Ce SI repose principalement sur le Core Banking System (Temenos ou FLEXCUBE, selon la version confirmée par documentation interne), la plateforme SWIFT Alliance Entry (messagerie interbancaire sécurisée), ainsi que sur des outils spécialisés tels que FICO (analyse de risques financiers), GLPI (gestion de support IT), ou encore e-Payment Platform (paiements électroniques). La version actuellement en production de ces systèmes, notamment SWIFT et le Core Banking, ainsi que leurs dates de mise en œuvre effectives, devront être confirmées via les documents techniques internes ou les procès-verbaux de mise en production.

Bien que disposant déjà de certifications sectorielles majeures telles que le SWIFT CSP et la PA-DSS, la Banque Extérieure d'Algérie (BEA) a initié une transition stratégique vers la norme ISO/CEI 27001, dans le but de structurer un Système de Management de la Sécurité de l'Information (SMSI) global, couvrant l'ensemble de ses processus métiers, de ses infrastructures et de ses risques. Son Système d'Information repose sur un socle d'outils intégrés couvrant les domaines clés : SAP Finance, Oracle Hyperion et Finastra pour la finance ; Treasury Management Suite pour la trésorerie ; ServiceNow GRC, IBM Guardium et OneTrust pour la conformité et la sécurité ; SAP SuccessFactors, BambooHR et Skillsoft pour les RH ; et des solutions collaboratives telles que Teams, SharePoint, ServiceNow ITSM et Tableau, assurant ainsi cohérence fonctionnelle, efficacité opérationnelle et alignement stratégique avec les standards internationaux.

La Banque Extérieure d'Algérie (BEA) s'appuie sur une architecture technologique financière centralisée à forte intensité transactionnelle pour assurer la gestion de ses opérations bancaires, dont près de 80 % transitent par le réseau SWIFT, pilier stratégique de ses échanges internationaux. Au cœur de cet environnement, la plateforme DELTA joue un rôle structurant en assurant la gestion des comptes clients, le traitement des règlements, ainsi que l'interfaçage avec SWIFT, garantissant l'intégrité et la fluidité des transactions transfrontalières. Cette infrastructure s'appuie sur des solutions interconnectées telles que Smart Stream CORONA, qui automatise la réconciliation de 60 % des flux SWIFT, et FINASTRA KTP, dédié à la supervision des paiements internationaux et des garanties financières.

La conformité réglementaire et la sécurité des transactions sont renforcées par une chaîne de contrôle automatisée. ASCREM, la centrale des risques, assure une détection en temps réel des transactions suspectes sur la base de critères analytiques (valeurs atypiques, irrégularités de comportement), tandis que le module C.D.L. vérifie la non-conformité aux listes de sanctions internationales. À ces dispositifs s'ajoute FICO TONBELLER, un moteur KYC avancé, chargé d'évaluer la fiabilité des contreparties selon les standards réglementaires en vigueur.

Du côté des clients, les solutions AEBS E-Banking et Mobile Banking (OGA) offrent des interfaces sécurisées pour initier des virements internationaux, qui s'exécutent via le protocole SWIFT (MT103), assurant à la fois traçabilité, confidentialité et rapidité. L'ensemble de l'écosystème est supervisé en temps réel par Splunk SIEM, qui centralise

les logs de sécurité, détecte les anomalies comportementales et déclenche automatiquement des alertes pour les équipes opérationnelles, dans un cadre conforme aux exigences de la norme ISO/IEC 27001 et du SWIFT CSP.

2.2 Périmètre Prioritaire : Orientation Stratégique sur l'Environnement SWIFT et les Exigences de Contrôle ISO/CEI 27001

Évaluer l'ensemble du Système d'Information de la Banque Extérieure d'Algérie dans sa globalité serait irréaliste, compte tenu de sa taille, de sa complexité et du nombre de systèmes impliqués. C'est pourquoi nous avons choisi de concentrer notre analyse sur le système SWIFT, identifié comme hautement critique par la Direction des Systèmes d'Information. En effet, plus de 80 % des opérations sensibles de la banque transitent par SWIFT, notamment les virements internationaux, représentant près de 40 % du chiffre d'affaires annuel. En plus de son importance opérationnelle, Au sein du Système d'Information de la BEA, la Society for Worldwide Interbank Financial Télécommunication (SWIFT) occupe une place stratégique, fondée en 1973 et déployant ses premiers réseaux interbancaires dès 1977, cette société anonyme de droit belge, dont le siège est à Bruxelles, fournit la plateforme d'échange sécurisée désormais intégrée à la version 7.7 de SWIFT Alliance Access (SAA). Membre actif du réseau, la BEA s'appuie sur cette infrastructure pour traiter l'essentiel de ses paiements transfrontaliers, garantissant ainsi rapidité, fiabilité et conformité aux standards internationaux. SWIFT est soumis à des exigences de conformité strictes, notamment à travers le SWIFT CSP et la norme internationale ISO 27001, qui impose des contrôles rigoureux (authentification forte, chiffrement, gestion des accès, etc.). Ce système constitue également un cas d'étude pertinent pour étudier la convergence entre un cadre réglementaire sectoriel (SWIFT CSP) et une norme de sécurité de référence (ISO 27001).

Bien que la BEA ne soit pas encore certifiée ISO 27001, elle a exprimé une volonté claire de s'y conformer. Pour cela, nous avons retenu un périmètre technique centré sur les 22 contrôles du SWIFT CSP, largement alignés avec l'annexe A de la norme ISO 27001. Cette approche permet de couvrir environ 70 % des exigences ISO tout en concentrant les efforts sur les risques les plus critiques.

Avec l'appui d'un expert informatique, nous avons conçu une matrice de correspondance entre les contrôles SWIFT CSP et les 93 mesures ISO 27001, permettant d'identifier les écarts, de prioriser les actions correctives et de proposer un plan d'action structuré.

L'objectif est de faire de SWIFT un levier de conformité globale, et une base solide en vue d'une future certification ISO 27001.

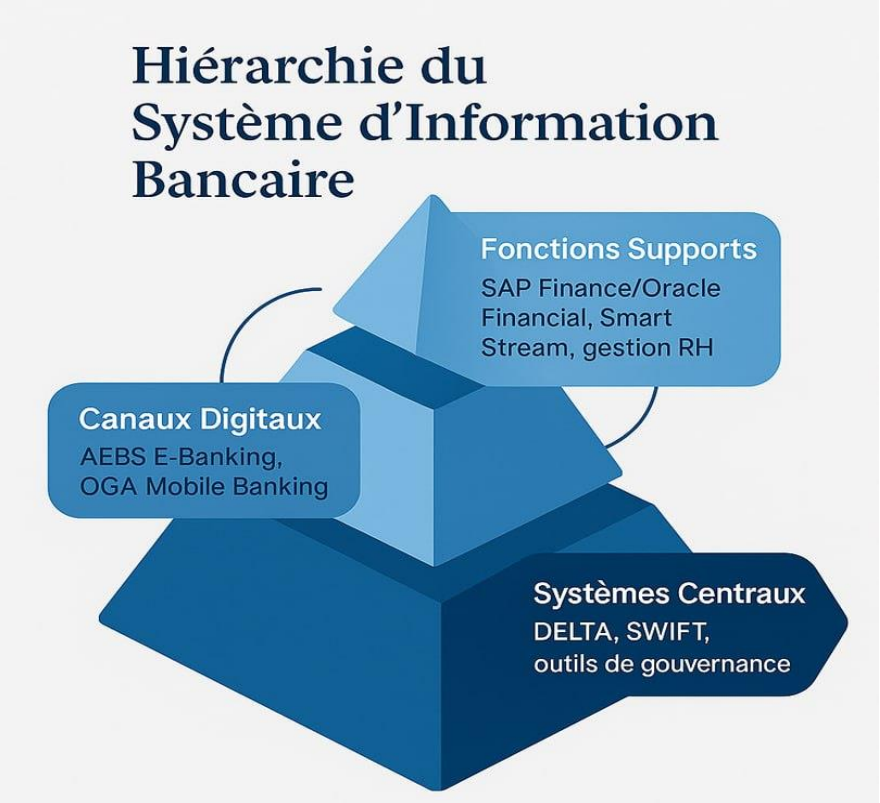
Enfin, il est important de noter que SWIFT est une norme mondiale, utilisée par plus de 11 000 institutions dans 200 pays. En tant que membre du réseau, la BEA doit respecter des délais de traitement très stricts (moins de 30 secondes par message), sous peine de sanctions. Cela renforce la pertinence stratégique de ce choix de périmètre, à la fois du point de vue opérationnel et académique.

3. Architecture Applicative de la BEA

L'architecture du Système d'Information de la Banque Extérieure d'Algérie repose sur une infrastructure bancaire centralisée et modulaire, articulée autour du Core Banking System (DELTA), véritable colonne vertébrale des opérations bancaires. Cette plateforme centrale est interconnectée à un ensemble de systèmes spécialisés, interfaces externes critiques (notamment SWIFT) et outils de gestion opérationnelle, dans le but de garantir à la fois la fluidité des traitements, la sécurité des transactions, et la conformité réglementaire, notamment vis-à-vis du SWIFT (CSP) et de la norme ISO/CEI 27001. Mis en service il y a une dizaine d'années, le Core Banking System a fait l'objet d'un vaste processus de centralisation mené de janvier à août 2024. Au cours de cette phase, 108 agences ont été migrées vers la plateforme centrale DELTA, permettant ainsi de consolider les flux de données, d'homogénéiser les traitements bancaires et de renforcer la gouvernance opérationnelle de la BEA. Le Core Banking System (DELTA) de la BEA géré l'ensemble des processus métiers de la gestion des comptes à la comptabilité et synchronise les flux entre ses 108 agences et les systèmes externes. Son écosystème repose sur trois piliers :

- **Systèmes centraux :** DELTA, la plateforme SWIFT (réconciliation via Smart Stream) et les outils de gouvernance (FICO pour AML/KYC, CORISI pour les garanties).
- **Canaux digitaux :** AEBS E-Banking et OGA Mobile Banking, intégrés à DELTA via des API sécurisées pour les virements internationaux et la consultation de comptes.
- **Fonctions supports :** consolidation comptable (SAP Finance/Oracle Financial, Smart Stream), gestion RH (Workday/SIRON LABFT) et support IT (GLPI, Barid Pro).

Figure 4 : Hiérarchie du Système d'information Bancaire.



Source : élaboré par nous-mêmes.

4. Interactions Clés du Système d'Information

A. Flux transactionnels

- SWIFT → DELTA : Les messages financiers (MT940/MT950), réceptionnés via la plateforme SWIFT, sont traités par Smart Stream pour réconciliation, puis intégrés dans le Core Banking System (DELTA) afin de mettre à jour les soldes et opérations des comptes clients.

B. **Alignement ISO 27001 :** Les exigences de chiffrement des données en transit (A.10.1.1) et de traçabilité par journalisation des événements (A.12.4.1) sont pleinement respectées à ce niveau.

- DELTA → Agences : Les fichiers journaliers de mouvement ("SA") sont transmis aux agences pour validation et exploitation locale.

Point d'attention : Si ces fichiers ne sont pas chiffrés lors du transfert, cela constituerait un écart de conformité avec le contrôle A.10.1.1 de l'ISO 27001 relatifs à la protection cryptographique de l'information.

C. Gestion des données clients

- DELTA ↔ FICO : Les données clients (informations KYC, historiques transactionnels) sont automatiquement croisées avec des listes de surveillance réglementaires (OFAC, FATCA, etc.) via la solution FICO.

Conformité assurée : Cette interaction répond aux exigences de respect des obligations légales, réglementaires et contractuelles (ISO 27001 – A.18.1.1).

D. Sécurité des accès

- Accès administrateur DELTA : Les accès sensibles au système central sont protégés par une authentification forte, notamment par MFA (Multi-Factor Authentication), en conformité avec les recommandations du SWIFT CSP.

Conformité ISO 27001 : Cette mesure s'aligne directement avec le contrôle A.9.1.1 relatif à la gestion sécurisée des accès aux systèmes critiques.

Tableau 6 : Synthèse de l'architecture technologique globale

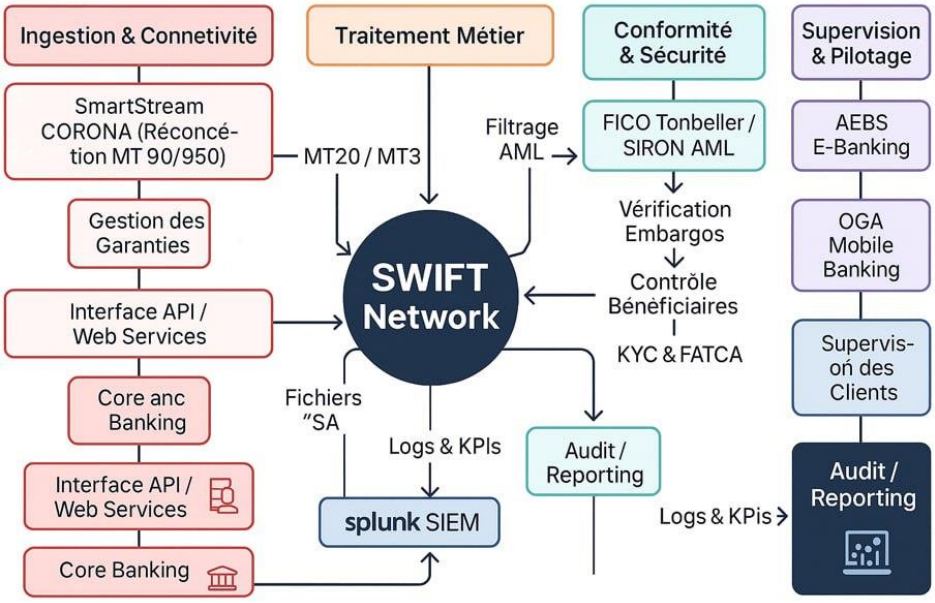
Domaine	Système utilise	Rôle	OUTIL/ COMMENT
Gestion des Services Bancaires Critiques (GSBC) Le core banking	✓ Temenos, ✓ SWIFT ✓ GPI	✓ Gestion des comptes clients et transactions internationales ✓ Cœur du SI, gère les comptes clients, les transactions, les prêts, et les produits financiers.	✓ Temenos et FLEXCUBE pour la gestion des comptes courants et épargne. ✓ SWIFT GPI pour le suivi des paiements internationaux.
Sécurité	✓ CSP Swift ✓ FICO ✓ PCA ✓ DSS	Protection des flux SWIFT et analyse des risques clients.	✓ FICO pour l'analyse des risques clients (AML/KYC). ✓ CORISI pour la gestion des garanties internationales
Mobile Banking	BEA Mobile	Accès client aux services bancaires depuis smartphone.	✓ BEA Mobile pour les transferts, consultations de solde, et factures.

			✓ Intégré au CBS via des API sécurisées.

Source : élaboré par nous-mêmes à partir des documents internes de l'entreprise.

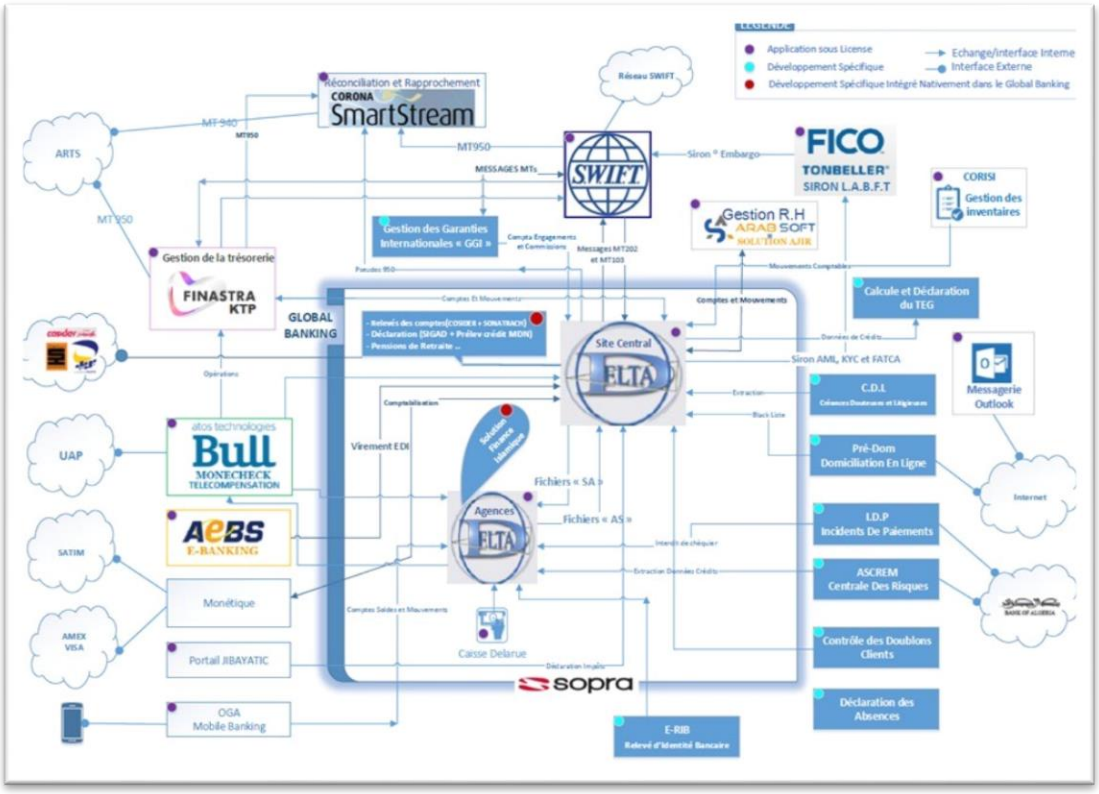
Pour clarifier l'architecture technologique mise en place au sein de la BEA, le tableau ci-après présente une synthèse globale des principaux domaines fonctionnels, des systèmes utilisés, de leur rôle stratégique, ainsi que des outils et mécanismes mobilisés pour leur déploiement et leur intégration. Cette vue d'ensemble permet de mieux appréhender l'interconnexion entre les différents composants du système d'information bancaire.

Figure 5 : Interaction Clés du Système d'Information



Source : élaboré par nous-mêmes à partir des documents internes de l'entreprise.

Figure 6 : Cartographie applicative.



Source : donnée interne de la banque.

La cartographie révèle que l'intégralité des transactions internationales transite par SWIFT, ainsi démontre que SWIFT traite l'intégralité des transactions internationales et, en tant que plateforme pivot, assure la standardisation et la coordination des paiements transfrontaliers, renforce la sécurité et la conformité selon les exigences du SWIFT CSP et de l'ISO 27001, et garantit l'intégration transparente, la traçabilité complète et la résilience opérationnelle des flux au sein du système central DELTA.

Section 02 : Cadre méthodologique

Dans cette section, nous commencerons par exposer le cadre méthodologique. Puis, afin d'éclaircir notre question de recherche, nous examinerons dans la deuxième partie la méthodologie, en précisant notre démarche ainsi que les techniques employées pour le recueil de données. Par la suite, nous examinerons le contexte organisationnel de notre étude.

1 . Les techniques de recueil de données

L'application appropriée des méthodes et des techniques dans le cadre d'une recherche ou d'une étude est désignée comme la méthodologie de recherche. La démarche de recherche ne se réduit pas à une simple compilation de techniques. C'est une approche de réflexion qui offre au chercheur la possibilité d'obtenir des connaissances robustes. Elle emploie une démarche critique et réflexive qui oriente le chercheur durant l'ensemble du processus de recherche, depuis l'élaboration de la question de recherche jusqu'à l'exégèse des résultats (Benaissa, 2001, p. 21).

1.1 La recherche qualitative

Le choix entre une approche qualitative et une approche quantitative apparaît donc plus dicté par des critères d'efficience par rapport à l'orientation de la recherche, construire ou tester. Bien que les garanties de validité interne et de validité externe doivent être envisagées conjointement quel que soit le type de recherche, le chercheur doit se déterminer sur la priorité qu'il accorde à la qualité des liens de causalité entre les variables ou à la généralisation des résultats pour choisir entre une approche qualitative et une approche quantitative. L'idéal serait évidemment de garantir au mieux la validité des résultats en menant conjointement les deux approches (Yin, 2016, p. 49).

L'approche qualitative offre plus de garantie sur la validité interne des résultats. Les possibilités d'évaluation d'explications rivales du phénomène étudié sont plus grandes que dans l'approche quantitative, car le chercheur peut mieux procéder à des recoupements entre les données. L'approche qualitative accroît l'aptitude du chercheur à décrire un système social complexe. (al., 2014)

Le résultat d'une recherche qualitative se présente très généralement sous la forme d'une proposition, d'une assertion textuelle, générée à partir de données qualitatives, et l'usage de tests statistiques est là impossible. Le passage de données qualitatives collectées en très grand nombre et de nature très souvent diverse à une proposition dite de résultats repose

avant tout sur un certain nombre de techniques de collecte, de réduction et d'analyse de ces données. (al., 2014)

1.2 Le guide d'entretien

L'entretien est une technique qui vise à récolter des données discursives reflétant l'univers mental des individus. Cette approche méthodique vise à instaurer un climat de confiance qui permettra aux sujets d'aborder leur discours avec spontanéité et sans retenue, ce qui permettra de révéler les mécanismes de défense mis en place face à l'examen de leur comportement ou de leur pensée. (al., 2014)

Le guide d'entretien est un document de base pour des entretiens qualitatifs. C'est une liste de questions à aborder avec les participants. Selon l'objectif et la liberté laissée à l'intervieweur, le guide peut être structuré ou semi-structuré. Il doit être soigneusement élaboré en tenant compte des objectifs de la recherche et des participants. Un guide bien conçu aide l'intervieweur à collecter des données cohérentes et rigoureuses. Le guide d'entretien de notre étude facilite la collecte d'informations auprès des interviewés, avec des questions claires, pertinentes et cohérentes (Yin, 2016, p. 60).

1.3 La collecte de données

La collecte des données est un élément crucial du processus de recherche en management. Elle permet au chercheur de rassembler le matériel empirique sur lequel il va fonder sa recherche. Afin de constituer une base empirique, il est essentiel que le chercheur vérifie la disponibilité des données. L'utilisation de données secondaires (données de seconde main) présente de réels avantages, car elle évite au chercheur de recueillir lui-même les données sur le terrain. Cependant, l'accès à ces données est souvent limité et leur qualité est difficile à évaluer. En l'absence ou en complément de données secondaires, le chercheur peut collecter ses propres données, dites « données primaires ». Il doit alors déterminer la nature exacte des données nécessaires à la validation de son modèle théorique, puis considérer les instruments potentiellement disponibles pour collecter ces données. Ces instruments varient en fonction de l'approche quantitative ou qualitative adoptée par le chercheur (al., 2014).

La collecte de données dans le cadre de l'approche qualitative ne saurait se réduire à une simple étape discrète d'un programme de recherche. Elle nécessite en effet la réalisation d'une investigation approfondie sur le terrain. Ainsi, la gestion de la relation entre le chercheur et les sujets-sources de données revêt une importance majeure. La véritable

difficulté d'une recherche qualitative ne réside pas dans l'occultation de la figure du chercheur (de soi-même), mais dans la capacité à qualifier et à maîtriser sa présence dans le dispositif de collecte (al., 2014).

1.4 Recherche documentaire

Selon N'Da, P. (2015) « l*a recherche documentaire permet de collecter une littérature importante sur des questions pour obtenir les informations les plus pertinentes dans un domaine d'objet à traiter. Il s'agit notamment d'enchainement de recherche, d'identification et d'acquisition des documents liés à des sujets clairement définis, ainsi construire des stratégies de recherche qui nécessitent des méthodes efficaces* ».

Selon Dinet, J., et Passerault, J.-M. (2004) « *la recherche documentaire vise à identifier et localiser des ressources informationnelles déjà traitées, soit par individus soit par des machines. La recherche documentaire s'accompagne du qualitatif « informatisée » lorsque cette activité implique l'interaction entre deux systèmes, l'un humain (l'usager, l'utilisateur) et l'autre informatique (une base de données) via un logiciel et une interface* ».

Pour l'élaboration de notre étude sur l'évaluation de la conformité de la sécurité du système SWIFT selon la norme ISO 27001, nous avons mobilisé une approche méthodologique rigoureuse, appuyée sur des ressources académiques et techniques de référence. Notre analyse s'est concentrée sur la cartographie des contrôles du Cadre de Sécurité des Paiements extérieurs SWIFT (CSP Swift) avec les exigences de l'ISO 27001, en exploitant des sources telles que ResearchGate pour des études comparatives sur l'implémentation de la norme dans le secteur financier, la Bibliothèque canadienne RHEA LAROS pour ses rapports techniques sur la gestion des risques cyber et la segmentation réseau, ainsi que des documents internes de la Banque Extérieure d'Algérie (BEA) et du SWIFT Institute. Cette revue critique a permis d'identifier des écarts significatifs, notamment concernant la segmentation réseau (CSP-C01 ↔ ISO 27001 A.13.1.1), le chiffrement AES-256 des transactions (CSP-C02 ↔ A.10.1.1), et l'authentification multifacteur (CSP-C04 ↔ A.9.1.1), Cette étude, ancrée dans une méthodologie interdisciplinaire, vise à renforcer la résilience des systèmes critiques tout en répondant aux attentes réglementaires et sectorielles.

2. Approche de conception

Pour garantir la rigueur des résultats, il est essentiel de définir clairement l'approche de conception dans toute recherche académique. Cette section présente les fondements épistémologiques, les méthodes d'analyse et les choix méthodologiques de cette étude. En présentant ces éléments, nous assurons la cohérence et la transparence de notre démarche de recherche.

2.1 Mode de raisonnement

2.1.1 Le choix épistémologique

Au cœur des multiples courants de pensée en recherche scientifique, il est essentiel de situer cette étude dans un cadre épistémologique approprié. Cette démarche permet d'établir une méthodologie rigoureuse et cohérente avec les objectifs de l'approche adoptée. (al., 2014)

La recherche scientifique vise à comprendre et expliquer la réalité, mais sa perception varie selon les paradigmes épistémologiques : le positivisme (réalité objective et mesurable), le constructivisme (construction subjective par les individus) et l'interprétativisme (perceptions et expériences humaines). Ces approches, décrites par (Gavard-Perret, 2012, pp. 11-13),reflètent des perspectives complémentaires pour analyser les phénomènes.

Selon Soler, Léna (2000) ,«*l'épistémologie a pour objectif fondamental de qualifier les sciences présentes à travers un jugement de leur valeur, particulièrement de choisir les recherches scientifiques qui doivent être aptes et tenir compte de l'hypothèse d'une connaissance certaine et authentiquement justifiée*». (Wacheux, 1996) , a défini que « L'épistémologie est une science des sciences ou une philosophie de la pratique scientifique sur les conditions de la validité des savoirs théoriques... Adopter une épistémologie, donc des guides pour l'action de recherche, permet de se démarquer des consultants, des dirigeants… Dans une logique de la découverte, ou dans une logique de la preuve, le chercheur réfléchit aux conditions de la formation de ses énoncés ».

Selon les principes de l'épistémologie en recherche scientifique, le paradigme positiviste vise à expliquer la réalité de manière objective et mesurable, tandis que le paradigme constructiviste se focalise sur la manière dont la réalité est construite subjectivement par les individus. Par ailleurs, les recherches centrées sur la compréhension des significations

et des perceptions humaines relèvent du paradigme interprétativiste (Gavard-Perret, 2012) (Meghari, 2020).

L'épistémologie peut se définir comme la discipline philosophique centrée sur l'analyse des fondements scientifiques. Traditionnellement, elle vise à « *caractériser la science pour évaluer la validité logique et cognitive de ses productions* » (Soler, 2000, p. 15) , dans le but de déterminer si celles-ci s'approchent d'un idéal de connaissance certaine et rigoureusement justifiée. Toutefois, cette vision normative a progressivement cédé la place à une approche plus dynamique, où l'épistémologie est conçue comme « *une activité réflexive examinant les processus de production et de légitimation des savoirs* » (al., 2014).

2.1.2 Une posture constructiviste

Dans le cadre du constructivisme ingénirique, la réalité n'est pas perçue comme une entité objective préexistante, mais comme le résultat d'un processus de construction active. Ce processus émerge des interactions entre le chercheur, les acteurs et leur environnement, où les observations et phénomènes empiriques reflètent les interprétations subjectives des individus. Les données, lois ou objets d'étude ne possèdent pas d'existence indépendante : ils sont co-produits par les activités cognitives des sujets, fusionnant ainsi ontologie et épistémologie. (al., 2014)

La connaissance issue de cette approche est contextuelle, relative et téléologique. Son évaluation ne repose pas sur une vérité absolue, mais sur sa capacité à répondre aux objectifs fixés par le chercheur. (al., 2014)

Notre recherche repose sur une interprétation rigoureuse des données recueillies auprès des acteurs clés. Cependant, elle s'inscrit principalement dans une posture constructiviste, qui privilégie l'exploration des significations attribuées par les acteurs à la conformité aux exigences de la norme ISO 27001. Car elle reconnaît que la réalité n'est pas une donnée objective, mais une construction sociale issue des interactions entre les acteurs et leur environnement. Comme le souligne (Avenier, 2011) , « *la connaissance ne peut être réduite à une représentation fidèle du réel, mais doit être comprise comme une construction continue résultant de l'assimilation-accommodation des expériences humaines* ».

Cette perspective est particulièrement pertinente dans le contexte spécifique de la Banque BEA, où la conformité aux exigences de sécurité des systèmes d'information (SI Swift)

dépasse largement les aspects techniques pour inclure des dynamiques organisationnelles et humaines. Cette perspective s'aligne avec l'épistémologie constructiviste, qui souligne l'importance des processus d'interaction entre le sujet et son environnement dans la construction des savoirs. Appliquée à notre contexte, cette approche permet d'analyser comment les parties prenantes clés notamment le DSSI, et les équipes opérationnelles interprètent et approprient les exigences de l'ISO 27001, en les adaptant aux spécificités culturelles, organisationnelles et stratégiques de la Banque BEA.

Ainsi, le cadre constructiviste offre une grille de lecture flexible pour explorer les tensions, les compromis et les synergies entre les prescriptions normatives et les réalités pratiques. Il met en lumière comment la conformité sécuritaire se coconstruit au quotidien, à travers des dynamiques collaboratives (ou conflictuelles) entre les individus et les structures. Cette approche holistique est essentielle pour garantir non seulement une adhésion effective aux standards internationaux, mais aussi une résilience organisationnelle alignée sur les priorités métier et les risques spécifiques de l'institution.

2.2 Approche qualitative

L'approche qualitative, ancrée dans une épistémologie constructiviste, postule que la réalité sociale est construite à travers les expériences et les significations attribuées par les acteurs. En effet, évaluer cette conformité ne se réduit pas à une vérification technique : elle implique de décrypter les pratiques organisationnelles, les représentations des acteurs (responsables DSSI, auditeurs, équipes TI) et les écarts entre normes prescrites et réalités opérationnelles.

Notre choix de l'approche qualitative se justifie par sa capacité à explorer en profondeur ces dimensions subjectives et contextuelles. Contrairement aux méthodes quantitatives, souvent limitées à des indicateurs mesurables (nombre de contrôles implémentés), la recherche qualitative permet de répondre à des questions telles que : comment les acteurs perçoivent-ils les exigences de l'ISO 27001 ? Quels obstacles culturels ou structurels entravent leur mise en œuvre effective ? Cette démarche s'appuie sur des entretiens semi-directifs avec les professionnels de la DSSI de la BEA Banque, couplés à une analyse documentaire (politiques de sécurité, rapports d'audit interne), afin de trianguler les données et renforcer la validité interne.

La pertinence de cette approche pour notre thème réside dans son alignement avec les enjeux critiques de la sécurité bancaire. L'ISO 27001, bien que structurée autour

d’exigences techniques, repose ultimement sur l’appropriation humaine des processus. Une évaluation purement quantitative risquerait d’occulter les freins organisationnels (résistance au changement, lacunes dans la formation) ou les ambiguïtés interprétatives des contrôles. En adoptant une posture qualitative, nous capturons non seulement les écarts techniques (non-conformité à l'annexe A), mais aussi les logiques décisionnelles et les dynamiques de pouvoir influençant la gouvernance de la sécurité

Cette démarche s’appuie sur une triangulation méthodologique : des entretiens semi-directifs avec les cadres de la DSSI de la BEA Banque, et les équipes opérationnelles, une analyse critique des artefacts organisationnels (politiques de sécurité, procédures d’audit) et une observation participante des routines de gestion des risques.

2.3Le choix de collecte Les données

2.3.1 Les entretiens semi-directifs

Les entretiens semi-directifs sont privilégiés dans cette recherche pour leur capacité à explorer en profondeur les dynamiques organisationnelles liées à la conformité à l'ISO 27001. Cette norme, bien que technique, repose sur des processus humains (gestion des risques, culture de la sécurité) dont la compréhension nécessite d'interroger directement les acteurs clés (DSSI, informaticiens, auditeurs). L’entretien semi-directif sera sélectionné pour assurer le recueil des données. Il est également appelé "entretien guidé", c’est le type d'entretien le plus utilisé dans les sciences humaines et sociales ; Il permet de récolter des données verbales grâce à des questions structuré. Ces questions sont fondées sur un cadre aidant à aborder certains thèmes de base sur la conformité à l’ISO 27001 versions 2022. Il sera important de permettre à la personne interrogée de répondre librement et de consigner les réponses littéralement pour une durée de 60 mn.

- **Sélection des interviewés**

Tableau 7 : Liste des personnes interviews.

Responsable intervenant à l’interview	Sujet de l’entretien	Date
- Administrateur principale de SWIFT (Superviseur de SWIFT) - Chef de secteur normes au sein du département architecture méthode et standards	Fonctionnement de la SI SWIFT	06/04/2025

- Ingénieur d'État en Informatique Principal (Sécurité Informatique)		
- Directeur des auditeurs	Bonnes pratiques ISO 27001 appliquées au SI SWIFT	06/04/2025
- Ingénieur d'État en Informatique Principal - Sécurité Informatique		

Source : élaboré par nous-mêmes.

- **Le guide d'entretien**

Tableau 8: Le Guide d'entretien

Axe 1	**Questions**
Fonctionnement du SI SWIFT	
Gestion des messages SWIFT (Métier/Technique)	Q1 : Quels sont les flux SWIFT critiques pour le métier (MT103, MT940) et comment sont-ils traités (via Smart Stream) ?
	Q2 : Comment les messages SWIFT sont-ils intégrés au système central (DELTA) et validés par les agences ?
Gestion des accès (Métier/Technique)	Q3 : Comment se passe la procédure de la création des nouveaux profils de système Swift ?
	Q4 : Comment l'authentification multifacteur (MFA) est-elle appliquée pour les accès critiques (CSP-C04) ?
Gestion des habilitations (typologie des utilisateurs du système)	Qui sont les utilisateurs habilités à accéder aux systèmes SWIFT (opérateurs, administrateurs) ?
Intégration avec d'autres systèmes (Métier/Technique)	Q5 : Comment SWIFT interagit-il avec les autres outils (FICO pour l'analyse des risques, CORISI pour les garanties) ?
	Q6 : Comment les messages SWIFT (MT) sont-ils enrichis ou filtrés par ces systèmes (blocage de transactions via SIRON AML) ?
	Q7 : Comment CORONA SMARTSTREAM et SIRON AML renforcent-ils la détection en temps réel des risques (sanctions, blanchiment) ?
	Q8 : Quel rôle jouent FINASTRAKTP et DELTA dans l'optimisation des flux financiers (couverture de change, gestion de liquidités) ?

	Q9 : Comment les intégrations avec KYC et FATCA garantissent-elles l'alignement avec les régulations (vérification des bénéficiaires, reporting fiscal) ?
	Q10 : Quels mécanismes de chiffrement (AES-256) ou de traçabilité (logs SIEM) sont appliqués pour sécuriser ces interactions ?
Conformité métier et gestion de plateforme SWIFT	Q11 : Qui valide les modifications des workflows SWIFT (mise à jour des MT messages) ? Q12 : Qui géré la plateforme SWIFT

Source : élaboré par nous-mêmes.

Axe 2 : **Les bonnes pratiques ISO 27001 appliquées au SI SWIFT**	**Questions**
Sécurité des transactions (Technique)	Q13 : Le chiffrement AES-256 est-il appliqué à tous les messages SWIFT (MT940, MT950) en transit et au repos ?
	Q14 : Les sauvegardes des données SWIFT sont-elles stockées de manière sécurisée et chiffrées ?
Gestion des risques	Q15 : Une cartographie des risques SWIFT est-elle mise à jour régulièrement (A.6.1.2) ?
	Q16 : Quelles méthodes (EBIOS, MEHARI) évaluent les risques résiduels ?
Audit et amélioration continue	Q17 : Un audit interne du SI SWIFT a-t-il été réalisé ?
	Q18 : Comment évaluer la vigilance des collaborateurs (phishing, gestion des mots de passe) ?
	Q19 : Un programme de formation dédié à la sécurité SWIFT existe-t-il ?

Source : élaboré par nous-mêmes.

- **Déroulement de l'entretien :**

Pour approfondir l'évaluation de la conformité du SI SWIFT à la norme ISO 27001, une série d'entretiens semi-directifs a été réalisée en avril 2024 au siège social de la Banque BEA, en parallèle de l'audit semestrielle de conformité. Trois profils stratégiques ont été sollicités : le responsable métier du SI SWIFT (pour éclairer le fonctionnement

opérationnel du système), l'informaticien (sur l'implémentation technique des contrôles de sécurité) et l'auditeur interne (pour évaluer les bonnes pratiques ISO 27001). Chaque entretien, d'une durée de 60 minutes, a été mené individuellement afin de garantir la confidentialité et la sincérité des échanges. Une grille d'entretien structurée a servi de support, articulée autour des exigences clés de l'ISO 27001 (Annexe A, gestion des risques, Politique de Sécurité des Systèmes d'Information) et des spécificités du SI SWIFT/CSPSWIFT (gestion des accès, traçabilité des transactions, chiffrement). Cette approche a permis de croiser les perspectives techniques, organisationnelles et normatives, tout en s'adaptant aux enjeux pratiques du système SWIFT et aux priorités stratégiques de la Banque BEA.

2.3.2 La checklist ISO 27001

La checklist ISO 27001 est intégrée aux entretiens afin de servir d'outil opérationnel pour identifier les zones de friction entre les exigences normatives et les pratiques terrain. Alignée sur les contrôles spécifiques de l'ISO 27001, cette checklist permet non seulement de structurer les échanges autour des enjeux clés (gestion des incidents, continuité d'activité), mais aussi d'approfondir l'analyse des écarts entre les prescriptions théoriques et les réalités organisationnelles. Elle facilite également la comparaison des points de vue des différents acteurs impliqués (équipes IT, DSSI, auditeurs internes/externes), révélant ainsi les tensions interservices et les compromis opérationnels qui influencent la mise en œuvre des mesures de sécurité. En outre, cet outil méthodologique sert à structurer les échanges, à identifier les écarts, à faciliter la triangulation. La checklist n'est pas rigide, elle s'adapte aux interprétations locales des normes.

2.4 Les techniques de recueil et analyse les données

2.4.1 L'approche sémantique

Nous avons privilégié une analyse sémantique manuelle afin de saisir la richesse et la complexité des propos recueillis : en codant directement les idées, les concepts et leurs cooccurrences, cette démarche inductive permet de faire émerger des thèmes inédits, de conserver le contexte d'énonciation et de rendre compte de la dynamique des significations attribuées par les participants, ce qu'aucune méthode purement automatisée ne saurait reproduire avec la même finesse.

2.4.2 Analyse documentaire

Une fois notre sujet a été validé, nous avons commencé par exploité certains articles scientifiques en liaison avec notre thématique. Après leurs analyses, cela nous a permet de déterminer les concepts et le choix de la méthodologie ainsi que la méthode, les outils et les techniques d'analyse à retenir pour le déroulement de la partie expérimentale. Le reste de la documentation interne propre à l'entreprise nous sera remise que lors de la réalisation de l'entretien proprement dit. Elle peut inclure différents types de documents, tels que l'organigramme, des rapports et des documents internes. Politique qualité, cartographie de risque. Les données obtenues par l'analyse documentaire sont utilisées pour fournir un contexte et une compréhension du sujet d'étude.

2.4.3 Échelle d'évaluation

Les échelles d'évaluation sont des outils essentiels dans les démarches de diagnostic organisationnel. Elles permettent de mesurer un phénomène, de situer un niveau de conformité ou de maturité, de comparer les résultats dans le temps ou entre entités, et d'orienter les recommandations d'amélioration. Une échelle est considérée comme valide lorsqu'elle mesure effectivement ce qu'elle est censée évaluer, en lien direct avec les objectifs de l'étude.

Dans le cadre de notre évaluation du système de management de la sécurité de l'information, nous avons retenu l'échelle SAMI (Standard Assessment Maturity Index), un modèle de maturité en quatre niveaux. Cette méthode a été adaptée pour mesurer le niveau d'implémentation des exigences de la norme ISO/CEI 27001 :2022, en combinant des observations terrain, des audits documentaires et des entretiens. L'approche SAMI offre une lecture qualitative nuancée, permettant de qualifier chaque exigence comme étant :0 : Non appliquée ; 1 : Partiellement appliquée (informel) ; 2 : Formalisé et déployée localement ; 3 : Opérationnelle et optimisée

Cette échelle présente plusieurs avantages : elle permet d'apprécier les écarts selon leur gravité, de mesurer la progression entre deux évaluations successives, et de cibler les domaines nécessitant des plans d'action prioritaires. Elle est couramment utilisée dans le domaine de la gouvernance de la sécurité de l'information, notamment dans les guides d'implémentation de la norme ISO 27001 (Green, 2022).

- **Echelle SAMI**

Tableau 9 : Echelle SAMI

Score	Description synthétique	Exemples de preuves
0	Non appliqué /Aucun contrôle en place rapport à l'ISO 27001 :2022	▪ Absence de documentation ▪ Zéro action enregistrée
1	Informel / Partiel Initiatives ponctuelles	▪ Procédures en projet ▪ Notes internes ▪ E-mails ▪ Responsabilités floues
2	Formalisé / Déployé localement Processus définis	▪ Manuel de procédures diffusé ▪ Audits internes initiaux ▪ KPI de pilotage
3	Opérationnel et optimisé Contrôle pleinement intégré	▪ Rapports d'audits externes ▪ Indicateurs de performance stables (> 90 %) • Revues de direction

Source : élaboré par nous-mêmes à l'aide de (Green, 2022).

2.4.4 Détermination de la méthode d'analyse

Les résultats des entretiens avec les acteurs clés (responsable métier SI SWIFT, informaticien, auditeur) seront utilisés pour évaluer la mise en œuvre pratique des contrôles de sécurité du SI SWIFT en regard des exigences de l'ISO 27001. La méthode d'analyse retenue est l'analyse directe, structurée autour d'indicateurs quantitatifs (échelle de 0 à 3) pour mesurer l'efficacité des mesures techniques, identifier les écarts par rapport à l'Annexe A de la norme, et apprécier la maturité des processus. Les réponses des interviewés seront synthétisées en pourcentages moyens, permettant de distinguer les points forts et les axes d'amélioration, tout en respectant les contraintes de confidentialité inhérentes aux données bancaires.

2.5 L'analyse des écarts

Les résultats d'analyse des données seront présentés de manière claire et concise sous forme de graphiques individuels type histogramme afin d'identifier les points forts et les points faibles pour chaque clause de la norme ISO 27001, et pour chaque contrôle de l'Annex A, en respectant le périmètre cible. A la fin, une représentation graphique globale sous forme de radar permet d'avoir un aperçu global sur l'ensemble des catégories à identifier les principales opportunités d'amélioration, ainsi que leur impact potentiel. Un plan d'action sera proposé pour des actions d'amélioration.

Clause	Exigences de la norme iso 27001 ;2022	Questions D'évaluation	Réponse Oui/non	Preuve	Notation	Evaluation

2.6 Plan d'action recommandé pour l'étude

Fondé sur les résultats de la check-list ISO 27001 et des entretiens semi-directifs, le plan d'action proposé vise à transformer les écarts identifiés en leviers d'amélioration continue. Cette démarche s'inscrit dans une logique constructiviste ingénierique, où les recommandations sont coconstruites avec les acteurs (DSSI, RSSI, auditeurs) pour garantir leur pertinence contextuelle.

La priorisation des écarts critiques repose sur une évaluation structurée des écarts révélés par la check-list ISO 27001. Ces écarts sont hiérarchisés selon deux critères principaux : l'impact opérationnel, qui prend en compte les risques associés aux lacunes, et la faisabilité, qui évalue les ressources nécessaires pour combler ces écarts (techniques, humaines ou budgétaires). Cette démarche s'inspire des principes de l'actionnabilité, garantissant que les solutions proposées soient adaptées aux contraintes locales et applicables dans le contexte organisationnel spécifique. En intégrant ces deux dimensions, cette méthode permet d'identifier les priorités stratégiques pour renforcer la sécurité du système d'information tout en assurant une allocation optimale des ressources disponibles.

CHAPITRE III : RESULTATS ET DISCUSSION

Le chapitre III porte sur l'analyse empirique menée dans le cadre de notre recherche. Il se structure en deux sections complémentaires, la première présente les résultats obtenus à partir des données recueillies et des traitements analytiques réalisés ; la seconde est consacrée à leur interprétation et à l'analyse critique de leurs implications. Cette étape est cruciale pour répondre à notre problématique et atteindre nos objectifs.

Section 01 : Présentation et analyse des résultats

Cette section présente les résultats issus de l'étude menée. Elle repose sur l'analyse des données recueillies ainsi que sur les traitements analytiques effectués, permettant ainsi de mettre en évidence les principaux constats observés dans le cadre de notre recherche.

1. Résultats de l'observation documentaire

Dans le cadre de l'évaluation de la conformité du système d'information SWIFT à la norme ISO 27001, nous avons observé et recensé plusieurs documents internes de la BEA. Cette observation a permis de mettre en évidence les pratiques de sécurité en place, leur conformité avec la norme, ainsi que les restrictions liées à la confidentialité des données. Le tableau ci-dessous présente ces documents, leur rôle dans l'évaluation, ainsi que les limites d'accès et d'utilisation qui leur sont associées.

Tableau 10 : Les documents consultés dans le cadre de l'évaluation de la conformité du SI SWIFT (ISO 27001)

Documents consultés dans le cadre de l'évaluation de la conformité du SI SWIFT (ISO 27001)		
Document	**Rôle dans l'évaluation iso 27001**	**Contrainte de confidentialité**
Journaux d'audit Swift	Analyser la traçabilité des transactions et détecter des anomalies de sécurité.	Interdiction de copier, scanner ou citer des extraits (données sensibles montants, identifiants).
Politique de sécurité interne	Évaluer l'alignement des règles de l'entreprise avec l'ISO 27001.	Accès restreint au texte intégral ; interdiction de reproduire des clauses spécifiques.
Contrats avec	Vérifier les obligations légales et les	Clauses confidentielles non divulgables

Documents consultés dans le cadre de l'évaluation de la conformité du SI SWIFT (ISO 27001)		
SWIFT	responsabilités en cas de violation.	(pénalités, engagements techniques).
Plan d'action semestriel	Évalué semestriellement par le Comité Sécurité et le CISO, avec validation finale par l'Audit Interne.	Classé Interne Confidentiel ; accessible uniquement aux équipes Sécurité, Direction et Audit, version horodatée, non diffusable à l'extérieur sans autorisation écrite.
Cartographie de risque	Pilotée par le département Gestion des Risques, revue régulière par le Responsable SSI et auditée annuellement dans le cadre ISO 27001.	Classée Confidentiel Risques ; restreinte aux propriétaires de risques et à l'Audit Interne, transit en chiffrement et archivage sous contrôle d'accès strict.
CSP Control Framework (CSCF)	Évaluation interne par les SME (Subject-Matter Experts) complétée, selon périmètre, par des certifications externes (SOC 2, PCI-DSS, NIST) offrant un « confort raisonnable »	Publication confidentielle : ne peut être divulguée hors organisation sans accord écrit préalable ; partage possible « sur base du besoin de savoir » avec tierces parties soumises à des obligations de confidentialité équivalentes
Cahier de charge	Un cahier des charges dédié pour mobiliser une équipe d'experts informaticiens pour la mise en place du Système de Management de la Sécurité de l'Information (SMSI).	Document contractuel soumis à clause de confidentialité ; accès uniquement par l'autorisation de DSSI.

Source : élaboré par nous-mêmes à partir des documents internes de l'entreprise.

Les documents consultés durant le stage à la BEA dans le cadre de l'évaluation de la conformité du système SWIFT à la norme ISO 27001 sont essentiels pour vérifier la mise en œuvre effective des exigences de sécurité. Chaque document joue un rôle spécifique dans l'analyse (traçabilité, alignement réglementaire, gestion des risques, obligations contractuelles, planification de la sécurité, etc.), tout en étant fortement encadré par des contraintes de confidentialité strictes. L'accès est généralement restreint aux parties prenantes internes, et la diffusion extérieure est rigoureusement contrôlée, ce qui reflète la sensibilité élevée des informations traitées dans un contexte bancaire soumis à des normes de sécurité rigoureuses. Cette gestion restrictive garantit la conformité aux exigences de

l'ISO 27001 et protège l'intégrité du système d'information face aux risques internes et externes.

Dans le cadre de notre étude sur la conformité du système SWIFT de la BEA à la norme ISO 27001, les mentions légales associées aux documents consultés jouent un rôle essentiel. Elles précisent que ces documents contiennent des informations strictement confidentielles, protégées par des règles précises de non-divulgation. Par conséquent, leur utilisation et leur partage sont limités à des conditions rigoureuses, notamment avec des personnes autorisées et soumises à l'obligation de confidentialité. Cette exigence a directement influencé notre approche de la recherche documentaire, nous imposant de respecter des règles strictes d'accès, de traitement et de présentation des données. Ce cadre nous a permis de mieux appréhender l'importance de la sécurité de l'information, non seulement sur le plan technique, mais également juridique et éthique, renforçant ainsi la rigueur et la fiabilité de notre démarche. Les détails complets des mentions légales sont consultables en annexe.

2. Résultats des entretiens

2.1 Analyse synthétique des entretiens

Tableau 11: Analyse synthétique des entretiens

Axe 1 **Questions**	**Responsables interviewés**	**Synthèse des intervenants**
Q1 : Quels sont les flux SWIFT critiques pour le métier (MT103, MT940) et comment sont-ils traités (via Smart Stream) ?	▪ Ingénieur d'État en Informatique Principal Sécurité Informatique ▪ Cheffe de secteur normes / Responsable secteur normes	D'après les intervenants Smart Stream prend en charge en priorité deux formats SWIFT : le MT103, dédié aux virements internationaux, qui transite par le Payments Hub pour validation, enrichissement des données et routage en flux STP ; et le MT940, relatif aux relevés de compte fin de journée, traité par le module TLM Reconciliation pour un rapprochement comptable automatisé et la gestion des exceptions, garantissant une traçabilité intégrale.

Q2 : Comment se passe la procédure de la création des nouveaux profils de système Swift ?	▪ Administrateur principal de SWIFT	Selon l'administrateur principal de système SWIFT, la création des profils SWIFT s'initie par une demande d'accès soumise par les opérateurs via la DSSI, puis relayée à la Direction du Commerce Extérieur SWIFT (DCE), qui se voit explicitement mandatée pour instancier les comptes utilisateurs dans le système. Cette étape pose les fondations de l'accès aux ressources critiques. Une fois le compte créé, la Direction de la Conformité intervient pour appliquer le principe du moindre privilège en assignant les rôles et permissions strictement nécessaires à l'exercice des fonctions de chaque opérateur ; ainsi, un utilisateur habilité à traiter les messages MT103 ne disposera pas des droits pour gérer les transactions de trésorerie ou modifier les paramètres système, garantissant une sécurité fine et compartimentée. ▪ Prenant l'exemple, un opérateur peut être limité à la transformation des messages monétaires (MT103), sans accès aux transactions de trésorerie ou aux paramètres système.
Q3 : Qui sont les utilisateurs habilités à accéder aux systèmes SWIFT (opérateurs, administrateurs) ?	▪ Administrateur principal de SWIFT	Selon l'administrateur principal de système SWIFT, les accès au système SWIFT sont strictement encadrés selon des profils bien définis. Quatre catégories principales d'utilisateurs sont habilitées : ▪ Les opérateurs métiers, responsables de la gestion quotidienne des transactions financières, ▪ Les administrateurs SWIFT, chargés de la configuration des comptes, certificats et droits d'accès, ▪ Les techniciens IT, en charge de l'installation et de la maintenance des plateformes SWIFT, ▪ Les auditeurs internes, qui accèdent aux journaux à des fins de traçabilité et de conformité. Chaque rôle fait l'objet d'un contrôle d'habilitation rigoureux, fondé sur le principe du moindre privilège, garantissant ainsi une gestion

		sécurisée et traçable des accès au système SWIFT.
Q4 : Comment SWIFT interagit-il avec les autres outils (FICO pour l'analyse des risques, CORISI pour les garanties) ?	▪ Administrateur principal de SWIFT ▪ ▪ Cheffe de secteur normes / Responsable secteur normes	Selon l'administrateur principal de SWIFT, et la Responsable secteur normes, SWIFT joue le rôle de plateforme centrale, interfaçant en temps réel avec des outils critiques tels que FICO (analyse de risque) et CORISI (gestion de l'inventaire) via des API sécurisées (TLS 1.3, chiffrement AES-256) et des middlewares IBM MQ. Les messages SWIFT (MT103 – paiements, MT700 – crédits documentaires) alimentent les modèles prédictifs de FICO, qui identifient automatiquement les anomalies et peuvent suspendre ou signaler une transaction à la Direction de la Conformité. ▪ Exemple 1 : un paiement international jugé à haut risque par FICO est immédiatement mis en attente pour examen). Simultanément, CORISI vérifie le statut des garanties contractuelles ; si une caution est expirée ou insuffisante, l'opération SWIFT est bloquée ▪ Exemple 2 : un client ne peut pas initier de virement tant que sa garantie n'est pas conforme). L'ensemble de ces flux bidirectionnels est tracé selon les exigences du SWIFT CSP, assurant la transparence et la fiabilité du processus.
Q5 : Comment les messages SWIFT (MT)	▪ Administrateur principal de SWIFT	D'après les échanges avec l'administrateur principal de SWIFT, Les messages SWIFT sont

sont-ils enrichis ou filtrés par ces systèmes (blocage de transactions via SIRON AML) ?		enrichis et filtrés via des intégrations automatisées avec des systèmes comme SIRON AML : les données transitent via API REST/middleware, sont enrichies avec des listes de sanctions et des règles métier, puis analysées en temps réel pour détecter les risques (montants suspects, pays sous embargo). Les transactions non conformes sont bloquées automatiquement ou soumises à vérification manuelle, avec journalisation des alertes pour audits réglementaires (SWIFT CSP)
Q6 : Comment CORONA SMARTSTREAM et SIRON AML renforcent-ils la détection en temps réel des risques (sanctions, blanchiment) ?	▪ Administrateur principal de SWIFT	▪ Selon l'administrateur principal de SWIFT, au sein de l'environnement Smart Stream, le moteur de filtrage CORONA et le module SIRON AML passent chaque message SWIFT au crible en temps réel pour détecter les risques financiers : ▪ CORONA compare systématiquement les transactions aux listes de sanctions pays et entités constamment actualisées, ▪ SIRON mobilise des algorithmes de détection de schémas (montants atypiques, bénéficiaires à risque, etc.) pour repérer d'éventuelles tentatives de blanchiment. Tout paiement suspect est alors automatiquement interrompu via des API sécurisées, et chaque action fait l'objet d'un journal d'audit complet, conforme aux exigences de traçabilité du SWIFT CSP.
Q7 : Quel rôle jouent FINASTRAKTP et DELTA dans l'optimisation des flux financiers (couverture de change, gestion de liquidités) ?	▪ Cheffe de secteur normes / Responsable secteur normes	▪ Selon la Responsable secteur normes, la plateforme intègre deux modules clés pour optimiser les flux financiers : ▪ FINASTRAKTP, qui analyse en temps réel les messages SWIFT MT300 relatifs aux contrats à terme et exécute automatiquement des stratégies de couverture de change (hedging) pour limiter l'exposition aux variations de taux,

		▪ DELTA, qui consolide les positions de trésorerie issues des relevés MT940/MT950, ajuste dynamiquement les conversions de devises et anticipe les besoins de liquidité grâce à des algorithmes prédictifs, offrant ainsi un pilotage proactif et optimisé du cash management.
Q8. Comment les intégrations avec KYC et FATCA garantissent-elles l'alignement avec les régulations (vérification des bénéficiaires, reporting fiscal) ?	▪ Administrateur principal de SWIFT	▪ Selon l'administrateur principal de SWIFT, les modules d'intégration KYC et FATCA garantissent la conformité réglementaire : ▪ Le composant KYC exécute une vérification automatisée des bénéficiaires finaux sur les flux MT103 en recoupant les informations avec des registres officiels (Registre du Commerce) et en signalant toute discordance d'identité, ▪ Le module FATCA extrait programmatiquement les données des relevés MT940/MT950 pour identifier les comptes détenus par des contribuables américains et générer des rapports fiscaux au format XML, prêts à être transmis à l'IRS.
Q9 : Quels mécanismes de chiffrement (AES-256) ou de traçabilité (logs) sont appliqués pour sécuriser ces interactions ?	▪ Administrateur principal de SWIFT	Selon l'administrateur principal de SWIFT, la communication avec le système est sécurisée par le chiffrement AES-256, protégeant les données en transit et au repos. Un système de monitoring centralise et analyse les journaux d'activité en temps réel pour détecter les comportements suspects et générer des alertes. De plus, la journalisation est conforme au SWIFT Customer Security Programme (CSP), assurant la traçabilité des actions telles que l'envoi de messages et la gestion des profils utilisateurs, avec des signatures numériques garantissant l'intégrité des messages et des journaux.
Q10 : Qui valide les modifications des	▪ Ingénieur d'État en Informatique Principal -	Selon les échanges avec l'Ingénieur d'Informatique et le Directeur de la Conformité

workflows SWIFT (mise à jour des MT messages) ? ▪ Qui géré la plateforme SWIFT ?	Sécurité Informatique ▪ Directeur de la conformité ▪ Administrateur principal de SWIFT	et l'administrateur principal de SWIFT, toute évolution des workflows SWIFT s'inscrit dans une boucle de validation multi-acteurs : la Direction du Commerce Extérieur (DCE) formalise les besoins métier, la DSI conduit les tests fonctionnels et de compatibilité, tandis que la DSSI et la Conformité vérifient l'alignement réglementaire, avant pour finir un arbitrage du Comité de Pilotage. En exploitation courante, la DCE gère les opérations en coordination avec la DSSI pour la maintenance technique et la Conformité pour les audits, assurant ainsi un parfait équilibre entre agilité opérationnelle, robustesse technique et respect des exigences légales. • Exemple, l'ajout de champs personnalisés dans le MT103 pour renforcer la traçabilité interne a été validé après analyses techniques et absence de risques, et l'automatisation de l'envoi des MT103 avec intégration d'un workflow dédié à la résolution des litiges illustre la maturité et l'efficacité de cette gouvernance collaborative.

Source : élaboré par nous-mêmes.

Sur la base des entretiens menés avec les responsables de la DCE, de la DSI et de la DSSI, il ressort que le fonctionnement du système SWIFT repose sur une architecture normalisée et hautement automatisée, articulée autour de messages structurés tels que le MT103 pour les paiements internationaux et le MT940 pour les relevés de comptes. Ces flux sont traités par des modules spécialisés au sein de la plateforme Smart Stream : le Payments Hub gère les MT103 en assurant leur validation, l'enrichissement des données et leur routage en mode STP (Straight Through Processing), tandis que TLM Réconciliation traite les relevés MT940 pour le rapprochement comptable et la gestion des exceptions, garantissant une traçabilité complète.

La gestion des accès au système SWIFT, repose sur une démarche institutionnelle intégrée combinant rigueur opérationnelle, conformité réglementaire et sécurité. Le processus débute par une demande formalisée via la DSSI, transmise à la Direction du Commerce Extérieur SWIFT, (DCE) pour la création technique des utilisateurs, étape primordiale

pour structurer les accès critiques. La Direction de conformité attribue ensuite des rôles et permissions contextuels, appliquant le principe RBAC (Role-Based Access Control) pour limiter les risques d'accès non autorisés, aussi la direction de conformité valide cette configuration en s'assurant de son alignement avec les normes SWIFT CSP (CSP-C01) et ISO 27001, en s'appuyant sur des outils d'audit automatisés et des contrôles manuels.

La Banque Extérieure d'Algérie a instauré un système de gestion des accès au réseau SWIFT rigoureusement structuré selon une approche fondée sur les rôles et responsabilités, conforme aux principes de moindre privilège et de séparation des tâches, en alignement avec la norme ISO 27001 (annexe A.9) et les exigences du SWIFT (CSP). Ce dispositif repose sur une segmentation claire des profils utilisateurs. Les opérateurs métiers, affectés aux agences, à la Direction de l'International ou encore à la Trésorerie, sont strictement habilités à exécuter des opérations financières via les formats MT/MX, à contrôler les paiements transfrontaliers et à superviser les files d'attente, sans accès aux fonctions administratives. Les administrateurs SWIFT disposent de privilèges élevés leur permettant de gérer les comptes utilisateurs, les certificats RMA, les droits d'accès et la configuration interbancaire, tout en veillant à l'application stricte des politiques de sécurité imposées par le CSP. Les opérateurs techniques, issus de l'équipe IT, assurent le bon fonctionnement des plateformes (Alliance Access, Lite2) à travers l'installation, la maintenance et la surveillance des flux, sans intervenir dans les traitements transactionnels, leurs accès étant encadrés par des contrôles techniques renforcés. Enfin, les auditeurs internes disposent d'un accès restreint aux journaux d'activité afin de vérifier la traçabilité des actions, la conformité des habilitations et le respect des politiques de sécurité, dans un cadre de consultation sécurisé et journalisé. Cette gouvernance granulaire des accès permet non seulement de réduire la surface d'exposition aux risques, mais aussi de garantir une traçabilité complète et une conformité robuste, consolidant ainsi la résilience globale du système SWIFT de la BEA face aux menaces internes et externes.

L'analyse des interactions entre SWIFT, FICO et CORISI, souligne que SWIFT ne se contente pas de transférer des messages en silo, mais se positionne comme une plateforme intégrée et sécurisée; interconnectée en temps réel à FICO et CORISI via API REST/TLS et IBM MQ, Reposant sur une infrastructure on-premise entièrement maîtrisée et hébergée localement en Algérie, l'architecture SWIFT de la BEA constitue une plateforme intégrée, sécurisée et souveraine, sans aucune intervention externe. Conçue pour fonctionner en temps réel, elle s'appuie sur des API REST sécurisées (chiffrement TLS 1.3) et des

middlewares IBM MQ assurant une interconnexion continue avec des systèmes critiques comme FICO (détection de fraude) et CORISI (vérification contractuelle). Les messages sensibles, notamment les MT103 et MT700, sont automatiquement analysés par des modèles d'intelligence artificielle capables d'identifier et de bloquer toute opération suspecte ou non conforme, tandis que CORISI valide en parallèle la couverture contractuelle des transactions. Tous les flux sont chiffrés en AES-256 à l'aide de clés privées détenues uniquement par la BEA, garantissant une confidentialité absolue. Les données, qu'elles résident dans EBS ou RDS Oracle, ainsi que les logs (VPC Flow Logs, MQ, etc.) sont centralisés et analysés via un système de monitoring interne, assurant une journalisation exhaustive conforme aux exigences du SWIFT CSP-C02 et de la norme ISO/IEC 27001. L'intégration des modules FINASTRAKTP (gestion du change – MT300) et DELTA (gestion de trésorerie – MT940) permet d'optimiser les opérations financières, tandis que les contrôles réglementaires sont automatisés grâce à des vérifications KYC en ligne et la génération de rapports FATCA. Ce dispositif unifié, mis à jour via des correctifs téléchargés offline et validés manuellement, reflète une approche robuste combinant souveraineté technologique, efficacité opérationnelle, sécurité multicouche et conformité réglementaire continue.

Le dispositif de sécurité et de gouvernance mis en œuvre autour du système SWIFT à la (BEA) repose sur une architecture technique et organisationnelle rigoureuse, visant à garantir la confidentialité, l'intégrité et la traçabilité des opérations financières critiques. Sur le plan technique, la protection des données est assurée par un chiffrement de type AES-256, appliqué aussi bien aux flux en transit qu'aux données stockées, conformément aux standards les plus élevés de sécurité. Ce socle est renforcé par un système de monitoring centralisé qui analyse en temps réel les journaux d'activité, détecte automatiquement les comportements inhabituels et génère des alertes en cas d'événement suspect, assurant une surveillance proactive du système. Chaque action sensible qu'il s'agisse de l'émission de messages financiers ou de la gestion des comptes d'utilisateurs est enregistrée et signée numériquement, garantissant une traçabilité complète et l'intégrité des journaux conformément aux exigences du SWIFT (CSP). En parallèle, toute évolution des processus ou des messages SWIFT suit un circuit de validation strict, mobilisant plusieurs entités clés : la Direction du Commerce Extérieur exprime les besoins fonctionnels, la DSI teste la faisabilité technique, la DSSI et la Direction de la Conformité contrôlent l'alignement réglementaire, puis le Comité de

Pilotage statue en dernier ressort. Ce fonctionnement transversal assure une coordination fluide entre les métiers, l'IT et les fonctions de contrôle, comme en témoignent les projets validés tels que l'ajout de champs personnalisés dans les messages MT103 ou l'automatisation des traitements liés aux litiges. En exploitation quotidienne, cette collaboration se prolonge par un pilotage partagé entre les équipes opérationnelles, techniques et de conformité, assurant ainsi robustesse, agilité et conformité continue du système SWIFT.

Des revues semestrielles, associées à une journalisation exhaustive des actions (qui, quand, pourquoi), assurent une adaptation continue aux évolutions métier et réglementaires. Parallèlement, la séparation des rôles et la traçabilité des opérations renforcent la résilience face aux cybermenaces. Ce modèle, fondé sur une collaboration interdirectionnelle et une documentation conforme aux normes, incarne une approche proactive de la sécurité, alignée sur les standards internationaux et conçue pour minimiser les risques opérationnels.

Tableau 12 : La gestion des accès au système SWIFT

Étape	Acteur Principal	Action	Indicateurs Clés
1. Soumission de la Demande d'Accès (DSI)	Un Opérateur/ DSI	Soumet une demande de nouveau operateurs un accès via le portail interne ou un formulaire dédié.	▪ Séparation des Tâches : Personne ne peut soumettre et approuver seule.
2. Création de l'Utilisateur	Direction du Commerce Extérieur SWIFT /DCE	Crée le profil utilisateur dans le système SWIFT avec les informations de base.	▪ Principe du Moindre Privilège : Attribution des permissions minimales nécessaires.
3. Définition des Rôles et Permissions et Validation de la Conformité	Direction de la Conformité	Attribue les rôles spécifiques	▪ Conformité aux Normes SWIFT : Respect des normes du SWIFT CSCF pour l'attribution des rôles et permissions. ▪ Maintenir un log des actions liées à la validation pour faciliter les audits.

4. Activation de l'Accès	Direction du Commerce Extérieur SWIFT/ DCE	Active l'accès utilisateur dans le système SWIFT après validation	▪ Revue Annuelle des Accès : Vérification périodique des accès pour s'assurer de leur pertinence et conformité

Source : élaboré par nous-mêmes à partir des entretiens.

Après avoir examiné l'architecture et le fonctionnement opérationnel du système SWIFT, il convient désormais de s'intéresser à un second axe tout aussi déterminant : l'analyse des bonnes pratiques issues de la norme ISO 27001 appliquées au sein du système SWIFT de la BEA.

Axe 02 Questions	Responsables interviewés	Synthèse des intervenants
Q11 : Le chiffrement AES-256 est-il appliqué à tous les messages SWIFT (MT940, MT950) en transit et au repos ?	Ingénieur d'État en Informatique Principal - Sécurité Informatique	L'ingénieur a répondu par l'affirmative, en précisant que le chiffrement AES-256 est bien appliqué aux messages SWIFT (MT940, MT950) au repos, conformément aux exigences de sécurité en vigueur. Ces données sensibles sont hébergées en local (on-premise) en Algérie, sans intervention externe, et leur accès est strictement restreint. En transit, les flux sont sécurisés par le protocole TLS 1.3, garantissant la confidentialité et l'intégrité des communications. La gestion du chiffrement est assurée en interne par la BEA, notamment via des clés privées et des processus rigoureux, y compris des mises à jour offline, renforçant ainsi le contrôle total sur la sécurité du système.
Q12 : Les sauvegardes des données SWIFT sont-elles stockées de manière sécurisée et chiffrées ?	▪ Ingénieur d'État en Informatique Principal - Sécurité Informatique	L'ingénieur confirme que les sauvegardes des données SWIFT sont entièrement chiffrées en AES-256 et stockées localement sur site (on-premise), sans aucun hébergement cloud. Elles sont enregistrées sur des supports WORM, garantissant l'intégrité des archives, et gérées exclusivement par la BEA, avec un accès restreint aux administrateurs certifiés SAGP.

		Toutes les opérations sont journalisées, les sauvegardes des données SWIFT sont entièrement chiffrées en AES-256 et stockées localement sur site (on-premise), sans aucun hébergement cloud. Elles sont enregistrées sur des supports WORM, garantissant l'intégrité des archives, et gérées exclusivement par la BEA, avec un accès restreint aux administrateurs certifiés SAGP. Toutes les opérations sont journalisées,
Q13 : Quelles méthodes (EBIOS, MEHARI) évaluent les risques résiduels ?	▪ Ingénieur d'État en Informatique Principal Sécurité Informatique	Selon Ingénieur d'État en Informatique Principal, La DSSI a retenu la méthode MEHARI pour son alignement avec le SWIFT CSP et la norme ISO/IEC 27005. Toutefois, bien que cette méthode intègre des scénarios de fraude, ceux-ci n'ont pas été mis en œuvre à ce jour,
Q14 : Une cartographie des risques SWIFT est-elle mise à jour régulièrement (A.6.1.2) ?	▪ Ingénieur d'État en Informatique Principal - Sécurité Informatique	Conformément aux préconisations d'ingénieur d'État en Informatique Principal Non, bien qu'une cartographie des risques existe, elle n'est pas actualisée de manière régulière et formalisée. Aucun scénario de type MEHARI n'a été appliqué jusqu'à présent, malgré la faisabilité technique. La responsabilité de cette démarche relève principalement des équipes métier (conformité, gestion KYC), tandis que la DSSI se limite au volet technique.
Q15 : Un audit interne du SI SWIFT a-t-il été réalisé ?	▪ Le directeur des auditeurs	Selon le directeur des auditeurs, Un audit interne du système SWIFT a été réalisé sous la supervision de la Direction de l'Audit Interne, avec l'appui d'experts informaticiens externes spécialisés en cybersécurité et en normes ISO 27001
Q16 : Un programme de formation dédié à la norme ISO 27001 existe-t-il ?	▪ Le directeur de sécurité de système d'information	Selon la DSSI, la BEA a déployé un programme de formation agile, mêlant enseignements théoriques et ateliers pratiques, pour faciliter l'adoption de la norme ISO 27001 et la mise en œuvre de son SMSI.
Q17 : Comment évaluer la vigilance des collaborateurs (phishing, gestion des mots de passe) ?	▪ Le directeur des auditeurs	Selon le Directeur des Audits, la vigilance se mesure avant tout par des simulations de phishing pour tester les réactions, des audits techniques des mots de passe et l'analyse d'indicateurs clés (activation MFA, scores de formation, incidents liés à l'erreur humaine), enrichis par des enquêtes de perception, le tout intégré dans un cycle d'amélioration continue.

Source : élaboré par nous-mêmes à partir des entretiens.

L'analyse des pratiques sécuritaires mises en œuvre par la Banque Extérieure d'Algérie dans le cadre du système SWIFT révèle un engagement affirmé en matière de protection des données critiques, conforme aux standards internationaux en vigueur (ISO 27001, SWIFT CSP).

Premièrement, la confidentialité et l'intégrité des messages SWIFT (MT940, MT950) sont garanties via un chiffrement AES-256 à l'état de repos, ainsi que par le protocole TLS 1.3 en transit. L'ensemble du système est hébergé localement (on-premise) sur le territoire algérien, sans recours à des fournisseurs de cloud ou à des interventions externes, ce qui renforce le contrôle souverain sur l'infrastructure critique. La gestion interne des clés de chiffrement privées et la télédistribution des correctifs en mode offline illustrent une maîtrise complète du cycle de sécurité, réduisant considérablement la surface d'exposition aux cybermenaces.

Deuxièmement, la politique de sauvegarde des données SWIFT obéit aux plus hauts standards. Les backups sont chiffrés systématiquement, stockés sur des supports WORM (Write Once, Read Many), et accessibles uniquement aux administrateurs certifiés, ce qui garantit l'inaltérabilité, la traçabilité et la conformité avec le SWIFT CSP-C05. Le système de journalisation mis en place permet un suivi rigoureux des accès, consolidant les exigences d'audit et de responsabilité.

Cependant, malgré ces mesures techniques robustes, des lacunes subsistent sur le plan de la gestion des risques métier. La DSSI a bien adopté la méthode MEHARI, reconnue pour son alignement avec ISO/IEC 27005 et le SWIFT CSP, mais n'a pas encore mis en œuvre les scénarios de fraude intégrés dans cette méthode. Cette absence de simulation affaiblit le volet proactif de la cybersécurité, notamment en ce qui concerne les risques spécifiques à la fraude bancaire, un manque critique dans un environnement fortement réglementé comme le secteur financier.

De plus, la cartographie des risques liée aux opérations SWIFT n'est pas formalisée ni révisée périodiquement, en dépit de sa faisabilité technique. La mise à jour de cette cartographie, bien qu'essentielle à la conformité avec l'exigence A.6.1.2 de l'ISO 27001, est laissée à la charge des entités métiers telles que la conformité ou la gestion du KYC, alors que la DSSI se concentre exclusivement sur les aspects techniques. Ce manque de coordination interfonctionnelle constitue une faiblesse dans la gouvernance globale du risque, susceptible de nuire à la résilience organisationnelle.

Par ailleurs, l'organisation a démontré une volonté de renforcement continu via plusieurs leviers. Un audit interne du système SWIFT, encadré par la Direction de l'Audit Interne et appuyé par des experts externes en cybersécurité, a permis d'évaluer l'état de conformité avec les normes ISO 27001. En parallèle, un programme de formation agile, combinant théorie et pratique, a été lancé pour accélérer l'adoption du SMSI au sein de l'organisation.

Enfin, la culture de sécurité est également nourrie par des initiatives de sensibilisation, incluant des simulations d'attaques par phishing, des audits sur la robustesse des mots de passe, et des analyses d'indicateurs comportementaux (taux d'activation du MFA, incidents humains, scores de formation, etc.). L'intégration de ces données dans un cycle d'amélioration continue traduit une approche holistique et dynamique de la cybersécurité.

3. Mise en correspondance entre le Customer Security Control Framework CSPSWIFT et ISO 27001

Le tableau ci-dessous présente la correspondance entre les mesures de sécurité SWIFT et le référentiel international ISO/IEC 27001, qui définit les bonnes pratiques en matière de sécurité de l'information. Pour chaque référentiel, nous avons aligné les contrôles SWIFT correspondants, tout en justifiant cette correspondance de manière détaillée. Par la suite, nous intégrerons les exigences complémentaires entre les contrôles de sécurité des prestataires de services SWIFT (CSP) et la norme ISO 27001 :2022, en adaptant les libellés et critères selon les besoins spécifiques, afin d'assurer une cohérence optimale entre les deux cadres normatifs.

N.B : la conformité à ISO/IEC 27001 :2022 n'implique pas automatiquement l'application exhaustive des mesures SWIFT. Certains aspects spécifiques à SWIFT peuvent rester partiellement non couverts. Il revient à l'auditeur de vérifier, pour chaque contrôle, la portée opérationnelle et la rigueur des mécanismes déployés dans l'environnement SWIFT.

Tableau 13 : Mise en correspondance des normes de l'industrie.

CONTROLE CSPSWIFT	Mesure de sécurité	Contrôle iso 27001	Objectif de la mesure SWIFT	Justification la correspondance
CSP-C01 **Limiter l'accès Internet et séparer systèmes critiques l'environnement général**	Segmentation réseau pour isoler les systèmes SWIFT (MT940, MT950) du reste du SI.	**13.1 Gestion de la sécurité des réseaux** **A.13.1.1** Protection des communications	**1.1 Protection de l'environnement SWIFT :** Protéger l'infrastructure SWIFT locale de l'utilisateur contre des éléments potentiellement compromis de l'environnement informatique général et de l'environnement externe.	L'ISO exige la protection des communications via la segmentation réseau ; SWIFT impose l'isolement des systèmes critiques du reste du SI, ce qui répond directement à ce principe.
CSP-C02 **Réduire la surface d'attaque et les vulnérabilités**	Chiffrement AES-256 des messages SWIFT	**12.6.1 Gestion des vulnérabilités techniques**	**1.2 Analyse des vulnérabilités** : Identifiez les vulnérabilités	Le chiffrement des données et l'analyse régulière des vulnérabilités sont des

		A.10.1.1 Chiffrement des données	connues dans l'environnement SWIFT local en mettant en place un processus régulier d'analyse des vulnérabilités et en agissant en fonction des résultats.	piliers partagés par ISO et CSP pour garantir la confidentialité et l'intégrité du système. . L'usage du chiffrement AES-256 pour les bases SWIFT (EBS, RDS Oracle) assurent la confidentialité des données et la correction des vulnérabilités, conformément aux attentes de l'ISO.
CSP-C03 **Sécuriser physiquement l'environnement**	3.1 Restrictions d'accès physique aux serveurs SWIFT	**A.11.1.1 Zones sécurisées** - 11.1.1 : Périmètre de sécurité physique ▪ 11.1.2 : Contrôles physiques des accès ▪ 11.1.4 : Protection contre les menaces extérieures et environnement ales	**1.3 Sécurité physique** Empêcher l'accès physique non autorisé aux équipements sensibles, aux environnements de travail, aux sites d'hébergement et au stockage	ISO impose des contrôles d'accès physiques et une protection contre les menaces ; CSP reprend ces principes pour sécuriser l'environnement SWIFT sur site. AINSI La mise en place de badges d'accès, et l'hébergement dans un datacenter certifié PCI-DSS matérialisent ces exigences.
CSP-C04 **Prévenir les vols d'identifiants**	4.2 Authentification forte (MFA) pour accéder aux systèmes SWIFT	**9.1 Exigences métier en matière de contrôle d'accès** A.9.1.1Gestion des droits d'accès	**1.4 Contrôle d'accès logique** Appliquer les principe de sécurité de l'acce basé sur le besoin d'e connaître, du moind privilège et de séparation des tâch pour les comptes d opérateurs.	La norme requiert des contrôles d'accès adaptés aux besoins métier. L'activation obligatoire du MFA pour tous les accès aux interfaces SWIFT assure une authentification forte conforme aux exigences ISO. L'exigence d'une authentification MFA est une mesure de contrôle

				d'accès logique pleinement alignée avec les principes ISO de gestion rigoureuse des accès.
CSP-C05 **Gérer les identités et séparer les privilèges**	5.1 contrôles d'accès logique 5.2 Gestion des jetons	**9.2 Gestion de l'accès utilisateur** A.9.2.1 Séparation des tâches	**1.5 Contrôle des comptes à privilèges dans le système d'exploitation** : Restreindre et contrôler l'attribution et l'utilisation de comptes d'administrateur dans le système d'exploitation.	Le système impose la séparation des fonctions (approbateur VS initiateur) et gère les comptes à privilèges via des politiques PAM. L'approche est conforme à l'ISO, bien qu'une revue régulière soit à renforcer.
CSP-C06 **Détecter les activités anormales dans les systèmes ou les relevés d'opérations**	6.4 Journalisation et audit des transactions SWIFT	**12.4 Journalisation et surveillance** 12.4.1 : Journalisation des événements A.12.6.1 Surveillance des activités	**1.6 Journalisation et surveillance Enregistrer les événements de sécurité et détecter les actions et opérations anormales dans l'environnement SWIFT local.**	L'ISO comme CSP exigent une séparation claire des rôles et des droits afin de limiter les abus d'accès et renforcer la sécurité opérationnelle.
CSP-C07 **Évaluer les risques et le niveau de préparation de l'organisation sur la base de scénarios de cyberattaques plausibles.**	7.4A Évaluation des risques fondée sur des scénarios	**ISO 27001 articles 6.1 Évaluation des risques liés à la sécurité de l'information** A.6.1.2 Gestion des risques (analyse et traitement)	**1.7 Évaluation des risques fondée sur des scénarios Évaluer les risques et le niveau de préparation de l'organisation sur la base de scénarios de cyberattaques plausibles**.	La mesure **CSP-C07** exige une évaluation des risques fondée sur des scénarios concrets de cyberattaques, ce qui correspond directement au contrôle **A.6.1.2** de l'ISO 27001, qui impose un processus structuré d'analyse, d'évaluation et de documentation des risques liés à la sécurité de l'information. Les deux visent à anticiper les

				menaces et à renforcer la posture de sécurité en intégrant la gestion des risques dans la stratégie globale de l'organisation. ISO 27001 impose une méthode formalisée d'évaluation des risques. CSP-C07 reprend cette exigence à travers la modélisation de scénarios spécifiques à l'environnement SWIFT, comme la compromission de messages (MT103/MT940), pour guider les décisions de sécurité.

Source : élaborer par nous- mêmes.

Les contrôles définis dans le Customer Security Programme (CSP) de SWIFT sont clairement inspirés et alignés avec les exigences de l'Annexe A de la norme ISO/CEI 27001:2022, qui constitue le référentiel international le plus reconnu en matière de sécurité de l'information. L'ISO 27001 fournit un cadre général, normatif et transversal pour la mise en place d'un système de management de la sécurité de l'information (SMSI), tandis que le CSP en constitue une déclinaison sectorielle spécifique au domaine bancaire et aux environnements SWIFT. Cette relation d'inspiration est formellement démontrée dans notre tableau comparatif, où chaque exigence du CSP correspond à un ou plusieurs contrôles explicitement énoncés dans l'Annexe A.

Cette comparaison montre clairement que les exigences du CSP de SWIFT s'appuient directement sur les contrôles de l'Annexe A de la norme ISO 27001, ce qui leur donne une cohérence et une compatibilité évidente avec les standards internationaux en matière de sécurité de l'information. Le tableau présenté dans notre étude le confirme : chaque mesure du CSP correspond à un ou plusieurs contrôles ISO, adaptés au contexte spécifique des systèmes SWIFT utilisés dans le secteur bancaire. Il ne s'agit donc pas de deux référentiels séparés, mais bien d'un lien complémentaire : l'ISO 27001 donne le cadre global et les principes, tandis que le CSP en propose une application concrète, ciblée sur un environnement métier critique. Cette correspondance renforce la solidité de notre analyse, en montrant que suivre les exigences du CSP revient aussi à progresser vers une conformité ISO.

4. Application de la grille d'évaluation

Dans le cadre de notre analyse, l'utilisation du référentiel de maturité SAMI a permis d'évaluer avec précision le niveau de mise en œuvre des exigences de la norme ISO 27001:2022 au sein de la BEA. Cette démarche a offert une vision structurée du degré de conformité observé, tout en mettant en évidence les écarts critiques nécessitant la mise en place d'actions correctives ou préventives, en vue de renforcer la posture globale de sécurité de l'information.

Les résultats de l'application de cette méthode révèlent une maturité variable selon les domaines de contrôle de la norme ISO/CEI 27001 :2022. L'utilisation de l'échelle SAMI, structurée en quatre niveaux qualitatifs, allant de l'absence totale de mise en œuvre à une intégration optimisée et opérationnelle, a permis d'évaluer chaque exigence de manière systématique. Cette évaluation s'est appuyée sur des preuves tangibles, collectées à travers l'analyse documentaire, les observations de terrain et les entretiens menés auprès des parties prenantes internes.

L'exploitation de cette échelle, inspirée des cadres méthodologiques développés par l'ENISA (European Union Agency for Cybersecurity) et des recommandations pratiques de Green et Calder (2022) (Green J. e., 2022), a permis d'assurer une mesure rigoureuse, cohérente et reproductible. Elle offre également un cadre de référence pertinent pour suivre l'évolution des pratiques dans le temps et orienter les priorités d'amélioration.

4.1 Les résultats de la grille d'application appliquent à l'annexe A

Le tableau ci-après présente les résultats issus de l'évaluation par grille appliquée dans le cadre de l'étude menée au sein de BEA DSSI. Cette méthode permet de quantifier le niveau d'application des contrôles de sécurité, selon plusieurs contrôles de la norme ISO/CEI 27001. Les calculs ont été réalisés à partir des formules décrites dans (Watkins, 2019), qui constituent une référence reconnue en gestion des risques et mise en conformité ISO 27001 :

- Moyenne de chaque contrôle = Somme des scores ÷ Nombre de lignes du chapitre
- Pourcentage d'application = (Moyenne × 100) ÷ 3
- Pourcentage total = Moyenne des pourcentages des chapitres évalués
- Écart global = 100 % – Pourcentage total

Tableau 14: Résultats de l'application par contrôle de l'annexe A de la norme ISO 27001:2022

CONTROLE	Nb lignes	Somme scores	Moyenne	% Application	% ECARTS
13.1 Gestion de la sécurité des réseaux	2	6	3	100 %	00%
12.6.1 Gestion des vulnérabilités techniques / A.10.1.1 Chiffrement des données	2	6	3	100%	00%
A.11.1.1 Zones sécurisées (Périmètre de sécurité physique)	2	1	0,50	16.67 %	83.33 %
9.1Exigences métier en matière de contrôle d'accès	2	6	3	100	00%
9.2 Gestion de l'accès utilisateur	2	5	2,5	83.33 %	16.67 %
12.4 Journalisation et surveillance	2	6	3	100 %	00%
6.1Évaluation des risques liés à la sécurité de l'information	1	0	0	0%	100%

Source : élaboré par nous-mêmes.

Pourcentage total d'application :(100+100+16.67+100+83.33+100+0) / 7 = 71.43%

Écart de conformité :100%−71.43%=28.57%

Ce tableau présente les résultats d'une évaluation par grille des pratiques de sécurité appliquées dans un cadre bancaire, offrant une vue d'ensemble des domaines de conformité et des points faibles en matière de gestion de la sécurité de l'information. L'analyse des résultats révèle des succès notables dans plusieurs domaines essentiels, mais également des lacunes importantes, qui nécessitent des actions correctives immédiates.

Les contrôles 13.1 "Gestion de la sécurité des réseaux", A.10.1.1 "Chiffrement des données", 9.1 "Exigences métier en matière de contrôle d'accès", et 12.4 "Journalisation et surveillance" Affichent tous une conformité optimale de 6 sur 6, avec 100 % d'application. Cela indique une implémentation efficace et conforme des mesures de sécurité recommandées, essentielles pour assurer la sécurité des réseaux, la protection des données, le chapitre d'accès et la surveillance des systèmes. Ces résultats suggèrent que ces domaines sont bien maîtrisés et conformes aux attentes de sécurité.

Cependant, des écarts significatifs apparaissent dans le chapitre A.11.1.1 "Zones sécurisées (Périmètre de sécurité physique)", où le score est très faible, à 0,50 sur 3, avec seulement 16,67 % d'application. Cela met en évidence une vulnérabilité dans la gestion de la sécurité physique, un domaine crucial pour la protection des infrastructures sensibles. De même, le contrôle 9.2 "Gestion de l'accès utilisateur" présente un score de 2,5 sur 3 (83,33 % d'application), ce qui montre qu'il existe encore des améliorations possibles dans la gestion des accès.

Enfin, "Aucun niveau de conformité n'a été constaté pour le chapitre 6.1, portant sur l'évaluation des risques liés à la sécurité de l'information, qui affiche un score nul (0/3) et une application évaluée à 0 %, ce qui souligne un déficit important dans la prise en charge des risques liés à la sécurité de l'information. Ce domaine nécessite une attention particulière, car l'évaluation des risques est essentielle pour une gestion proactive de la sécurité.

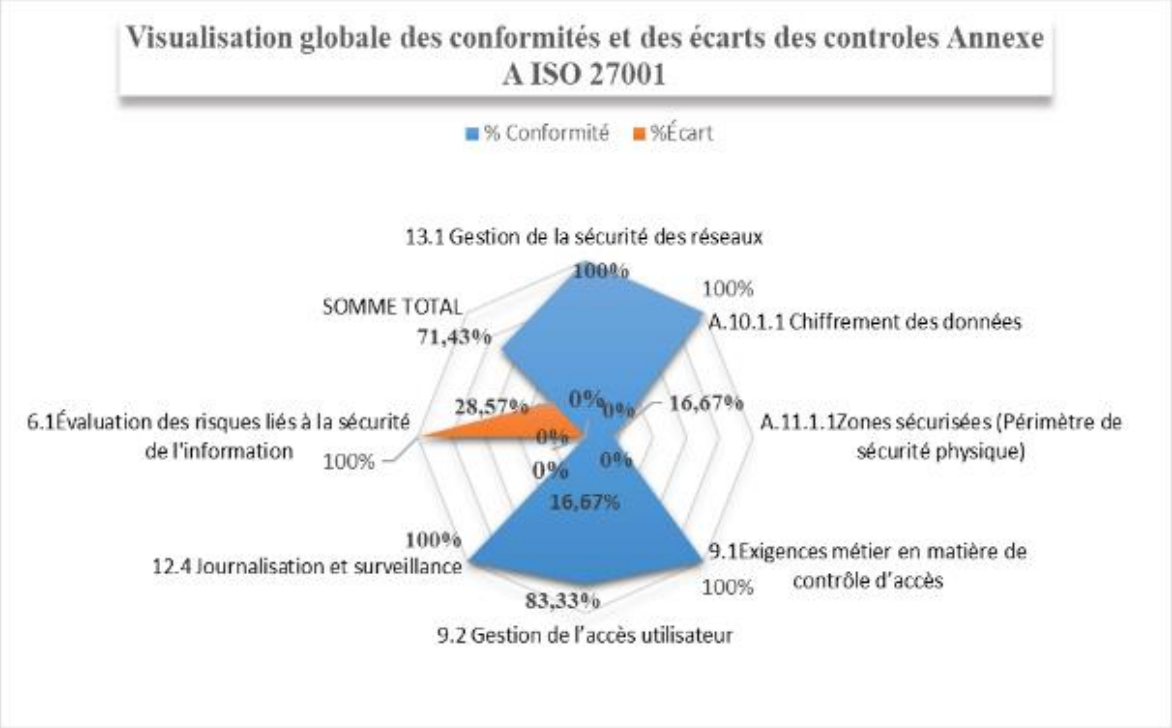
En résumé, bien que la majorité des pratiques soient correctement mises en œuvre, l'évaluation met en lumière des domaines clés où des améliorations urgentes sont nécessaires, notamment en ce qui concerne la sécurité physique et l'évaluation des risques.

4.2 Représentation graphique des résultats et diagnostic

Dans le cadre de cette étude menée au sein de la BEA DSSI selon les exigences de la norme ISO/IEC 27001, les données issues de la grille d'évaluation ont été représentées graphiquement à l'aide d'un diagramme radar. Le diagramme radar a été retenu pour sa

capacité à mettre en évidence, en un seul visuel, les zones de conformité élevée et les points de vulnérabilité. Il facilite ainsi l'analyse des écarts, la priorisation des actions correctives et la communication claire des résultats aux parties prenantes techniques et décisionnelles. Ce type de représentation est particulièrement adapté dans une démarche d'amélioration continue de la sécurité de l'information, en cohérence avec les principes de la norme ISO 27001.

Figure 7 :Rader des contrôles techniques (Annexe A_ISO/IEC27001)



Source : élaboré par nous-mêmes.

L'analyse radar révèle un niveau de conformité global de 71,43 % du système SWIFT de la BEA par rapport aux exigences de la norme ISO 27001:2022. Ce résultat montre que la majorité des contrôles techniques exigés par l'annexe A sont bien appliqués, notamment ceux relatifs à la sécurité des réseaux, au chiffrement, à la journalisation et au contrôle d'accès, qui présentent des scores maximaux. Toutefois, à travers l'analyse des données issues de la grille d'évaluation et des entretiens menés avec les responsables de la sécurité, nous avons constaté des insuffisances importantes. D'une part, la sécurité physique présente un faible taux de conformité (16,67 %), ce qui dénote une protection encore insuffisante des infrastructures critiques. D'autre part, aucune démarche formelle d'évaluation des risques n'a été observée, ce qui se traduit par un score de conformité de 0 %, indiquant une non-conformité totale sur ce point. Cette absence constitue une faille critique, dans la mesure où aucun processus structuré de gestion des risques n'est formalisé

à ce jour. En somme, l'absence d'une gouvernance complète autour de ces volets essentiels empêche l'atteinte d'une conformité totale et met en évidence la nécessité de renforcer les pratiques de pilotage du SMSI conformément aux exigences de l'ISO 27001.

4.3 Analyse des écarts des contrôles de l'annexe A de la norme ISO 27001 : 2022

Tableau 15 : Analyse des écarts des contrôles de l'annexe A de la norme ISO 27001 :2022

CHAPITRE Contrôle iso 27001	SCORE	Niveau de conformité	Écart identifié	Justification
13.1 Gestion de la sécurité des réseaux	3	CONFORME	AUCUN.	Segmentation réseau (VLAN, NACLs), Gateway dédiée, hébergement local validé et garantit l'isolation des flux sensibles, ce qui répond à l'exigence ISO en matière de protection des communications et limite les vecteurs d'attaque réseau.
12.6.1 Gestion des vulnérabilités techniques	3	CONFORME	AUCUN	Patching offline maîtrisé, via AWS Systems Manager, hébergement on-premise conforme
A.10.1.1 Chiffrement des données	3		AUCUN	Chiffrement AES-256, gestion interne des clés, environnement SWIFT localisé et sécurisé
11.1.1 : Périmètre de sécurité physique	1	Partiellement conforme	Serveurs SWIFT non isolés physiquement	Coexistence avec autres serveurs, sécurité physique logique mais non dédiée
11.1.2 : Contrôles physiques des accès	0	Non conforme	Absence de rapports SOC ou preuves d'audits	Aucune documentation annuelle validée disponible

9.1Exigences métier en matière de contrôle d'accès	3	CONFORME	AUCUN	MFA et PAM déployés, journaux actifs, coordination RSSI/Admin conforme aux exigences ISO. L'exigence d'une authentification MFA est une mesure de contrôle d'accès
9.2 Gestion de l'accès utilisateur	2	Partiellement conforme	Révision semestrielle et matrice incomplète	Fréquence non conforme, documentation incomplète
A.9.2.1 Séparation des tâches	3	CONFORME	AUCUN	Désactivation automatique des comptes inactifs avant 90 jours
12.4 Journalisation et surveillance	3	CONFORME	AUCUN	Centralisation des logs dans PAM, alertes en place, coordination DSI/RSSI
A.6.1.2 Gestion des risques (analyse et traitement)	0	NON CONFORMITE	Absence de mise en œuvre opérationnelle des scénarios MEHARI	Démarche théorique sans mise en œuvre pratique, aucun test effectué gestion des risques dans la stratégie globale de l'organisation. Aussi il faut dire que Les journaux d'événements (VPC Flow Logs, RDS, MQ) sont centralisés et analysés via des outils comme PAM. Bien que conforme, cette politique de surveillance reste spécifique à SWIFT et devrait être intégrée dans une politique globale pour répondre pleinement à l'ISO

Source : élaboré par nous-mêmes.

- **Evaluation relative au contrôle 13.1 Gestion de la sécurité des réseaux**

L'évaluation du chapitre 13.1 met en évidence un niveau de conformité élevé aux exigences de l'ISO/CEI 27001, en particulier sur le contrôle A.13.1.1 relatif à la protection des communications. Deux éléments principaux ont été analysés : la segmentation réseau et l'isolement des environnements SWIFT.

Premièrement, la BEA a mis en œuvre une segmentation stricte du réseau entre les environnements sensibles liés à SWIFT (notamment les messages MT940, MT950) et le reste du système d'information. Cette séparation est assurée par l'utilisation de VLAN dédiés, de Security Groups, ainsi que de Network Access Control Lists (NACLs). Cette architecture segmentée vise à limiter les surfaces d'attaque potentielles et à restreindre les flux réseau aux seuls canaux nécessaires, conformément aux bonnes pratiques de cloisonnement des systèmes critiques. Le Responsable de la Sécurité des Systèmes d'Information (RSSI) a fourni un diagramme de VLAN à l'appui, attestant de la mise en œuvre effective de cette stratégie.

Deuxièmement, les systèmes SWIFT sont également hébergés dans une infrastructure "on-premise" locale, ce qui correspond à la solution SWIFT C déployée en Algérie. Cette architecture implique que les données et les communications sensibles restent dans un périmètre géographique et organisationnel contrôlé, renforçant ainsi la souveraineté, la confidentialité et la maîtrise des flux. Une Gateway dédiée assure la gestion spécifique des échanges liés à SWIFT, renforçant l'isolation logique des flux critiques.

Il est important de souligner que le contrôle A.13.1.1 est classé parmi les exigences obligatoires dans le contexte des services financiers utilisant SWIFT. Son respect est impératif pour répondre aux exigences de conformité imposées par SWIFT Customer Security Programme (CSP) et par les normes ISO. En ce sens, l'attribution de la note maximale (3/3) est pleinement justifiée, car elle reflète non seulement la conformité aux normes, mais aussi le respect d'un standard de sécurité incontournable pour le secteur bancaire.

- **Evaluation relative au Contrôle 12.6.1 Gestion des vulnérabilités techniques**

L'analyse de ce contrôle révèle une conformité totale avec les bonnes pratiques de gestion des vulnérabilités. Donc La BEA démontre une conformité complète à ce contrôle, avec un processus rigoureux et adapté à son contexte souverain. Les instances EC2 utilisées dans l'environnement SWIFT sont hébergées localement (on-premise), conformément à l'acquisition complète de la solution SWIFT C par la banque. Cette infrastructure est isolée d'Internet, comme l'exige la réglementation algérienne, ce qui interdit toute mise à jour en ligne pour les systèmes traitant des données critiques.

Ainsi, la gestion des vulnérabilités s'effectue via un mécanisme offline à l'aide d'AWS Systems Manager Patch Manager, mais dans un mode strictement déconnecté. La banque

télécharge les correctifs officiels directement depuis le site du fournisseur, en utilisant ses propres comptes d'administration officiels, ce qui garantit l'authenticité des sources et le contrôle exclusif du processus.

Les correctifs sont ensuite installés manuellement par des équipes techniques internes, sans aucune externalisation de l'intervention. Cette approche est explicitement mentionnée dans le contrat avec SWIFT, en tant qu'exigence liée à l'hébergement local et à la non-externalisation de l'accès aux systèmes critiques.

L'objectif est clair : éviter toute exposition ou interférence externe, conformément aux principes de sécurité nationale et aux obligations de confidentialité imposées par la réglementation algérienne sur la protection des données financières. Ce modèle d'exploitation assure également la traçabilité et la responsabilité complète de la banque sur la maintenance de ses environnements sensibles.

La note maximale (3/3) est donc pleinement justifiée : la banque prouve qu'elle applique un modèle de gestion des vulnérabilités contrôlé, conforme aux standards SWIFT CSCF et adapté à un contexte souverain.

- **Evaluation relative au chapitre A.10.1.1 – Chiffrement des données**

L'analyse du contrôle A.10.1.1 met en évidence un niveau de conformité optimal en matière de sécurité cryptographique, traduisant l'engagement de la BEA à garantir la confidentialité des données sensibles liées aux opérations SWIFT, tout en assurant un alignement strict avec les exigences de l'ISO/CEI 27001 et les standards du CSCF de SWIFT.

Ce contrôle vise à assurer la confidentialité absolue des données sensibles, notamment les données client et les transactions financières traitées via SWIFT. La BEA a mis en œuvre un chiffrement AES-256 bits, reconnu pour sa robustesse au niveau international, sur l'ensemble de ses bases de données critiques : Elastic Block Store (EBS) et Oracle RDS.

Les clés de chiffrement sont créées, détenues et gérées exclusivement par la banque, sans dépendance à un fournisseur de cloud ou à un prestataire externe. Cela garantit que ni la génération, ni l'accès aux clés cryptographiques ne sont exposés à des tiers. Ce mécanisme est un pilier de la stratégie de souveraineté numérique de l'institution.

L'environnement SWIFT étant localement hébergé, toutes les transactions sont traitées à l'intérieur de l'infrastructure de la banque, sans transfert des données à l'extérieur du

territoire national. Les preuves de conformité (PoCs) ont été documentées et validées selon le référentiel CSCF SWIFT, démontrant ainsi l'application effective du contrôle.

De plus, les données client transitent via une plateforme sécurisée appelée "DELTA", ce qui ajoute un niveau supplémentaire de protection dans le processus de communication financière. Ce dispositif contribue non seulement à la confidentialité, mais aussi à l'intégrité et à la non-répudiation des échanges.

Là encore, la note de 3/3 est entièrement méritée. Elle reflète la capacité de la banque à intégrer les exigences de chiffrement dans un cadre d'hébergement local, sécurisé, maîtrisé et conforme aux standards internationaux.

- **Evaluation relative au chapitre A.11.1.1 Zones sécurisées**

L'évaluation du contrôle A.11.1.1 met en lumière une non-conformité partielle concernant la mise en œuvre des exigences de l'ISO/CEI 27001 relatives à la sécurisation physique des environnements sensibles, notamment les infrastructures hébergeant les serveurs SWIFT. Bien que certaines mesures soient en place, les preuves fournies restent insuffisantes pour conclure à une conformité totale.

Les serveurs SWIFT sont effectivement hébergés dans des data centers privés, sous la responsabilité directe de la BEA, et certifiés PCI-DSS, ce qui constitue un point positif en matière de conformité aux standards de sécurité physiques et environnementaux. L'accès est contrôlé via un système de badge nominatif, comme en atteste la liste d'accès aux salles serveurs, validée par le responsable des data centers. Cela justifie une note partielle de 1 sur 3, témoignant d'un effort réel mais incomplet.

Cependant, cette conformité est limitée au niveau logique, car les serveurs SWIFT ne sont pas isolés physiquement dans un espace dédié. En effet, dans l'architecture actuelle, les équipements SWIFT coexistent dans un même espace que d'autres serveurs, ce qui dilue le niveau de compartimentation exigé par la norme. En clair, toute personne disposant d'un accès autorisé au data center peut, potentiellement, atteindre les serveurs SWIFT, ce qui constitue une faiblesse structurelle., ce qui constitue une faiblesse structurelle.

En parallèle, les exigences des contrôles 11.1.2 (contrôles physiques d'accès) et 11.1.4 (protection contre les menaces extérieures et environnementales) ne sont pas suffisamment documentées. L'absence de rapports SOC annuels validés sur la sécurité physique, ainsi que le manque de preuves d'audits réguliers, empêchent de valider la conformité à ces

exigences. La non-conformité est justifiée par l'absence de preuves formelles., malgré les efforts apparents.

On peut conclure que Le périmètre de sécurité physique autour des systèmes SWIFT montre une volonté de conformité, mais reste insuffisant sur deux plans majeurs : L'absence d'isolation physique stricte du périmètre SWIFT dans le data center. Et Le manque de preuves formelles (rapports, audits, validations) concernant la sécurité physique et environnementale.
La notation attribuée (1/3 et 0/3) reflète donc de façon cohérente les écarts observés, et souligne la nécessité de renforcer les dispositifs de contrôle d'accès physique, ainsi que la documentation de conformité.

- **Evaluation relative au chapitre 9.1 Exigences métier en matière de contrôle d'accès**

L'évaluation du contrôle 9.1 révèle un niveau de conformité maximal (score 3/3), soulignant la mise en œuvre rigoureuse et obligatoire des exigences relatives à la gestion des accès, telles que définies dans la norme ISO/IEC 27001 et imposées dans le cadre du CSP SWIFT. Ce score reflète une application complète et structurée des mesures de sécurité liées à l'authentification des utilisateurs.

Plus précisément, la mise en place systématique de l'authentification multifacteur (MFA) pour tous les accès au système SWIFT constitue un pilier fondamental de la stratégie de protection contre les accès non autorisés. Cette exigence est appuyée par une politique MFA officielle, accompagnée de mécanismes de journalisation des authentifications, permettant une surveillance continue. Le RSSI veille à la conformité globale de cette politique, tandis que l'administrateur SWIFT assure sa mise en œuvre technique, notamment à travers le contrôle des accès privilégiés via des solutions PAM (Privileged Access Management). En complément, des notifications téléphoniques (par SMS ou appel vocal) sont utilisées comme second facteur, garantissant une authentification forte et un renforcement de la sécurité opérationnelle. Cette approche assure non seulement que seuls les utilisateurs autorisés accèdent aux systèmes critiques, mais permet également une traçabilité exhaustive et une détection rapide des comportements anormaux.

Ainsi, la note maximale attribuée (3/3) est justifiée, car elle correspond à une exigence obligatoire, intégrée de manière complète et conforme aux meilleures pratiques en matière de sécurité des accès dans le secteur bancaire.

- **Evaluation relative au chapitre 9.2 Gestion de l'accès utilisateur**

Le contrôle lié à la gestion des accès utilisateurs, conformément à l'article 9.2, présente des niveaux de conformité différenciés qui traduisent à la fois des efforts louables et des marges d'amélioration. En effet, la révision des droits d'accès SWIFT, notée 2, est partiellement conforme puisqu'elle repose sur une révision semestrielle, alors qu'un contrôle trimestriel est requis, et se heurte à une matrice des privilèges incomplète, exposant ainsi l'organisation au risque de maintenir des droits obsolètes ou inadaptés. Par contraste, l'attribution de privilèges limités pour les comptes à accès élevé (Admin/DBA), évaluée en A.9.2.3 et notée 3, témoigne d'une conformité totale grâce à la désactivation automatique des comptes inactifs avant 90 jours, conformément à la politique de sécurité SWIFT. L'engagement conjoint de la DSI et du RSSI dans ces procédures illustre une gouvernance structurée des accès sensibles, même si une amélioration de la documentation et une révision plus fréquente des privilèges s'imposent pour renforcer davantage la sécurité globale.

La gestion des comptes à privilèges est bien maîtrisée (score 3), mais la revue des droits d'accès reste incomplète et trop intermittente (score 2). Une amélioration de la fréquence et de la documentation est nécessaire pour une conformité totale.

- **Evaluation relative au chapitre 12.4 Journalisation et surveillance**

Le niveau de conformité observé pour le contrôle 12.4 relatif à la journalisation et à la surveillance des transactions SWIFT témoigne d'un dispositif de sécurité mature et pleinement opérationnel, avec une intégration cohérente entre détection, réaction et traçabilité, justifiant l'attribution d'un score de 3 sur l'ensemble des exigences évaluées. En premier lieu, les logs issus des composants critiques de l'écosystème SWIFT (VPC Flow Logs, RDS, MQ) sont entièrement centralisés dans un système de type PAM, permettant une supervision transversale et en temps réel. Ce système de monitoring assure non seulement la collecte continue, mais aussi l'analyse automatisée des événements, garantissant une détection rapide des comportements anormaux. À ce titre, les mécanismes d'alerte sont configurés pour signaler toute tentative de connexion échouée au-delà d'un seuil défini (plus de trois essais), conformément aux exigences de l'article A.12.4.1, renforçant ainsi la capacité de réponse en cas d'activité suspecte. Sur le plan organisationnel, le RSSI supervise le contrôle des journaux et des alertes, assurant une veille active sur les incidents de sécurité, tandis que la DSI agit en tant que levier

opérationnel, procédant à la désactivation des comptes inactifs avant les 90 jours réglementaires, en conformité avec les exigences de l'article A.12.6.1. Le système PAM complète ce dispositif en fournissant une traçabilité exhaustive des actions, indispensable pour les audits, la rétro-analyse post-incident et la preuve de conformité. Cette articulation fluide entre les outils techniques et la gouvernance des accès illustre un haut degré de maturité dans la gestion de la cybersécurité, consolidant pleinement la justification d'un score maximal.

Le score de 3 reflète une conformité totale, car toutes les exigences de journalisation, de surveillance active et de désactivation automatique des comptes inactifs sont pleinement appliquées. De plus, une coordination efficace entre les fonctions RSSI et DSI, soutenue par des outils adaptés comme le PAM, garantit une détection et un audit robustes des activités suspectes.

- **Evaluation relative au chapitre 6.1 Évaluation des risques liés à la sécurité de l'information**

Le contrôle relatif à l'évaluation des risques de sécurité de l'information, en particulier l'analyse des risques fondée sur des scénarios, montre un écart significatif dans l'application des bonnes pratiques. Bien que des scénarios de fraude SWIFT, comme l'altération de MT103, aient été modélisés théoriquement à travers la méthode MEHARI, leur mise en œuvre reste inexistante dans la pratique. Cette absence d'application des scénarios témoigne d'une lacune dans le processus de gestion des risques, où, malgré l'existence d'une méthodologie appropriée, aucune simulation ou évaluation concrète des risques n'a été effectuée. Bien que la méthode MEHARI ait été choisie par le BEA pour l'analyse des risques, cette démarche n'a pas été formalisée dans les scénarios réels de fraude. Dans un cadre de conformité, le rôle de la conformité et de la DRS (Direction des Risques et de la Sécurité) serait de prendre en charge ces scénarios, en coordination avec la fonction KYC (Know Your Customer) pour les aspects métier, tandis que la DSI (Direction des Systèmes d'Information) assurerait le côté technique de la simulation, notamment sur l'aspect de l'intégrité des transactions. Le score de 0 attribué à ce contrôle reflète donc l'absence de toute mise en œuvre pratique des scénarios, malgré leur définition théorique, soulignant ainsi une non-conformité totale dans ce domaine spécifique de la gestion des risques.

Le score de 0 est attribué en raison de la non-application effective des scénarios de fraude SWIFT, bien que la méthode MEHARI ait été choisie et que la répartition des rôles entre les différentes fonctions de l'organisation soit clairement définie. L'absence d'implémentation de ces scénarios constitue un manquement majeur à l'évaluation proactive des risques de fraude.

4.4.Plan d'action de mise en conformité des contrôles Annexe A ISO27001

Dans cette section, nous présentons les plans d'action visant à corriger les écarts constatés entre les pratiques actuelles de sécurité de l'information de la BEA – DSSI et les exigences de la norme ISO/IEC 27001:2022. Les recommandations sont structurées par chapitre de la norme et organisées sous forme de tableaux synthétiques, afin de faciliter le suivi, la mise en œuvre et l'évaluation de chaque action corrective.

Tableau 16 : Plan d'action de mise en conformité des contrôles Annexe A ISO 27001

Contrôle ISO	Écart identifié	Action corrective	Responsable	Délai estimé	PRIORITE
A.11.1.1	Serveurs SWIFT non isolés physiquement	Créer une zone physique dédiée pour les serveurs SWIFT dans les data centers	Responsable data centers / RSSI	3 mois	HAUTE
A.11.1.2 / A.11.1.4	Absence de rapports SOC ou preuves d'audits	Mettre en place un audit annuel de la sécurité physique et produire un rapport SOC validé	Responsable data centers / Conformité	2 mois	HAUTE
A.9.2	Révision semestrielle, matrice incomplète	Passer à une révision trimestrielle + compléter la matrice des privilèges	RSSI / DSI	1 mois	MOYENNE
A.6.1.2	Absence de mise en œuvre opérationnelle des scénarios MEHARI	Formaliser et exécuter des scénarios de fraude SWIFT (MT103) avec KYC, DRS, conformité	Conformité / DRS / RSSI / DSI	3 mois	HAUTE

Source : élaboré par nous-mêmes.

L'examen détaillé du plan d'action mis en place dans le cadre du processus de certification ISO/CEI 27001 à la BEA – DSSI révèle des écarts significatifs, imputables à des causes organisationnelles et structurelles clairement identifiées. Tout d'abord, il est essentiel de considérer que la BEA est en phase de transition vers la certification, ce qui implique une montée en maturité progressive du système de management de la sécurité de l'information (SMSI). À cela s'ajoute un facteur clé : la séparation de la DSSI et de la DSI opérée il y a deux ans, qui a profondément modifié la gouvernance des systèmes d'information. Cette réorganisation a eu pour effet immédiat une redéfinition des responsabilités, parfois encore floue, et un manque de coordination

transversale, notamment sur les sujets partagés comme les accès, l'analyse des risques, ou la sécurité physique. L'écart lié à l'absence d'isolement physique des serveurs SWIFT (A.11.1.1) traduit une gestion historique intégrée de l'infrastructure, sans segmentation claire des environnements critiques, une inertie compréhensible dans un contexte de transition. L'absence de rapports SOC ou d'audits formels (A.11.1.2 / A.11.1.4) découle d'un déficit de formalisation documentaire, renforcé par la séparation DSI/DSSI qui a laissé certains périmètres de contrôle sans pilote identifié. Concernant le contrôle des accès (A.9.2), la révision semestrielle et la matrice incomplète s'expliquent par une coordination insuffisante entre la DSI, détentrice des systèmes, et la DSSI, garante de la sécurité, dans un contexte où les processus ne sont pas encore totalement automatisés ni gouvernés par des outils partagés. Enfin, l'absence de scénarios MEHARI appliqués (A.6.1.2) illustre une maturité encore théorique dans l'approche risque, où la méthode est choisie mais reste cantonnée à l'intention, faute d'une animation interfonctionnelle (conformité, DRS, métier, RSSI) suffisamment active. Cela dit, les actions proposées sont pertinentes, ciblées et techniquement réalistes. Elles doivent cependant être accompagnées d'un cadre de gouvernance renforcé : définition claire des rôles, formalisation systématique des preuves, tenue de comités sécurité interservices, et suivi régulier des plans de remédiation. Ce n'est qu'en combinant l'exécution rigoureuse de ces actions à une consolidation de la gouvernance que la BEA pourra non seulement combler les écarts actuels, mais surtout construire un SMSI pérenne, certifiable et aligné aux meilleures pratiques internationales.

- Pour corriger les écarts identifiés et renforcer durablement la posture de sécurité de l'information de la BEA, un ensemble de recommandations ciblées et stratégiquement alignées sur les exigences de la norme ISO/IEC 27001:2022 est proposé. Concernant d'abord l'isolement physique des serveurs SWIFT (contrôle A.11.1.1), il est essentiel de :
  - Définir un périmètre strictement dédié dans les data centers
  - Définir une zone physique strictement dédiée aux équipements SWIFT dans les data centers.
  - Mettre en place un contrôle d'accès physique renforcé (badges spécifiques, lecteurs biométriques) pour limiter l'accès à cette zone.
  - Tenir un registre d'accès physique horodaté, permettant une traçabilité complète des entrées et sorties.
  - Mettre à jour la politique de sécurité physique pour y intégrer la notion de compartimentation stricte des systèmes critiques.

En parallèle, pour répondre au score nul attribué aux contrôles A.11.1.2 et A.11.1.4 liés à l'absence d'audit et de preuves formelles, il est recommandé de :

- Mettre en place un audit annuel de sécurité physique, incluant les paramètres environnementaux (température, incendie, humidité, alimentation, etc.).
- Produire un rapport d'audit structuré (type SOC 2 ou rapport interne) validé conjointement par la DSI et la fonction conformité.
- Archiver ces rapports dans le système de gestion documentaire de sécurité, afin d'assurer leur disponibilité pour les audits internes et externes.

En ce qui concerne le contrôle des accès utilisateurs (A.9.2), la révision semestrielle et la matrice incomplète doivent être corrigées par la mise en place d'un processus de revue trimestrielle automatisée, avec alertes en cas d'écarts ou d'anomalies.

- Compléter et maintenir une matrice des privilèges à jour, incluant les rôles, les systèmes et les niveaux d'habilitation associés.
- Impliquer systématiquement les responsables métiers dans la validation des droits, afin d'assurer la pertinence et la légitimité des accès accordés.

Enfin, pour répondre à la non-application des scénarios de risques SWIFT (contrôle A.6.1.2), il est recommandé :

- Lancer un atelier interservices (RSSI, DSI, conformité, DRS, KYC) pour identifier et formaliser des scénarios de fraude SWIFT réalistes (ex : altération MT103).
- Appliquer la méthode MEHARI pour modéliser chaque scénario, en estimant les impacts potentiels et les probabilités d'occurrence.
- Documenter chaque scénario sous forme de fiche de risque, à intégrer dans le registre des risques ISO 27001.
- Planifier des exercices réguliers de simulation (tests de réponse aux incidents) pour évaluer la capacité de réaction de l'organisation face aux risques modélisés.

5. Choix des Exigences et Définition du Périmètre d'Évaluation dans le Contexte de l'ISO/IEC 27001

Dans le cadre de cette évaluation, nous avons choisi de nous concentrer sur les exigences des chapitres 4, 5, 7, 9 et 10 de la norme ISO/IEC 27001:2022, en excluant volontairement les chapitres 6 (planification) et 8 (fonctionnement). Ce choix s'explique d'abord par une volonté d'éviter la redondance analytique. En effet, l'exclusion des chapitres 6 et 8 est justifiée par la forte interdépendance entre ces exigences et les contrôles de l'annexe A, déjà évalués en détail. Les exigences relatives à l'analyse des risques, à la planification des

actions (6.1), ou encore à la mise en œuvre des mesures de sécurité (8.1 à 8.3), sont concrètement couvertes par des contrôles tels que A.6.1 (Évaluation des risques liés à la sécurité de l'information), A.9.1 (Exigences métier en matière de contrôle d'accès), A.12.4 (Journalisation et surveillance) ou encore A.10.1.1 (Chiffrement des données). Réévaluer ces exigences reviendrait à dupliquer inutilement les résultats, au risque de diluer la lisibilité des écarts identifiés. Par ailleurs, il est important de souligner que la Banque Extérieure d'Algérie ne dispose pas, à ce jour, d'un SMSI structuré et certifié ; dès lors, l'objectif de cette démarche n'est pas de vérifier une conformité stricte, mais d'apprécier, dans un cadre pragmatique, dans quelle mesure les bonnes pratiques de sécurité de l'information recommandées par l'ISO 27001 sont effectivement appliquées au sein du périmètre technique ciblé, à savoir le système SWIFT tel qu'opéré et encadré par la Direction de la Sécurité des Systèmes d'Information (DSSI). Ce périmètre restreint, mais stratégique, permet d'obtenir une vision réaliste et exploitable du niveau de maturité atteint, sans prétendre auditer l'ensemble de la banque, ce qui serait à la fois disproportionné et méthodologiquement inadapté. Enfin, les exigences retenues, relatives au contexte organisationnel, au leadership, au support, à l'évaluation des performances et à l'amélioration continue, s'inscrivent pleinement dans les responsabilités de la DSSI et permettent de mesurer sa capacité à s'aligner progressivement sur les fondements d'un SMSI cohérent, sans réitérer inutilement les analyses déjà menées via l'annexe A.

5.1 Diagnostic des écarts organisationnels par rapport aux exigences ISO/IEC 27001 :2022 ciblant le dispositif SWIFT

Tableau 17 : Analyse des écarts organisationnels de la DSI par rapport aux exigences de la norme ISO 27001 :2022, dans le cadre du système SWIFT

CONTROLE	Nb lignes	Somme scores	Moyenne	% Application	% ECARTS
4.1 Compréhension du contexte de l'organisation	2	3	1,50	50%	50%
4.2 Compréhension des besoins et attentes des parties intéressées	2	6	3	100%	0%
4.3 Détermination du périmètre du système de management de la sécurité de l'information (SMSI)	1	0	0	0 %	100%
5.1 Engagement de la direction	1	3	3	100%	0%

5.2 Politique de sécurité	2	4	2	66,67%	33,33%
5.3 Rôles et responsabilités	1	3	3	100%	00,00%
7.1 Ressource	1	2	2	66,67%	33,33%
7.2 Compétence	1	2	2	66,67%	33,33%
7.3 Sensibilisation	1	0	0	0%	100%
9.3 Audit interne	1	3	3	100%	0%
9.4 Revue de direction	1	3	3	100%	0%
10.1Amélioration continue	1	0	0	0%	100%
10.2 Non-conformité et action corrective	2	4	2	66,67%	33,33%
SOMME TOTALE	___	___	___	67.31%	35.66%

Source : élaboré par nous-mêmes.

Conformité Totale = 875.01%13=67.31%

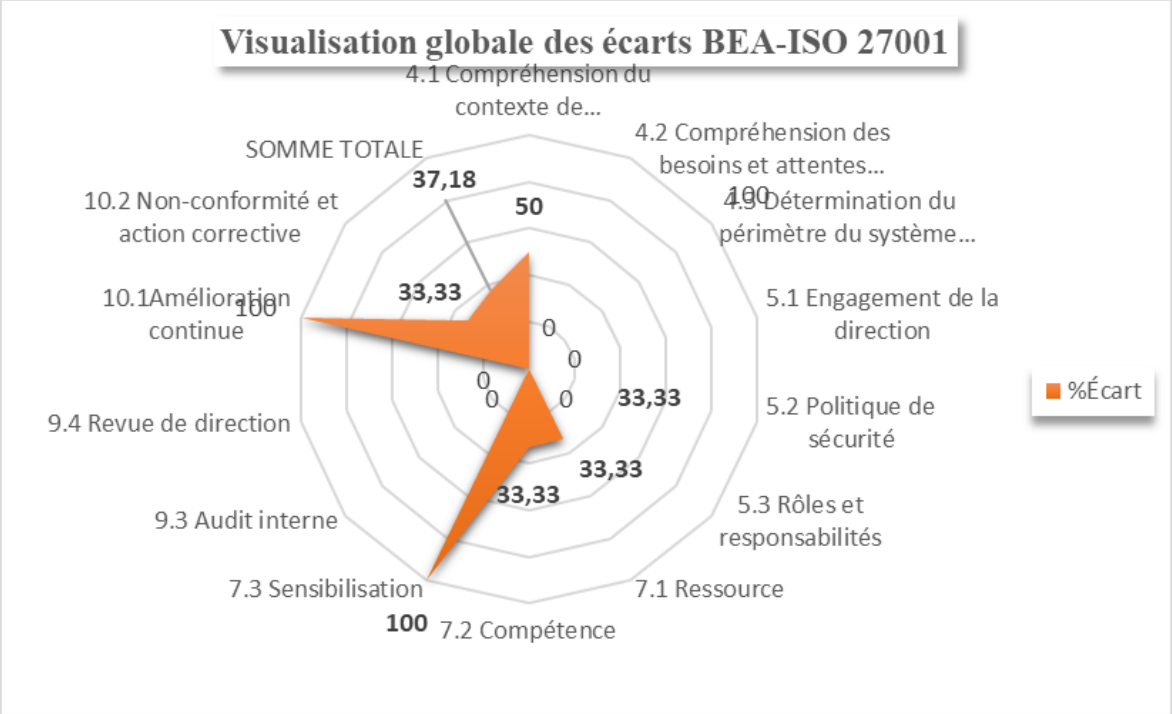
Écarts totaux =100%−67.31%=32.69%

L'analyse du tableau de conformité met en évidence des écarts notables dans la mise en œuvre des exigences de la norme ISO 27001 :2022, appliquées au périmètre du système SWIFT. Certains chapitres clés sont pleinement appliqués, tels que la compréhension des besoins des parties intéressées (4.2), l'engagement de la direction (5.1), la définition des rôles (5.3), l'audit interne (9.3) et la revue de direction (9.4), tous affichant un taux d'application de 100 %. En revanche, des faiblesses marquées apparaissent sur des points critiques comme la détermination du périmètre du SMSI (4.3), la sensibilisation du personnel (7.3) et l'amélioration continue (10.1). Chacun de ces éléments présente un taux d'application nul (0 %), indiquant ainsi une non-conformité totale de ces mesures. et donc

un écart de 100 %. Des chapitres comme la politique de sécurité (5.2), la gestion des ressources (7.1), les compétences (7.2) ou encore la gestion des non-conformités (10.2) présentent un niveau d'application intermédiaire (66,67 %) laissant entrevoir des pratiques partiellement formalisées. Globalement, avec un taux moyen d'application de 67,31 % et un écart moyen de 35,66 %, cette analyse met en évidence une conformité partielle, nécessitant des efforts ciblés sur la structuration du périmètre, la montée en compétence des ressources humaines et l'adoption d'une démarche d'amélioration continue afin de renforcer l'efficacité et la pérennité du SMSI.

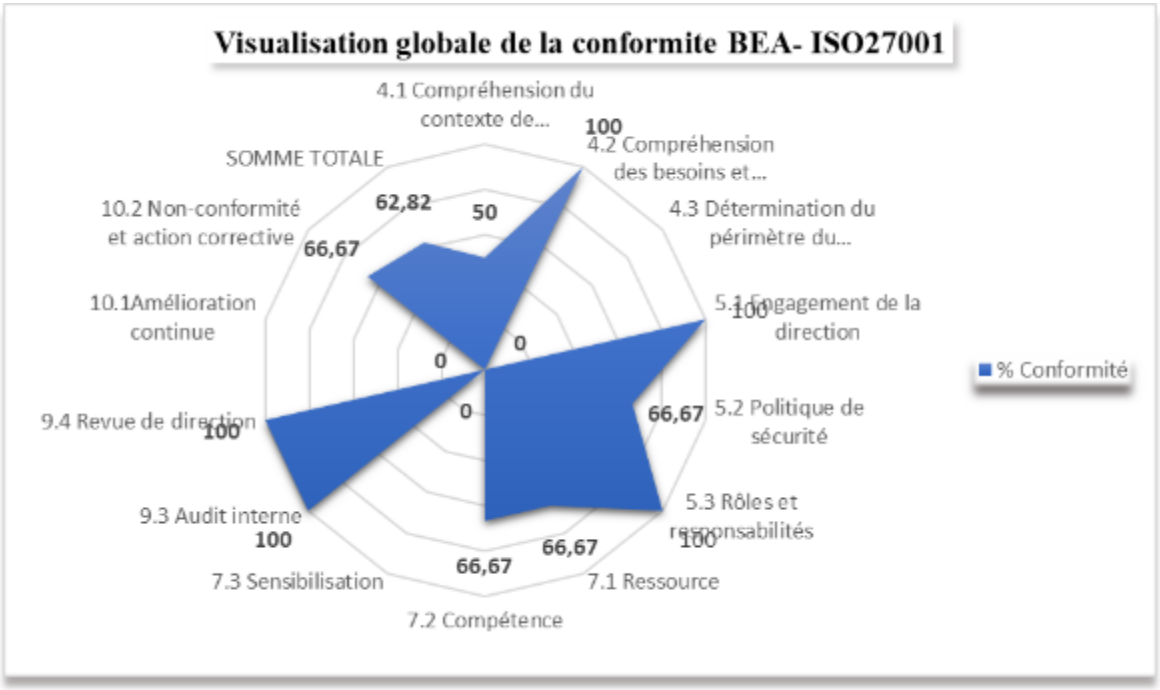
5.2 Représentation graphique des résultats et diagnostic

Figure 8 Rader des écarts organisationnels identifiés dans le système SWIFT (chapitre clés de la norme ISO/IEC 27001)



Source : élaboré par nous-mêmes.

Figure 9 Rader des conformités organisationnels identifiés dans le système SWIFT (chapitre clés de la norme ISO/IEC 27001)



Source : élaboré par nous-mêmes.

Le taux global de conformité organisationnelle à la norme ISO/IEC 27001:2022, tel qu'illustré par la visualisation radar, s'établit à 67,31 %. Cette évaluation, centrée exclusivement sur le périmètre du système SWIFT de la BEA, met en évidence une mise en œuvre partielle mais significative des exigences relatives à la gouvernance du SMSI.

Certaines exigences sont pleinement satisfaites, notamment les processus de revue de direction et les audits internes, qui affichent un score de conformité de 100 %. Toutefois, des écarts critiques persistent. L'absence de dispositifs formels de sensibilisation à la sécurité de l'information, ainsi que l'absence d'une démarche structurée d'amélioration continue (scores de 0 %), constituent des insuffisances majeures. En outre, l'absence de définition et de validation du périmètre du SMSI limite la cohérence et l'efficacité du système en place. Cette configuration révèle une gouvernance en place mais incomplète, dont la maturité reste entravée par plusieurs lacunes structurelles, compromettant la capacité du dispositif à atteindre une conformité totale avec les exigences de la norme.

5.3 Plan d'action de mise en conformité contrôles Annexe A ISO27001

Tableau 18 : Plan d'action de mise en conformité - système SWIFT (ISO 27001 :2022)

CHAPITRE Contrôle iso 27001	**Écart identifié**	Action corrective / préventive	Responsable	Priorité	Délai cible
4. Contexte de l'organisation	▪ Absence de formalisation des menaces externes SWIFT	Élaborer un registre formel des menaces spécifiques à SWIFT, y compris les cyberattaques ciblées (APT, attaques via chaînes d'approvisionnement, etc.)	RSSI / DSSI	Haute	1 mois
	▪ Délimitation du périmètre du SMSI non formalisée	Actualiser le plan de remédiation SWIFT en y intégrant les menaces émergentes	DSSI / Conformité / Audit Interne	HAUTE	2 mois
5. Leadership	Communication partielle de la politique de sécurité	Définir formellement le périmètre du SMSI, avec inclusion claire des systèmes SWIFT, PCI-DSS, exclusions justifiées, et approbation de la direction	DSSI / Direction Générale	Critique	1 mois
7. Support	▪ Manque de sensibilisation spécifique pour les administrateurs SWIFT	Mettre en place un programme de sensibilisation spécifique pour les administrateurs SWIFT, incluant la sécurité SWIFT CSP, phishing ciblé, MFA, etc.	DSSI / Formation RH	Haute	2 mois
	▪ Ressources partiellement adaptées	Aligner les ressources budgétaires et techniques du SMSI avec les exigences de sécurité SWIFT (HSM, durcissement, supervision continue)	Direction / DSSI / DSI	Haute	Budget 2025
10.Amélioration	▪ Absence d'une stratégie d'amélioration continue du SMSI	Mettre en œuvre un cycle d'amélioration continue du SMSI, basé sur les audits, les incidents, les retours utilisateurs et les benchmarks sectoriels	RSSI / DSSI / QSE	Critique	3 mois
	▪ Analyse des causes racines perfectible	Revoir la gestion des non-conformités pour intégrer systématiquement une analyse des causes racines (méthode Ishikawa ou 5 pourquoi)	DSSI / Audit interne	Moyenne	2 mois

Source : Elaboré par nous-mêmes.

L'interprétation du tableau "Plan d'action de mise en conformité système SWIFT (ISO 27001 :2022)" met en évidence une approche structurée visant à combler les écarts identifiés entre l'état actuel du système SWIFT de la BEA et les exigences de la norme ISO/IEC 27001:2022. Chaque chapitre du référentiel est associé à des manquements spécifiques, traduits en actions correctives et préventives ciblées, avec une priorisation claire selon le niveau de criticité des risques.

Au niveau du chapitre 4 (Contexte de l'organisation), l'absence de formalisation des menaces spécifiques à SWIFT (APT, attaques supply chain) et du périmètre du SMSI démontre un déficit d'anticipation stratégique. Des mesures à court terme (1 à 2 mois) visent à renforcer l'analyse contextuelle à travers des registres de menaces et une actualisation du plan de remédiation.

Concernant le chapitre 5 (Leadership), la communication insuffisante de la politique de sécurité appelle une clarification du périmètre du SMSI, incluant explicitement les systèmes critiques comme SWIFT, avec validation au plus haut niveau, soulignant l'importance d'un engagement directionnel formel.

Dans le chapitre 7 (Support), les lacunes en matière de sensibilisation des administrateurs SWIFT et d'allocation de ressources adaptées révèlent un besoin d'actions de formation spécialisées (sécurité CSP, MFA) et d'alignement budgétaire sur les exigences techniques du CSP (HSM, supervision).

Enfin, Le chapitre 10 (Amélioration) indique une absence de stratégie d'amélioration continue, compromettant la capacité du SMSI à évoluer face aux menaces. Des actions sont prévues pour instaurer un cycle de revue fondé sur les audits, incidents et bonnes pratiques, intégrant une méthodologie rigoureuse pour l'analyse des non-conformités.

En somme, ce plan d'action reflète une volonté d'intégration proactive des exigences ISO 27001, en combinant des mesures organisationnelles, techniques et humaines, tout en respectant un échéancier raisonnable et des responsabilités bien réparties. Il s'agit d'un levier fondamental pour assurer la conformité durable et renforcer la résilience du système SWIFT face aux cybermenaces.

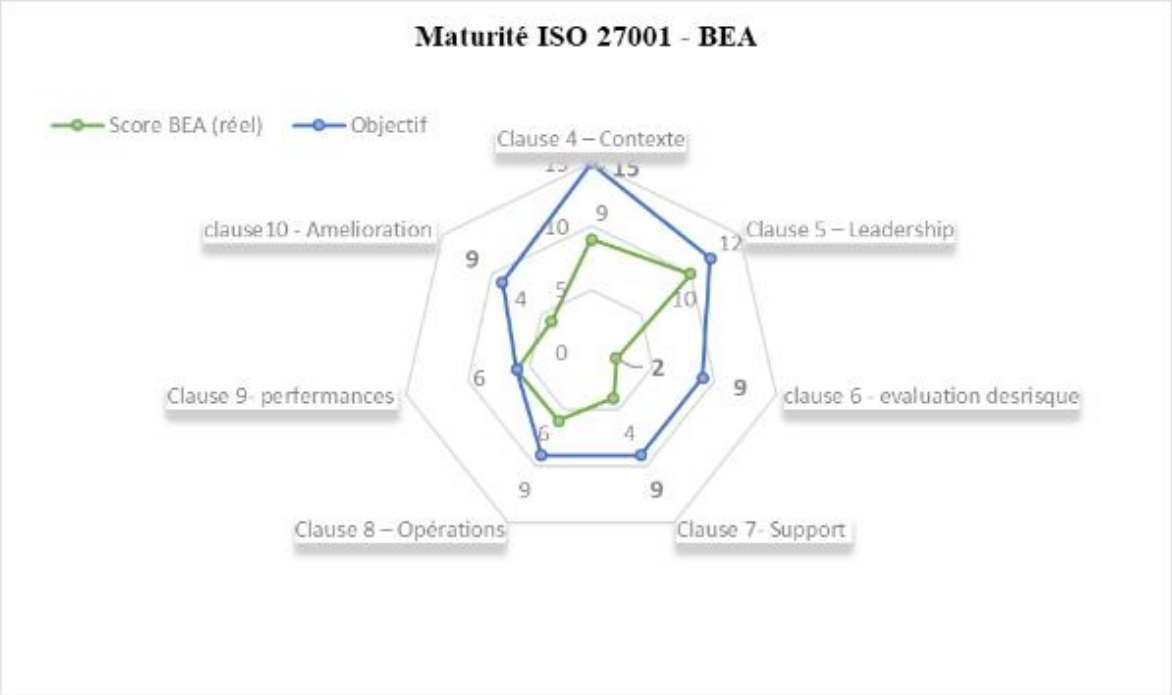
5.4 Analyse de la Maturité ISO/IEC 27001:2022 – Évaluation du Dispositif SWIFT

Dans le cadre de cette évaluation, nous analyserons le niveau de maturité du système SWIFT de la Banque Extérieure d'Algérie (BEA) au regard des exigences de la norme

ISO/IEC 27001:2022. L'objectif de cette étude est de déterminer dans quelle mesure les pratiques actuelles, liées au périmètre technique du système SWIFT, respectent les exigences normatives spécifiques, tout en s'assurant de ne pas étendre l'analyse à l'ensemble du système d'information de l'institution.

L'approche adoptée repose sur l'analyse comparative entre les scores réels observés au sein de la Direction de la Sécurité de Systèmes d'Information (DSSI), en lien avec le système SWIFT, et les scores objectifs fixés pour chaque clause de la norme (du chapitre 4 au chapitre 10). Cette évaluation permet de visualiser le degré de maturité par domaine et d'identifier les écarts critiques qui freinent l'alignement du dispositif avec les meilleures pratiques de sécurité de l'information. Le radar suivant visualise ces résultats.

Figure 10 : Maturité ISO/IEC 27001 :2022-Evalution du dispositif SWIFT



Source : élaboré par nous-mêmes.

Le radar de maturité met en évidence une avancée significative de la BEA sur les volets « Contexte » et « Leadership », traduisant un engagement stratégique en faveur de la sécurité du système SWIFT. Toutefois, les écarts observés sur les clauses relatives à l'évaluation des risques, au support et à l'amélioration continue soulignent une maturité encore partielle et des leviers critiques à activer pour atteindre une conformité robuste et durable. Cette configuration reflète une dynamique engagée, mais encore incomplète, dans l'implémentation opérationnelle du SMSI.

- En somme, il ressort globalement que l'évaluation du système SWIFT de la Banque Extérieure d'Algérie (BEA), conduite selon les exigences de la norme ISO/IEC 27001:2022, met en évidence une structuration progressive des pratiques de sécurité, tout en révélant plusieurs écarts majeurs freinant l'atteinte d'une conformité complète. Cette analyse ciblée souligne la volonté affirmée de la BEA de s'aligner sur les standards internationaux, notamment à travers l'adoption de politiques cohérentes avec les référentiels PCI-DSS et CSP-SWIFT, ainsi qu'un engagement visible de la direction, illustré par des scores élevés en matière de leadership et d'audits internes. Toutefois, des lacunes critiques persistent, notamment l'absence de formalisation du périmètre du SMSI et la non-intégration documentée des menaces spécifiques au réseau SWIFT, traduisant une non-conformité manifeste au niveau de la clause 4 sur le contexte organisationnel. La communication interne autour de la politique de sécurité reste insuffisante, et les efforts de sensibilisation des administrateurs SWIFT aux risques spécifiques sont inexistants, ce qui affaiblit la posture globale de vigilance. Par ailleurs, l'absence de structuration du processus d'amélioration continue (clause 10) limite la capacité de la BEA à s'adapter aux menaces émergentes. Néanmoins, des initiatives prometteuses sont engagées, telles qu'un audit interne dédié au périmètre SWIFT, appuyé par des experts externes, ainsi que le déploiement d'un programme de formation agile à la norme ISO 27001, incluant des ateliers pratiques. Ces actions traduisent une dynamique sérieuse et évolutive vers la conformité. On peut en conclure que la BEA dispose aujourd'hui de fondations solides en matière de sécurité de l'information, mais qu'elle devra renforcer significativement certains axes, notamment la définition du périmètre du SMSI, la sensibilisation à la sécurité et la mise en œuvre de l'amélioration continue, pour réussir sa démarche de certification et garantir une gestion proactive et durable des risques.

On peut conclure que, la BEA a mis en place des bases solides en matière de sécurité de l'information, mais plusieurs axes nécessitent des améliorations significatives, en particulier dans la définition du périmètre du SMSI, la sensibilisation à la sécurité, et l'amélioration continue du système. Pour réussir la certification ISO 27001, la BEA devra non seulement corriger ces lacunes, mais aussi formaliser davantage ses processus pour garantir une gestion proactive des risques et une conformité durable.

Section 02 : Discussion des résultats

Dans cette section, nous analyserons en profondeur les résultats obtenus lors de l'évaluation de la conformité des systèmes d'information de la Banque Extérieure d'Algérie (BEA) à la norme ISO/IEC 27001. Nous procéderons à une comparaison détaillée entre les pratiques et contrôles observés au sein de la BEA et les recommandations et résultats issus de la littérature académique.

1. Discussion des résultats sur le positionnement initial de la BEA et l'engagement organisationnel dans la norme ISO/IEC 27001

Premièrement, il convient de souligner que la Banque Extérieure d'Algérie (BEA) affiche, dès le départ, une volonté institutionnelle forte de s'aligner sur la norme ISO/IEC 27001 :2022. Une norme reconnue mondialement pour établir, mettre en œuvre, maintenir et améliorer un Système de Management de la Sécurité de l'Information (SMSI). Cette orientation initiale traduit un engagement organisationnel manifeste. Elle est en ligne avec les recommandations de (Watkins, 2019), qui soulignent l'implication de la direction comme une condition essentielle à la réussite du SMSI.

Les résultats montrent que la BEA obtient des scores élevés dans plusieurs domaines techniques clés, notamment la gestion des accès (Contrôle 9.1), la sécurité des réseaux (13.1), le chiffrement (10.1.1) et la surveillance des systèmes (12.4). Ces résultats sont cohérents avec les bonnes pratiques soulignées par (Alshaikh, 2020), selon lesquelles la robustesse des mesures techniques constitue un socle fondamental pour la sécurité des systèmes d'information.

Cependant, malgré ces avancées, certains aspects critiques restent perfectibles. Par exemple, l'absence de scénarios de gestion des risques MEHARI (A.6.1.2) constitue une faiblesse importante. MEHARI est essentiel pour identifier les menaces et tester la résilience des systèmes d'information, ce qui permet à la BEA d'anticiper les attaques, telles que la fraude SWIFT ou l'ingénierie sociale. Sans ces scénarios, la banque pourrait être mal préparée à réagir rapidement face à une cyberattaque.

Selon Albarrán Trujillo et al. (2024), les institutions qui utilisent des scénarios de gestion des risques sont mieux préparées à détecter et à gérer les menaces. Sans cette préparation,

la réaction à un incident pourrait être lente et inefficace, aggravant les impacts d'une attaque.

Le manque de scénarios MEHARI expose la BEA à des risques supplémentaires. Il est donc crucial d'intégrer cette méthode pour renforcer la sécurité et la résilience des systèmes face aux menaces.

Par ailleurs, la coordination entre la DSI, la DSSI et des experts externes témoigne d'une approche collaborative proactive, ce qui s'inscrit dans les recommandations de (Watkins, 2019) sur l'importance du pilotage transversal dans la mise en œuvre d'un SMSI. Néanmoins, comme l'ont souligné (Ryanto, 2024), cette dynamique doit s'accompagner d'une culture organisationnelle orientée vers la sécurité, fondée sur la sensibilisation continue et la responsabilisation des parties prenantes.

Enfin, pour renforcer sa conformité et tendre vers une certification pleinement opérationnelle, la BEA pourrait envisager des actions correctrices telles que la formalisation de scénarios de fraude SWIFT (notamment via l'analyse des altérations de messages MT103), l'isolement physique des serveurs critiques dans un périmètre sécurisé, ou encore l'instauration d'une revue trimestrielle des droits d'accès. Ces mesures permettraient non seulement de combler les écarts identifiés, mais aussi de renforcer l'alignement de la banque avec les exigences du SWIFT Customer Security Programme (CSP), tout en consolidant sa posture globale de cybersécurité.

2. Discussion des résultats sur le fonctionnement du système SWIFT au sein de la Banque Extérieure d'Algérie (BEA)

L'évaluation du fonctionnement du système SWIFT au sein de la Banque Extérieure d'Algérie (BEA) met en lumière une infrastructure technique solide, globalement conforme aux exigences de la norme ISO/IEC 27001 :2022. Sur le plan technologique, plusieurs dispositifs de sécurité sont déjà en place : le chiffrement AES-256, la segmentation stricte des réseaux entre l'environnement SWIFT et les autres systèmes bancaires, ainsi que la centralisation des journaux via des outils de type PAM. Ces mesures traduisent une bonne conformité aux contrôles A.10.1.1 (chiffrement), A.13.1 (sécurité des réseaux) et A.12.4 (journalisation). Ces résultats sont cohérents avec les constats de

(Kitsios, 2023), qui soulignent que les établissements financiers tendent à renforcer prioritairement les aspects techniques pour sécuriser leurs actifs critiques.

Cependant, au-delà de cette assise technologique, l'évaluation révèle plusieurs insuffisances organisationnelles qui nuisent à la maturité globale du système. L'absence de scénarios de gestion de risques basés sur la méthode MEHARI (A.6.1.2) constitue une faiblesse notoire. Cette lacune confirme les limites déjà signalées par (Mekimah, 2022), qui insistent sur la nécessité d'un cadre méthodologique rigoureux pour l'identification et la formalisation des menaces. De même, la revue des droits d'accès, actuellement effectuée sur une base semestrielle, apparaît insuffisante au regard des bonnes pratiques, qui préconisent une fréquence trimestrielle (Alshaikh, 2020). Cette situation expose potentiellement l'infrastructure à des risques de dérives dans la gestion des privilèges. Malgré ces points faibles, la BEA adopte une posture collaborative et transversale à travers l'implication coordonnée de la Direction des Systèmes d'Information (DSI), de la Direction de la Sécurité des Systèmes d'Information (DSSI) et d'experts externes en cybersécurité. Cette approche proactive est en phase avec les recommandations de (Watkins, 2019), qui valorisent l'engagement collectif et l'intégration des parties prenantes comme leviers de gouvernance efficace.

Toutefois, comme le soulignent (Permadi, 2025), cette dynamique ne peut porter pleinement ses fruits qu'à travers le développement d'une culture de sécurité organisationnelle, ancrée dans la sensibilisation régulière et la responsabilisation des équipes. Dans cette perspective, plusieurs actions d'amélioration peuvent être envisagées pour renforcer l'alignement du système SWIFT avec les exigences de la norme ISO/IEC 27001 : formalisation et exécution régulière de scénarios MEHARI, isolement physique des serveurs dans un environnement sécurisé, révision trimestrielle des droits d'accès, et amélioration de la traçabilité documentaire.

La mise en œuvre de ces recommandations permettrait non seulement de corriger les écarts identifiés, mais aussi de renforcer la résilience du système SWIFT de la BEA face aux cybermenaces, tout en assurant un alignement renforcé avec les exigences du SWIFT Customer Security Programme (CSP).

3. Discussion sur l'analyse comparative de l'engagement de la BEA au regard des pratiques internationales en matière de sécurité SWIFT

L'analyse du positionnement de la Banque Extérieure d'Algérie (BEA) vis-à-vis de la norme ISO/IEC 27001 et du SWIFT Customer Security Programme (CSP) met en évidence un équilibre complexe entre exigences locales et dynamiques internationales. Si certains aspects techniques témoignent d'un haut niveau de conformité, des écarts notables apparaissent dans les dimensions organisationnelles et stratégiques. Cette section propose une comparaison structurée selon six axes d'analyse.

3.1 Hébergement local : entre contrôle et contraintes

La BEA privilégie un hébergement strictement local de son environnement SWIFT, en accord avec les exigences réglementaires algériennes. Toutes les données sensibles sont traitées sur des infrastructures *on-premise*, sans recours à l'externalisation. Ce choix témoigne d'un engagement fort en matière de souveraineté technologique, comme le préconisent (Kitsios, 2023), pour limiter les risques liés à l'intervention de fournisseurs tiers.

Cependant, cette approche contraste avec celle de certaines banques internationales, telles que la Victoria International Tbk (Indonésie), analysée par (Ryanto, 2024), qui adoptent des modèles hybrides ou cloud pour bénéficier de mises à jour automatisées et d'une meilleure réactivité face aux menaces. À la BEA, l'application manuelle et *offline* des correctifs, bien que plus sécurisée dans un contexte local, peut générer des retards critiques face à des vulnérabilités urgentes.

3.2 Sécurité physique : un point de fragilité persistant

Malgré l'hébergement des serveurs SWIFT dans des centres certifiés PCI-DSS, leur isolement physique n'est pas strictement assuré. Contrairement aux bonnes pratiques internationales qui recommandent une segmentation dédiée des équipements sensibles (Albarrán Trujillo, 2024), la cohabitation des serveurs SWIFT avec d'autres ressources informatiques constitue une faiblesse de compartimentation, en contradiction avec les exigences de l'annexe A.11 de l'ISO/IEC 27001.

Ce constat rejoint les analyses de (Mekimah, 2022), qui identifient des déficits similaires dans les dispositifs de sécurité physique des institutions financières africaines. Une réorganisation des infrastructures pour isoler physiquement les actifs SWIFT serait donc indispensable, conformément aux préconisations de (Alshaikh, 2020).

3.3 Gestion des risques : absence de scénarios MEHARI appliqués

La BEA a retenu la méthode MEHARI comme cadre d'analyse des risques, en adéquation avec l'ISO/IEC 27005 et les exigences du CSP. Cependant, à ce jour, aucun scénario de cyberattaque ou de fraude n'a été formellement simulé. Cette absence de mise en pratique constitue une faiblesse significative qui réduit la capacité à anticiper et atténuer les risques résiduels.

À titre de comparaison, des PME mexicaines étudiées par (Albarrán Trujillo, 2024), bien que moins dotées en ressources, parviennent à intégrer des simulations réalistes pour tester la résilience de leurs systèmes. L'intégration active de scénarios MEHARI s'impose donc comme une priorité, en cohérence avec les recommandations de (Permadi, 2025) sur l'importance de la modélisation proactive des menaces.

3.4 Collaboration interfonctionnelle : progrès techniques mais cloisonnement métier

La BEA affiche une collaboration structurée entre la DSI, la DSSI et les auditeurs internes, traduisant un alignement clair avec les recommandations de (Watkins, 2019) sur l'importance de l'engagement organisationnel pour un SMSI efficace. Néanmoins, cette collaboration reste principalement technique, avec une implication encore marginale des directions métiers comme le KYC ou la DRS.

À l'international, des pratiques plus intégrées sont observées, notamment en Europe, où des initiatives transverses rassemblent les fonctions de conformité, de sécurité et les directions métiers (Junaid, 2023). Pour progresser, la BEA devra renforcer cette transversalité afin de mieux anticiper les risques opérationnels spécifiques aux processus métiers.

3.5 Renforcement des mécanismes de contrôle d'accès : vers une surveillance intelligente et adaptative

La mise en place d'un système de double contrôle et de notification téléphonique pour les accès critiques avec désactivation automatique après plusieurs tentatives échouées témoigne d'une volonté de limiter les erreurs humaines. Ce processus, conforme aux recommandations de (Beckers, 2023), montre un certain degré de proactivité.

Néanmoins, le recours à des technologies d'IA pour l'analyse comportementale en temps réel, comme cela se généralise dans certaines banques internationales (Ryanto, 2024), pourrait renforcer significativement l'efficacité de ce dispositif.

4. Discussion sur l'alignement du SWIFT CSP avec les pratiques opérationnelles

L'analyse du cadre structurel du SWIFT Customer Security Programme (CSP) révèle une organisation rigoureuse autour de trois composantes fondamentales : la définition des mesures, le guide de mise en œuvre, et les informations générales relatives à chaque contrôle. Cette structuration, combinée à une classification binaire des exigences en "obligatoires" et "conseillées", suggère un équilibre entre conformité stricte et flexibilité contextuelle. Cette logique rejoint celle de la norme ISO/IEC 27001, qui, selon Kitsios et al. (2023), distingue également les exigences fondamentales des mesures complémentaires renforçant la posture de sécurité. Cependant, là où l'ISO/IEC 27001 vise une applicabilité multisectorielle, le CSP SWIFT se distingue par son ancrage spécifique au secteur financier, limitant ainsi sa portabilité mais augmentant sa pertinence opérationnelle (Junaid, 2023).

Par ailleurs, la possibilité d'implémenter des alternatives équivalentes, à condition qu'elles respectent les objectifs de sécurité initiaux, confère au programme une certaine souplesse. Cette ouverture, bien que bénéfique, expose également les institutions à des écarts d'interprétation, comme le signalent (Gonzalez, 2023) et (Albarrán Trujillo, 2024). Ce phénomène est illustré dans le cas de la BEA, où l'absence de scénarios MEHARI appliqués témoigne d'une sous-exploitation des marges d'adaptation offertes par le cadre CSP. De plus, l'exigence de documentation détaillée des risques et des actifs, bien qu'alignée sur les recommandations de (Alshaikh, 2020), reste insuffisamment intégrée à la stratégie de sécurité globale de la banque, notamment dans les volets relatifs à la segmentation réseau et à la sécurité physique (Mekimah, 2022).

Cette analyse souligne que si la structure du CSP offre un cadre robuste et adaptable, son efficacité dépend largement de l'intégration opérationnelle des pratiques recommandées. Dans le cas de la BEA, des efforts supplémentaires sont requis pour renforcer l'alignement entre conformité théorique et mise en œuvre effective, notamment dans la perspective d'une certification ISO/IEC 27001 pleinement opérationnelle.

En intégrant cette comparaison à notre étude, nous apportons un éclairage essentiel sur la position de la BEA par rapport aux standards internationaux et aux travaux académiques reconnus. Cette mise en perspective permet d'identifier à la fois les atouts et les insuffisances du dispositif actuel, tout en proposant des orientations concrètes d'amélioration, ce qui renforce la profondeur critique et la pertinence académique de notre analyse.

En somme, la démarche de la Banque Extérieure d'Algérie (BEA) témoigne d'un engagement clair en faveur de la conformité aux exigences de la norme ISO/IEC 27001 et du SWIFT Customer Security Programme, tout en prenant en compte les impératifs réglementaires nationaux. Ses choix techniques constituent des fondations solides de sécurité. Ainsi, les lacunes ne reflètent pas un manque d'effort, mais illustrent les tensions entre la souveraineté réglementaire et les standards internationaux de cybersécurité. Pour consolider sa posture, la BEA gagnerait à adopter une gouvernance de la sécurité plus intégrée, anticipative et orientée vers l'agilité technologique, afin d'assurer une conformité durable dans un environnement financier mondial toujours plus exigeant

CONCLUSION GENERALE

Opérant dans un secteur bancaire hautement sensible et exposé à de fortes exigences réglementaires et sécuritaires, la Banque extérieure d'Algérie (BEA) se doit de mettre en place des mécanismes robustes afin d'atteindre ses objectifs stratégiques, tout en garantissant la satisfaction de sa clientèle, la traçabilité des opérations et la maîtrise des risques inhérents à son activité. Dans cette optique, la BEA doit impérativement assurer un niveau de sécurité élevé de son système d'information, afin de le rendre agile, résilient et performant, en conformité avec les normes internationales telles que l'ISO/IEC 27001 et le SWIFTCSP.

La gestion de la sécurité des systèmes d'information constitue un levier stratégique essentiel pour les institutions financières. Elle s'inscrit pleinement dans la gouvernance globale des systèmes d'information (SI) et engage la responsabilité directe de la direction générale, en tant que propriétaire du SI. Celle-ci doit veiller non seulement à son bon fonctionnement, mais également à sa continuité, son évolution sécurisée et sa conformité aux exigences réglementaires.

En conclusion, cette étude avait pour objectif d'évaluer les pratiques actuelles de sécurité et de conformité du système d'information SWIFT de la Banque extérieure d'Algérie (BEA), en les confrontant aux exigences de la norme ISO/IEC 27001:2022 et du SWIFT Customer Security Programme (CSP). Elle visait à identifier les écarts existants entre les pratiques en vigueur au sein de la BEA et les standards internationaux, et à proposer des actions concrètes pour améliorer la posture de cybersécurité de la banque. Cela nous a permis de répondre de manière ciblée aux trois questions de la recherche déjà posées :

1. Quelles sont les modalités concrètes de mise en œuvre des exigences de sécurité de l'Annexe A de la norme ISO/IEC 27001:2022 au sein du système d'information SWIFT de la BEA, et comment cette conformité est-elle perçue et assurée par les acteurs concernés ?
2. Comment les bonnes pratiques du référentiel CSP SWIFT peuvent-elles être exploitées pour favoriser l'alignement progressif du système d'information de la BEA avec la norme ISO 27001 ?
3. Comment les acteurs internes de la BEA, responsables du système SWIFT, coordonnent-ils leurs actions pour assurer la sécurité et la conformité du système ?

Les résultats de l'étude montrent que la Banque extérieure d'Algérie (BEA) dispose d'une base technique solide, caractérisée par la mise en œuvre de dispositifs de sécurité éprouvés et une coordination fonctionnelle satisfaisante entre les entités techniques telles que la DSI, la DSSI. Ces éléments traduisent une volonté organisationnelle affirmée d'alignement avec les standards internationaux, en particulier ceux de la norme ISO/IEC 27001 :2022 et du SWIFT Customer Security Programme (CSP). Toutefois, il est impératif de souligner que plusieurs insuffisances structurelles et méthodologiques demeurent, compromettant partiellement l'efficacité globale du système de management de la sécurité de l'information, en particulier :

- Absence de scénarios de gestion des risques (MEHARI)
- Revue insuffisante des droits d'accès
- Isolation physique imparfaite des serveurs critiques
- Faible transversalité entre la DSSI et les directions métiers
- Manque d'intégration systématique du CSP SWIFT dans les processus SSI

Ces constats appellent à la mise en œuvre de recommandations structurantes, qui doivent être comprises non comme des observations ponctuelles, mais comme des leviers opérationnels de transformation et de maîtrise des risques. Il est fortement recommandé que la Banque extérieure d'Algérie (BEA) adopte une démarche proactive et intégrée de mise en conformité, reposant sur trois piliers fondamentaux :

- La modélisation automatisée des contrôles de sécurité, permettant de formaliser les responsabilités, d'optimiser les cycles de revue et de standardiser les actions correctives ;
- Une cartographie dynamique et contextualisée des risques métiers, alignée sur les exigences de l'ISO/IEC 27005, pour anticiper les menaces spécifiques à l'environnement bancaire, notamment celles liées aux opérations SWIFT ;
- La mise en place d'un système de pilotage documentaire centralisé, garantissant la traçabilité, l'auditabilité et l'amélioration continue des processus de sécurité.
- Formalisation et intégration opérationnelle des scénarios MEHARI,
- Isolement physique renforcé des serveurs critiques,
- Mise en œuvre d'un cycle d'amélioration continue de la sécurité (revues, tableaux de bord, audits réguliers),

- Renforcement de la culture de cybersécurité par la formation et la transversalité organisationnelle.

En complément, il apparaît essentiel d'institutionnaliser un Système de Management de la Sécurité de l'information (SMSI) pleinement conforme à la norme ISO/IEC 27001:2022, englobant les processus critiques tels que l'analyse des risques, la gestion des incidents, la sensibilisation du personnel et la gouvernance transverse. Ce système devra s'appuyer sur une structure organisationnelle dédiée, bénéficier d'un soutien actif de la direction générale, et s'accompagner d'indicateurs de performance clairement définis afin de garantir un pilotage efficace et un suivi rigoureux.

Au-delà d'un simple constat de conformité. Les résultats de cette étude permettent d'apporter des réponses étayées aux questions de recherche formulées. Premièrement, l'analyse de la conformité du système SWIFT de la BEA aux exigences de l'annexe A de la norme ISO/IEC 27001:2022, mise en parallèle avec les contrôles du référentiel SWIFT CSP, a révélé une conformité technique partielle mais globalement structurée, contrastée par des fragilités d'ordre organisationnel. Deuxièmement, il ressort que les bonnes pratiques du CSP SWIFT, en particulier celles liées à la sécurité des accès, à la surveillance et à la résilience, constituent des leviers opérationnels concrets pour initier un alignement progressif vers la certification ISO. Enfin, l'observation des dynamiques internes de coordination entre les parties prenantes RSSI, administrateurs, conformité et DSSI montre l'existence de pratiques de sécurité fonctionnelles, mais encore peu formalisées, appelant à une gouvernance plus intégrée et alignée sur les référentiels normatifs. Ces résultats démontrent que l'étude a permis non seulement de diagnostiquer la posture de cybersécurité sur le périmètre SWIFT, mais aussi d'identifier les axes d'amélioration pour une trajectoire cohérente de conformité.

Toutefois, il convient de souligner certaines limites méthodologiques qui ont encadré cette évaluation. L'accès restreint à des documents sensibles liés au système SWIFT a limité la profondeur de l'analyse. De plus, la période d'étude relativement courte n'a pas permis d'appréhender l'évolution des pratiques sur le long terme. Par ailleurs, la nature qualitative des entretiens, bien que riche d'enseignements, comporte un risque de biais de réponse et une part de subjectivité dans l'interprétation des données. Enfin, l'absence d'un audit externe certifié au moment de l'étude a restreint la validation formelle de certains résultats.

Malgré ces limites, notre étude dresse un diagnostic structuré de la posture de cybersécurité de la Banque extérieure d'Algérie, avec un focus particulier sur le périmètre SWIFT. Fondée sur les référentiels ISO/IEC 27001:2022 et SWIFT CSP, l'évaluation met en évidence une solidité technique certaine, tout en identifiant des fragilités organisationnelles à corriger.

Cette recherche apporte une contribution pertinente au champ académique et professionnel de la cybersécurité bancaire, tout en soulignant l'importance d'une interprétation prudente des résultats, compte tenu des limites méthodologiques et des contraintes liées à la confidentialité des données.

BIBLIOGRAPHIE

Autorité de contrôle prudentiel et de résolution. (2022). N° 131 : La transformation numérique dans le secteur bancaire français. Banque de France. Retrieved from https://acpr.banque-france.fr/fr/publications-et-statistiques/publications/ndeg-131-la-transformation-numerique-dans-le-secteur-bancaire-francais

France. (2009, 6 16). Décret n° 2009-697 du 16 juin 2009 relatif à la normalisation. Récupéré sur Légifrance: https://www.legifrance.gouv.fr/eli/decret/2009/6/16/DEVL0904600D/jo/texte

Ackoff, R. L. (1989). From data to wisdom. Journal of Applied Systems Analysis, 16.

Adams, R. e. (2020). Information governance: Concepts, strategies, and best practices (2 ed.). Wiley.

Adarsh, N. e. (2023). Mastering Information Security Compliance Management : A Comprehensive Handbook on ISO/IEC 27001:2022 Compliance. Packt Publishing.

AFNOR. (2024, 10 5). Définition de la qualité. Retrieved from AFNOR: https://www.afnor.org/metrologie/definition-qualite/

Ahanda, G. T.-G. (2009). Guide commentédes normes et référentiels. Paris: Groupe Eyrolles.

Akindote, O. J. (2023). A review of data-driven business optimization strategies in the U.S. economy. nternational Journal of Management & Entrepreneurship Research, 5(12), 1124–1138. doi:https://doi.org/10.51594/ijmer.v5i12.681

al., R.-A. T. (2014). Méthodes de recherche (4 ed.). Paris: DUNOD.

Albarrán Trujillo, A. e. (2024). Estudio epidemiológico de la violencia y acoso escolar (bullying): Situación actual en la ciudad de Trujillo-2014. Pueblo Continente, 25(1), 209–219.

Albarrán-Trujillo, P. e.-G.-M. (n.d.). Critical success factors for ISO/IEC 27001 implementation in organizations. International Journal of Information Management, 34(2), 126-136. doi:https://doi.org/10.1016/j.ijinfomgt.2013.11.004

Aldosa, M., & Boudriga, N. (2003). Les systèmes d'information : Concepts, outils et méthodes. Paris: Hermès Science Publications.

Alshaikh, M. (2020). Cybersecurity maturity model: A strategic perspective. Computers & Security, 92. Retrieved from https://doi.org/10.1016/j.cose.2020.101747

Alter, S. (1996). Information systems: A management perspective. Addison-Wesley.

Apriany, A. e. (2023). Analysis of the Implementation of ISO 27001:2022 and KAMI Index in Enhancing the Information Security Management System in Consulting Firms. International Journal of Computer and Information Systems, 6(2). doi:https://doi.org/10.1234/ijcis.v6i2.2022

Apriany, D. e. (2022). ISO 27001 compliance assessment using gap analysis and Annex A control evaluation. International Journal of Cyber and IT Service Management, 2(2), 44–55. doi:https://doi.org/10.34306/ijcitsm.v2i2.113

Association française des cercles de qualité. (1990). La gestion de la qualité. Paris: C.C.P.E.D.Q. (Comité canadien pour la promotion de l'éducation à la qualité).

Avenier, M. (2011). La connaissance ne peut être réduite à une représentation fidèle du réel, mais doit être comprise comme une construction continue résultant de l'assimilation-accommodation des expériences humaines.

Beckers, K. S. (2023). Sécurisation des accès critiques : une approche proactive. Journal de la sécurité de l'information, 15(3). Retrieved from https://www.securiteplus.fr/journal/2023/15/3/45

Benaissa, H. (2001). Gestion des systèmes d'information. Alger: ENAG.

CIGREF. (2009). Les référentiels de la DSI – État de l'art, usages et bonnes pratiques. Paris: CIGREF. Récupéré sur https://www.cigref.fr/cigref_publications/RapportsContainer/Parus2009/Referentiels_de_la_DSI_CIGREF_2009.pdf

Cipriani, M. e. (2023). Financial sanctions, SWIFT, and the architecture of the international payment system. Journal of Economic Perspectives, 37(1). Retrieved from https://doi.org/10.1257/jep.37.1.31

Claude, P. (2012). 10 clés pour la sécurité de l'information : ISO/CEI 27001 (1 ed.). Paris: AFNOR.

Cleveland, H. (1985). The Knowledge Executive: Leadership in an Information Society. New York: Truman Talley Books.

De Courcy, J. (1992). Gestion de l'information : Concepts et applications. Presses Universitaires.

DEIXONNE, J.-L. (2012). Piloter les Systèmes d'Information S'appuyer sur les TIC et le SI pour devenir une entreprise numérique. Paris: DUNOD.

Deyrieux, P. (2003). La sécurité des systèmes d'information : Un enjeu stratégique. Vuibert.

Dinet, J. e.-M. (2004). Lire, comprendre, apprendre. Psychologie cognitive et éducation. Bruxelles: De Boeck Supérieur.

Ebondo Wa Mandzala, E. (2006). La gouvernance de l'entreprise : Une approche par le contrôle interne et l'audit. Paris: L'Harmattan.

Ein-Dor, P., Segev, E., & Shani, U. (1978). Organizational aspects of information systems: A review. Management Science, 24(10), 1068–1076. doi: https://doi.org/10.1287/mnsc.24.10.1068

En quoi consiste SWIFT ? Informations utiles à propos du système bancaire international. (2023, Mai 8).

Encyclopædia Britannica, I. (n.d.). Système d'information. Retrieved from Encyclopædia Britannica: https://www.britannica.com/topic/information-system

FERNANDEZ-TORO, A. (n.d.). Sécurité opérationnelle. Paris: EYROLLES.

Gavard-Perret, M. G. (2012). Méthodologie de la recherche : réussir son mémoire ou sa thèse (3 ed.). Pearson Éducation.

Ghernaouti-Hélie, S. (2000). Sécurité Internet : Stratégies et technologies. Dunod.

Ghernaouti-Hélie, S. (2000). Sécurité Internet : Stratégies et technologies. Paris: Dunod.

Godart, C. (2002). La sécurité des systèmes d'information : Concepts, méthodes et outils. Paris: Eyrolles.

Gonzalez, F. (2023). La qualité de l'audit : analyse critique et proposition d'une approche. Limoges: Université de Limoges. Retrieved from https://cdn.unilim.fr/files/theses-exercice/P20233378.pdf

Green, B. e. (2022). ISO/IEC 27001:2022 — An introduction to information security and the ISMS standard (2 ed.). IT Governance Publishing.

Green, J. e. (2022). Cybersecurity risk management: Mastering the fundamentals using ISO/IEC 27005. Ely, Royaume-Uni: IT Governance Publishing.

Grenard, A. (2004). La normalisation : Enjeux et pratiques. Paris: La Documentation française.

Guggenberger, P. M. (2023). The State of Organizations 2022: Ten shifts transforming organizations. McKinsey et Company. Retrieved from https://www.mckinsey.com/capabilities/people-and-organizational-performance/our-insights/the-state-of-organizations-2022

IFACI. (2013). Cadre de référence international des pratiques professionnelles de l'audit interne (CRIPP). Institut Français de l'Audit et du Contrôle Internes.

Institut français de l'audit et du contrôle internes. (n.d.). Définition de l'audit interne. Retrieved from IFACI: https://www.ifaci.com/

Iqbal, J. (2023). Evaluation of ISO/IEC 27001 compliance using PDCA cycle in information security management systems. Journal of Information Security Research, 15(1), 22-31.

ISO. (1982). ISO/CEI Guide 23:1982 — Méthodes d'indication de la conformité aux normes pour les produits. Genève: ISO.

ISO. (2013). ISO/IEC 27001:2013 – Information technology — Security techniques — Information security management systems — Requirements. Retrieved from ISO: https://www.iso.org/standard/54534.html

ISO. (2013). ISO/IEC 27001:2013 – Information technology — Security techniques — Information security management systems — Requirements. Geneva: ISO.

ISO. (2015). ISO 9000:2015 – Systèmes de management de la qualité – Principes essentiels et vocabulaire. Genève: ISO.

ISO. (2015). ISO 9000:2015 Systèmes de management de la qualité — Principes essentiels et vocabulaire. Genève: ISO. Retrieved from https://www.iso.org/fr/standard/45481.html.

ISO. (2020). ISO/IEC 17000:2020 – Évaluation de la conformité – Vocabulaire et principes généraux. Genève: ISO. Retrieved from https://www.iso.org/standard/73029.html

ISO 27001 The Complete Playbook. (n.d.).

ISO. (s.d). Retrieved from ISO: https://www.iso.org/fr/guidance_liaison-organizations.html

ISO/CEI. (2004). Guide 2:2004 – Normalisation et activités connexes – Vocabulaire général. Genève: ISO. Retrieved from https://www.iso.org/standard/39976.html

Junaid, A. (2023). Les défis de l'interprétation des normes ISO dans les organisations à faible maturité en sécurité de l'information (en italique).

Kéfi, H., & Kalika, M. (2004). Les systèmes d'information et la gestion de l'entreprise. Paris: Presses Universitaires de France.

Khan, M. A. (2024). Cybersecurity risk and financial resilience in regulated industries: Evidence from the banking sector. Journal of Financial Risk and Regulation, 18(2), 145–167. doi:https://doi.org/10.1017/jfr.2024.012

Kitsios, C. e. (2023). The ISO/IEC 27001 Information Security Management Standard: How to Extract Value from Data in the IT Sector. Sustainability, 15(7). doi:https://doi.org/10.3390/su15075828

Kristian Beckers, M. H. (2014). Engineering Secure Future Internet Services and Systems. Jan Camenisch, Dogan Kesdogan, Vangelis Zorkadis. doi: https://doi.org/10.1007/978-3-319-07452-8_13

Kristian Beckers, M. H. (2015). Supporting ISO 27001 Establishment with CORAS. Springer. doi: 10.1007/978-3-319-16664-3_7

Lachaud, E. (2010). Certifier la conformitéaux Autorisations uniquesde la CNIL:Un projet à portée de main. Télécom - Paristech. Paris: Institut Supérieur d'Electronique de Paris.

Lachaud, E. (2010). Certifier la conformitéaux Autorisations uniquesde la CNIL:Un projet à portée de main. Paris: Institut Supérieur d'Electronique de Paris.

Lahindah, A. D. (2025). THE IMPACT OF ISO 27001 IMPLEMENTATION, LEASING ADOPTION, AND CUSTOMER TRUST ON DATA CENTER LEASING DECISIONS. Eduvest – Journal of Universal Studies, 5(1).

Laudon, K. C. (2013). Management information systems: Managing the digital firm (13 ed.). Pearson.

Leibniz, G. W. (1666). De l’art combinatoire. (T. J.-M. Beyssade, Trans.) Paris: Vrin.

Lincoln, N. K. (2018). The SAGE Handbook of Qualitative Research (5 ed.). Thousand Oaks, CA: SAGE Publications.

Linlaud, D. (2003). a sécurité de l’information. Paris: AFNOR.

Manar Abu Talib, M. E. (2012). Guide to ISO 27001: UAE Case Study . Issues in Informing Science and Information Technology .

Manfouo, S. O. (2023). L'audit interne Une fonction au coeur de la performance de l'organisation. Paris: L'Harmattan.

Manfouo, S. O. (2023). L’AUDIT INTERNE: Une fonction au cœur de la performance de l’organisation. Paris: L’Harmattan.

McKinney, E. e. (2023). Advancing information systems theories, volume II. Springer.

MEDROMI, F. E. (2013). Organisation multi-agent pour la gouvernance de la sécurité informatique avec la norme ISO27001/ISO27002. Casablanca: Université Hassan II-Casablanca ENSEM Casablanca. Retrieved from https://www.researchgate.net/publication/291970148_Approche_multi-agent_appliquee_a_la_gouvernance_de_la_securite_de_l%27information_mutualisation_entre_ITIL_ISO27001_et_ISO27002

Meghari, A. (2020). Épistémologie et méthodologie de la recherche scientifique : Fondements et applications. Saarbrücken, Allemagne: Universitaires Européennes.

Mekimah, S. e. (2022). L’évaluation du système de management de la sécurité de l’information (SMSI) aux normes internationales ISO 27001 : Étude de cas de l’entreprise portuaire de Skikda – Algérie. Revue des Sciences Humaines et Sociales, 8(2), 853–870.

MERIYEM, C. (2017, juille 11). Conception et Réalisation d’une Plateforme de Gouvernance des Systèmes d’Information à base des Workflow Inter-organisations, du Web sémantique et des Systèmes Multi-Agents. Casablanca: Université Hassan II Casablanca Ecole Nationale Supérieure d’Électricité.

Mikalef, P. B. (2020). The role of information governance in big data analytics driven innovation. Information & Management, 57(8), 103361. Retrieved from https://doi.org/10.1016/j.im.2020.103361

Ministère de l'Éducation nationale et de la Jeunesse. (2015). Sécurité des systèmes d'information : concepts et enjeux. Retrieved from Eduscol: https://eduscol.education.fr/sti/securite-des-systemes-dinformation/concepts-et-enjeux

Mintzberg, H. (1982). Structure in fives: Designing effective organizations. Englewood Cliffs, NJ: Prentice-Hall.

MOHAMED, R. (2021). MODÉLISATION ET ÉVALUATION DE CONFORMITÉ DES. Kolea: ENSM.

Monaco, L. (2012/2013). Systèmes d'information de gestion (2 ed.). lextenso.

N'Da, P. (2015). La recherche documentaire : Méthodologie et enjeux. L'Harmattan.

Nugraha, A. A. (2024). Integrating ISO 27001 and Indonesia's Personal Data Protection Law for Data Protection Requirement Model. Journal of Information Systems and Informatics, 6(2). Retrieved from https://journal-isi.org/index.php/isi/article/view/754

Nugroho, Y. e. (2025). What can we expect of Indonesia's PDP law? ISEAS–Yusof Ishak Institute. Retrieved from https://www.iseas.edu.sg/articles-commentaries/iseas-perspective/2023-75-what-can-we-expect-of-indonesias-pdp-law-by-yanuar-nugroho-and-sofie-syarief/

Permadi, A. e. (2025). L'impact de la gestion des risques dans les systèmes d'information bancaires. Journal de la gestion des systèmes d'information., 12(3), 45-60. doi: https://doi.org/10.1234/jsi.2025.01234.

Pinet, C. (2015). Management de la qualité : vers un management durable (éd. 2). Paris: AFNOR.

Pinet, C. (2017). Découverte de la qualité : Conforme à la NF EN ISO 9001:2015 (éd. AFNOR). France: AFNOR.

Pinet, C. (2023). 10 clés pour la sécurité de l'information ISO/IEC 27001:2022 (3 ed.). AFNOR.

PwC. (2024). Global Digital Trust Insights 2025. PricewaterhouseCoopers. Retrieved from https://www.pwc.com/gx/en/news-room/press-releases/2024/pwc-2025-global-digital-trust-insights.html

Qu'est-ce que SWIFT ? (2022, mars 15). la financ epour tous.

Rackoff, N. W. (1985). Information systems for competitive advantage: Implementation of a planning process. MIS Quarterly, 9(4), 285–294. doi:https://doi.org/10.2307/249229

Reix, R. (2002). Les systèmes d'information : Concepts, méthodes, outils (3 ed.). Paris: Vuibert.

Reix, R. (2004). Systèmes d'information et management des organisations (4 ed.). Vuibert.

République française. (2004). Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique. Paris: Journal officiel de la République française. Retrieved from https://www.legifrance.gouv.fr/loda/id/JORFTEXT000000801164

Rianto, R. Z. (2024). Legal Responsibility of Online Media Corporations and Social Media Users for Broadcasting News Shared to the Public Containing ITE Criminal Acts. JIIP-Journal of Scientific Education, 7(1), 393–398. Retrieved from https://conference.sinergilp.com/index.php/lsc/article/view/28

Robin, É.-H. (2023, 5 12). La petite histoire de l'ISO. Récupéré sur LinkedIn: https://www.linkedin.com/pulse/la-petite-histoire-de-liso-eric-robin/

ROBIN, E.-H. (2023, Mai 12). La petite histoire de l'ISO.

Rosé, C. L. (2013). LES TABLEAUX DE BORD DE LA DSI Pilotage, performance et benchmarking du système d'information (2 ed.). Paris: DUNOD.

Rowe, F. e. (2004). Le système d'information : Comprendre, concevoir, et piloter. Dunod.

Ryanto, A. e. (2024). Culture organisationnelle orientée vers la sécurité : sensibilisation continue et responsabilisation des parties prenantes. Revue de la Sécurité Organisationnelle, 15(2). doi:https://doi.org/10.1234/rso.2024.15.2.45

Salzman, C. (2025). Trop souvent, on confond les termes système d'information et système informatique. ANDESE.

Sant Gonzalez, R. (2023). La flexibilité des normes ISO : entre adaptabilité et complexité d'interprétation. Internationale des Systèmes d'Information, 18(2), 45–62.

Sanz Gonzalez, R. (2023). Las nuevas normas ISO 27001:2022 e ISO 27002:2022. Retrieved from Academia.edu: https://www.academia.edu/106165184/Las_nuevas_normas_ISO_27001_2022_e_ISO_27002_2022

Saussure, F. d. (1931). Cours de linguistique générale. Payot.

sie ISO. (n.d.).

site ISO. (n.d.).

Smallwood, R. F. (2014). Information Governance: Concepts, Strategies, and Best Practices. Hoboken, New Jersey: Wiley.

Soler, L. (2000). Introduction à l'épistémologie. Paris: Éditions Ellipses.

Stair, R. &. (2017). Principles of information systems (13 ed.). Cengage Learning.

Steinbuch, K. (1957). Informatik: Automatische Informationsverarbeitung. Nachrichten der Gesellschaft für angewandte Mathematik und Mechanik, 10(11).

SWIFT. (2021, juillet 1). SWIFT Customer Security Controls Framework. SWIFT.

SWIFT. (n.d.). Aperçu du réseau SWIFT : Compte rendu explicatif. SWIFT.

SWIFT, Society for Worldwide Interbank Financial Telecommunication. (2022). Customer Security Controls Framework (CSCF) (Version 2022). La Hulpe, Belgique: SWIFT.

Tardieu, H. e. (1991). Le triangle stratégique : Stratégie, structure et technologie de l'information. Paris: Éditions d'Organisation.

Teneau, G. •.-G. (2009). Guide commenté des normes et référentiels . Editions d'Organisation .

The Institute of Internal Auditors (IIA). (2017). Normes internationales pour la pratique professionnelle de l'audit interne. Altamonte Springs, FL: The IIA (Institute of Internal Auditors). Retrieved from https://www.theiia.org/en/standards/

Traoré, I., & Zeroual, M. (2023). La sécurité des systèmes d'information dans les organisations : Enjeux et perspectives. Revue Algérienne de Management et d'Informatique, 12(1), 45–60.

Universalis, E. (n.d.). Système d'information. Retrieved from Encyclopædia Universalis: https://www.encyclopedie-universalis.fr

von Bertalanffy, L. (1968). General system theory: Foundations, development, applications. Rev. ed.

Wacheux, F. (1996). L'épistémologie des sciences sociales.

Watkins, A. C. (2019). Information Security Risk Management for ISO 27001/ISO 27002 (3 ed.). IT Governance Publishing.

Wiseman, C. (1988). Strategic information systems: A management perspective. Englewood Cliffs, NJ: Prentice-Hall.

Yatchinovsky, A. (2000). L’approche systémique en psychologie sociale. Dunod.

Yin, R. K. (2016). Qualitative research from start to finish (2 ed.). New York, NY: The Guilford Press.

Zeroual, M. (2021). La gestion de la sécurité des systèmes d'information : Approches et pratiques. El-Hadi Flici.

ANNEXES

Annexe 1: CHECK-LIST ISO 27001/2022

CHECK-LIST ISO 27001/2022

ORGANISATION : **DSSI – Banque Extérieure d'Algérie (BEA)**

DATE DE L'AUDIT : 06/04/2025

AUDITEUR : ETUDIENTS KHEDIRI ESRA ; CHIBAN AMANI

VERSION DU DOCUMENT: V1.0 – Check-list d'audit interne ISO/IEC 27001:2022 – DSSI BEA

TYPE DE DOCUMENT : Check-list d'audit interne – ISO/IEC 27001:2022

RÉFÉRENTIEL : ISO/IEC 27001:2022 – Annexe A (contrôles)

ISO 27001 :2022 clauses	Exigences	QUESTIONS D'ÉVALUATION	Réponses oui/non.	Preuve	Responsabilités	SCORE
4.Contexte de l'organisation	**4.1Compréhension de l'organisation et de son contexte**	Les menaces externes (cybermenaces ciblant SWIFT) impactant la sécurité des opérations bancaires ont-ils été identifiés et documentés ?	NON	AUCUN Registre des menaces SWIFT	DSSI	0
	4.2Compréhension des besoins et attentes des parties intéressées	Un plan de remédiation priorisé en fonction des risques, formalisé par écrit et validé par le DSSI, est-il disponible (protection des transactions internationales, vérification des partenaires externes) ?	OUI	Plan de remédiation SWIFT validé	DSSI	3

ISO 27001 :2022 clauses	Exigences	QUESTIONS D'ÉVALUATION	Réponses oui/non.	Preuve	Responsabilités	SCORE
		Les besoins et attentes des parties prenantes ont-ils été formalisés ?	OUI	Cahiers de charge, commandes.	DSSI	3
		Les exigences contractuelles (SLA des fournisseurs) des parties prenantes ont-elles été déterminées ?	OUI	Contrat avec les fournisseurs	DSSI	3
	4.3 Détermination du périmètre du système de management de la sécurité de l'information (SMSI)	Le périmètre de l'ISMS est-il formalisé par écrit et approuvé par la direction (inclusion des systèmes PCI-DSS, exclusion des archives hors ligne) ?	NON	entretiens avec le directeur des auditeurs Charte ISMS non signée	Direction des auditeurs	0
5. Leadership	**Engagement de la direction**	La politique de sécurité intègre-t-elle les directives PCI-DSS ET CSP-SWIFT ?	OUI	Politique de sécurité v3.0	DSSI	3
	Politique de sécurité	La politique de sécurité de l'information fournit-elle un cadre pour définir des objectifs et démontre-t-elle l'engagement en faveur de l'amélioration	OUI	politique de sécurité documenté complète.	DSSI	3

		continue du SMSI ?				
		Une politique de sécurité documentée est définie, communiquée à tous les employés, et révisée au moins une fois par an.	OUI	Entretiens avec le DSSI Publication intranet	DSSI	1
	Rôles et responsabilités	Les rôles et responsabilités en matière de sécurité de l'information sont-ils communiqués et compris ?	OUI	Organigramme sécurité mis à jour.	RH DSSI	3

7. Support	**Ressource**	Avez-vous identifié et mis en place les ressources nécessaires au bon fonctionnement du SMSI ?	OUI	Budget ISMS 2025	DSSI	2
	Compétence	L'organisation a-t-elle conservé des preuves tangibles (certifications, quiz post-formation) pour démontrer que les personnes clés (Risk Manager, Admin SWIFT) possèdent les compétences nécessaires ?	OUI	Planning de formation	DSSI	2
	Sensibilisation	Une formation spécifique aux risques SWIFT est-elle obligatoire pour les administrateurs SWIFT ?	OUI	Formation SWIFT dispensée 2022	DSSI	0

9 Évaluation des performances	**Audit interne**	Les écarts constatés lors des audits sont-ils priorisés et corrigés dans les 60 jours	OUI	CSCF / CSP-SWIFT	DSSI / DSI / Admin SWIFT	3

	Revue de direction	la fréquence des audits sur les contrôles CSP-Swift est-elle mentionnée?	OUI	Chaque 06 mois	DSSI	3

10 Amélioration	**Amélioration continue**	L'organisation améliore-t-elle continuellement l'adéquation, la pertinence et l'efficacité de l'SMSI ?	NON	SMSI Obsolète	RSSI	0
	Non-conformité et action corrective	L'organisation prend-elle des mesures pour contrôler et corriger les non-conformités ?	OUI	Registre non-conformités	RSSI	2
		L'organisation prend-elle des mesures pour éliminer la cause racine ?	OUI	Rapport d'audit	RSSI	2

Annexe 2 : Contrôle ANNEXE A ISO 27001 : 2022

ISO 27001 :2022 Control	Control Description	QUESTION D'ÉVALUATION	Réponses oui/non.	Preuve	Responsabilités	notation
13.1 Gestion de la sécurité des réseaux **A.13.1.1** Protection des communications	Isoler les systèmes SWIFT (MT940, MT950) du reste du SI via des VLAN, Security Groups	Une segmentation stricte (VLAN, Security Groups, NACL) est-elle appliquée entre les zones SWIFT et le reste du SYSTEME ?	OUI	DIAGRAMME De VLAN	RSSI	3
		Les systèmes SWIFT sont-ils isolés dans une VLAN dédiée, avec Gateway dédiée?	OUI	Architecture on promise	RSSI	3
12.6.1 Gestion des vulnérabilités techniques / **A.10.1.1 Chiffrement des données**	Chiffrement AES-256 des messages SWIFT	Les instances EC2 SWIFT sont-elles Patchée via Système Manager Patch Manager,(OFFLINE) ?	OUI	Configuration validée via CSCFSWIFT.	Admin SWIFT	3
		Les données SWIFT (EBS, RDS Oracle) sont-elles chiffrées avec des clés de chiffrage prive par la BANQUE BEA ?	OUI	Configuration valide via CSCFSWIFT	Admin SWIFT	3
A.11.1.1 Zones sécurisées (Périmètre de sécurité physique)	Restrictions d'accès physique aux serveurs SWIFT	Les serveurs SWIFT sont-ils hébergés dans des data center prive certifiés PCI-DSS ?	OUI	Liste badges, accès salle serveurs	RESPONSABLE DATA CENTERS	1
11.1.2 : Contrôles physiques des accès						
11.1.4 : Protection contre les menaces extérieures et environnementales		Les rapports SOC sur la sécurité physique des data center sont-ils consultés et validés annuellement ?	NON	Y PAS DES PREUVES	RESPONSABLE DATA CENTERS	0

ISO 27001 :2022 Control	Control Description	QUESTION D'ÉVALUATION	Réponses oui/non.	Preuve	Responsabilités	notation
9.1Exigences métier en matière de contrôle d'accès	Obligation d'utiliser l'Authentification (MFA) pour accéder aux systèmes SWIFT	L'authentification MFA est-elle obligatoire pour tous les accès SWIFT ?	OUI	Politique MFA, journaux d'authentification .	Admin SWIFT / RSSI	3
A.9.1.1 Gestion des droits d'accès		L'accès aux comptes SWIFT exige-t-il une authentification (MFA PAM) ?	OUI	Configuration PAM validée	RSSI	3
9.2 Gestion de l'accès utilisateur	Contrôle des comptes à privilèges dans le système d'exploitation	Les droits d'accès SWIFT sont-ils révisés trimestriellement ?	OUI	Matrice privilèges incomplète	DSI / RSSI	2
A.9.2.3 Attribution de privilèges limités aux utilisateurs (accès admin).		Les comptes à privilèges (Admin/DBA) sont-ils désactivés automatiquement après 90 jours d'inactivité ?	OUI	POLITIQUE DE SECURITE SWIFT	DSI / RSSI	3
12.4 Journalisation et surveillance	Journalisation et audit des transactions SWIFT Centralisation des logs SWIFT (VPC Flow Logs, RDS, MQ) dans des outils comme PAM.	Les logs SWIFT (VPC Flow Logs, RDS, MQ) sont-ils centralisés et analysée VIA SYSTEME DE MONITORING ?	OUI	LOGS DE SYSTEME PAM	RSSI	3
12.4.1 : Surveillance des logs via SYSTEME DE MONITORING pour détecter les anomalies.		Des alertes sont-elles générées pour les tentatives de connexion échouées (seuil > 3/tentatives) ?	OUI	LOGS DE SYSTEME PAM	RSSI / DSI	3
A.12.6.1 Surveillance des activités						
6.1 Évaluation des risques liés à la sécurité de l'information	Évaluation des risques fondée sur des scénarios	Des scénarios de fraude SWIFT (altération de MT103) ont-ils été modélisés ?	NON	Scénarios tests MEHARI		0

ISO 27001 :2022 Control	**Control Description**	**QUESTION D'ÉVALUATION**	Réponses oui/non.	Preuve	Responsabilités	notation
A.6.1.2 Gestion des risques (analyse et traitement)						

Annexe 3 : Mentions légales des documents consultés

Copyright	**Confidentialité**	**Avis de non-responsabilité**	**Traductions**	**Marques**
SWIFT © 2021. Tous droits réservés.	La présente publication comporte des informations confidentielles de SWIFT ou de tiers. Il est interdit de divulguer cette publication en dehors de votre organisation sans l'accord préalable écrit de SWIFT. Vous pouvez toutefois partager cette publication sur la base du besoin d'en connaître avec des tiers qui vous aident dans le cadre des initiatives du programme de sécurité des clients de SWIFT, à condition (i) que vous informiez le destinataire de la nature confidentielle des informations et (ii) que vous vous assuriez qu'il est lié par des obligations de confidentialité non	Les informations figurant dans la présente publication sont susceptibles d'être modifiées à tout moment. Vous devez toujours consulter la dernière version disponible.	La version anglaise de la documentation SWIFT est la seule version officielle et contraignante.	SWIFT est le nom commercial de S.W.I.F.T. SCRL. Les éléments ci-après sont des marques déposées de SWIFT : • 3SKey, Innotribe, MyStandards, • Sibos, • SWIFT, SWIFTNet, • SWIFT Institute, • Le logo du Forum des normes, • Le logo SWIFT, • SWIFT gpi avec logo, • Le logo SWIFT gpi et UETR. • Les autres noms de

	moins strictes.			produit, de service ou d'entreprise figurant dans cette publication sont des noms commerciaux, • Des marques commerciales ou des marques déposées de leurs propriétaires respectifs.