



RÉPUBLIQUE DU BÉNIN
MINISTÈRE DE L'ENSEIGNEMENT SUPÉRIEUR
ET DE LA RECHERCHE SCIENTIFIQUE

UNIVERSITÉ D'ABOMEY-CALAVI

INSTITUT DE FORMATION ET DE
RECHERCHE EN INFORMATIQUE

BP 526 Cotonou Tel : +229 21 14 19 88
<http://www.ifri-uac.net> Courriel : contact@ifri.uac.bj



MÉMOIRE

pour l'obtention du

Diplôme de Master en Informatique

Option : Sécurité Informatique

Présenté par :

Jospy K. B. GOUDALO

Évaluation et renforcement de la sécurité du système d'information de la Caisse Autonome de Gestion de la Dette (CAGD)

Sous la supervision :

Dr Amadou Tidjani SANDA MAHAMA

Ing Hervé M. AKAPKO

Membres du jury :

AHOUCANDJINOUE Arnaud	Docteur	IFRI	Président
ASSOGBA Emery	Docteur	IFRI	Examineur
SANDA MAHAMA Tidjani	Docteur	IFRI	Rapporteur

Année Académique : 2023-2024

Sommaire

Dédicace	ii
Remerciements	iii
Résumé/Abstract	iv
Liste des Figures	vi
Liste des Tableaux	vii
Sigles et Abréviations	viii
Introduction	1
1 Revue de littérature	3
2 Méthodologie d'évaluation	18
3 Résultats & Recommandations	31
Conclusion	43
Bibliographie	44
Webographie	45
Table des matières	47

Dédicace

A ma famille.

Remerciements

Je souhaite exprimer ma plus profonde gratitude et adresser mes remerciements les plus chaleureux à toutes les personnes qui ont contribué, de près ou de loin, à la réalisation de ces travaux :

- **M. Eugène C. EZIN**, Directeur de l'Institut de Formation et de Recherche en Informatique (IFRI), dont l'attention bienveillante, la disponibilité constante et les orientations précieuses ont été essentielles tout au long de ce parcours.
- **M. Amadou Tidjani SANDA MAHAMA**, mon Maître de mémoire, pour son engagement indéfectible, ses conseils éclairés et ses orientations déterminantes, qui ont grandement enrichi mon travail.
- **M. Hervé M. AKAPKO**, Chef du Département des Systèmes d'Information de la CAGD pour son accompagnement et son mentoring inspirant, qui ont apporté une valeur inestimable à ce projet.
- **L'ensemble de l'administration et des enseignants de l'IFRI**, pour la qualité exceptionnelle de la formation reçue et leur soutien tout au long de mon parcours académique.

Je n'oublie pas également **vous, chers lecteurs**, dont l'intérêt et la lecture de ces lignes témoignent de l'importance que vous accordez à ce travail.

Résumé

Dans un contexte où les systèmes d'information jouent un rôle crucial dans la gestion des données stratégiques et financières, la sécurité informatique de la Caisse Autonome de Gestion de la Dette ([CAGD](#)) est essentielle. L'institution gère des données sensibles liées à la dette publique et fait face à des menaces croissantes. Une évaluation rigoureuse est donc nécessaire pour garantir la robustesse et la conformité de ses dispositifs de sécurité. L'audit réalisé s'est appuyé sur la Politique de Sécurité des Systèmes d'Information de l'État (PSSIE) et la norme [ISO/CEI 27001](#). Il a permis d'identifier les écarts entre les pratiques actuelles et les exigences de ces référentiels. Les analyses techniques approfondies, les revues documentaires et les entretiens stratégiques ont révélé plusieurs faiblesses. Ces failles concernent notamment la gestion des risques, la sécurisation des flux et les politiques d'accès. Ces travaux ont conduit à des recommandations concrètes et adaptées pour renforcer la posture de sécurité de la [CAGD](#). Ce travail a permis d'améliorer la protection des actifs critiques de l'institution et de sensibiliser les équipes aux enjeux de cybersécurité. En intégrant ces mesures dans une stratégie globale, la [CAGD](#) renforce sa résilience face aux cybermenaces et assure également une conformité durable avec la [PSSIE](#) et l'[ISO/CEI 27001](#).

Mots clés : Audit de sécurité, systèmes d'information, [PSSIE](#), [CAGD](#), vulnérabilités, cybersécurité, gouvernance.

Abstract

In a context where information systems play a crucial role in managing strategic and financial data, the cybersecurity of the Autonomous Debt Management Agency ([CAGD](#)) is essential. The institution handles sensitive data related to public debt and faces increasing threats. A rigorous assessment is therefore necessary to ensure the robustness and compliance of its security measures. The audit conducted was based on the State Information Systems Security Policy ([PSSIE](#)) and the [ISO/ 27001](#) standard. It identified gaps between current practices and the requirements of these frameworks. In-depth technical analyses, document reviews, and strategic interviews revealed several weaknesses, particularly in risk management, data flow security, and access policies. This work resulted in concrete and tailored recommendations to strengthen the [CAGD](#)'s security posture. It improved the protection of the institution's critical assets and raised awareness among teams about cybersecurity challenges. By integrating these measures into a comprehensive strategy, the [CAGD](#) enhances its resilience against cyber threats and ensures sustained compliance with the [PSSIE](#) and [ISO/ 27001](#).

Key words: Security audit, information systems, [PSSIE](#), [CAGD](#), vulnerabilities, cybersecurity, governance.

Liste des Figures

1.1	Cycle de vie d'un audit de sécurité	4
1.2	Démarche d'audit des systèmes d'informations.	5
1.3	Méthodologie EBIOS [20]	7
1.4	Méthodologie MEHARI [20]	8
1.5	Méthodologie OCTAVE [20]	8
1.6	Le processus du système de management.	14
1.7	La roue de Deming[17]	16
2.1	Architecture réseau de la CAGD	25
3.1	Taux de maturité global PSSIE	31
3.2	Taux de maturité global ISO 27001	31
3.3	Tableau récapitulatif des niveaux de maturité PSSIE.	32
3.4	Tableau récapitulatif des niveaux de maturité ISO.	32

Liste des Tableaux

1.1	Tableau comparatif de mise en œuvre des trois solutions EBIOS, MEHARI et OC-TAVE[20]	9
1.2	Tableau récapitulatif de la Famille de la norme ISO/CEI 27k	12
1.3	Historique des normes en matière de sécurité de l'information	14
2.1	Planning de la mission	21

Sigles et Abréviations

ACL :	Access Control List 24 , 39 ,
ASSI :	Agence de la Sécurité des Systèmes d'Information 24 ,
BSI :	British Standards Institution 10 ,
CAA :	Caisse Autonome d'Amortissement 18 ,
CAGD :	Caisse Autonome de Gestion de la Dette iv , v , 1 , 2 , 18–24 , 30 , 32 , 33 , 42 , 43 , 48 ,
CEI :	Commission Electrotechnique Internanationale iv , vii , 9–12 , 48 ,
CLUSIF :	Club de la Sécurité de l'information Français 7 ,
CMMI :	Capability Maturity Model Integration 28 ,
DCSSI :	Direction Centrale de la Sécurité des Systèmes d'Information 7 ,
DMZ :	Demilitarized Zone 39 ,
EBIOS :	Expression des Besoins et Identification des Objectifs de Sécurité vi , vii , 3 , 7 , 9 , 47 ,
GDPR :	Règlement Général sur la Protection des Données 13 , 48 ,
GLPI :	Gestionnaire Libre de Parc Informatique 40 ,
IDS :	Intrusion Detection System 26 , 36 ,
IFRI :	Institut de Formation et de Recherche en Informatique
IP :	Internet Protocol 6 ,
IPS :	Intrusion Prevention System 26 , 36 ,
IPsec :	Internet Protocol Security 39 ,
ISO :	International Organization for Standardization iv , v , vii , 3 , 9–12 , 14 , 16 , 17 , 47 , 48 ,
IT :	Information Technology 13 , 33 ,
ITIL :	Information Technology Infrastructure Library 13 , 48 ,
LAN :	Local Area Network 24 ,

MEHARI :	Méthode Harmonisée d'Analyse des Risques vi , vii , 3 , 7–9 , 47 ,
MFA :	Multi-Factor Authentication 37 ,
NIST :	National Institute of Standards and Technology 12 , 48 ,
OCTAVE :	Operationally Critical Threat, Asset and Vulnerability Evaluation vi , vii , 7–9 , 47 ,
OHSAS :	Occupation Health and Safety Assessment Series 14 ,
P2P :	Peer to Peer 40 ,
PCI :	Plan de Continuité Informatique 33 ,
PCI DSS :	Payment Card Data Security Standard
PDCA :	Plan Do Check Act 16 , 17 , 48 ,
PSSI :	Politique de Sécurité des Systèmes d'Information 13 , 16 , 17 , 48 ,
PSSIE :	Politique de Sécurité des Systèmes d'Information de l'État iv , v , 21 , 22 , 30 , 48 ,
SEI :	Software Engineering Institute 8 ,
SI :	Système d'Information 1 , 3 , 17 , 23 , 27 , 30 , 33 , 34 , 37–39 , 49 ,
SLA :	Service Level Agreement 33 ,
SMSI :	Système de Management de la Sécurité de l'Information 10–12 , 15–17 , 48 ,
SNSN :	Stratégie Nationale de Sécurité Numérique 21 ,
SOC :	Security Operation Center 34 ,
SQL :	Structured Query Language 35 , 36 ,
SSH :	Secure Shell 39 ,
SSI :	Sécurité des Systèmes d'Information 17 ,
USA :	United States of America 8 ,
XSS :	Cross-Site Scripting 35 , 36 ,

Introduction

Le paysage numérique se marque par une prolifération des cyberattaques, dont la sophistication et la fréquence ne cessent de croître. La complexité croissante des systèmes d'information, l'interconnexion des réseaux et la multiplication des points d'accès constituent autant de vulnérabilités que les cybercriminels exploitent pour mener des attaques de plus en plus audacieuses. Cette menace grandissante pèse lourdement sur tous les systèmes d'information notamment celles des institutions financières, qui constituent des cibles privilégiées en raison de la nature sensible des données qu'elles traitent. Les conséquences de ces intrusions peuvent être dévastatrices, se traduisant par des pertes financières conséquentes, des atteintes à la réputation et des interruptions de service pouvant impacter l'économie toute entière. Dans ce contexte, un audit de la sécurité du système d'information se révèle être une stratégie cruciale pour détecter les insuffisances afin de prévenir et répondre efficacement aux menaces de sécurité. Ce mémoire se focalise de façon générale sur la réalisation de cet audit et sur la prise en compte des recommandations effectuées.

1 Contexte et justification

La Caisse Autonome de Gestion de la Dette ([CAGD](#)) joue un rôle crucial dans la gestion de la dette et des finances publiques, ce qui en fait une entité stratégique au sein du paysage financier national. Avec l'essor des cybermenaces et des attaques informatiques sophistiquées, la sécurité de son système d'information est devenue une priorité absolue. Les récents incidents de sécurité dans le domaine financier ont mis en lumière plusieurs risques potentiels auxquels les institutions telles qu'elles sont exposées, nécessitant une évaluation approfondie de leurs dispositifs de sécurité informatique. Le manque d'informations sur les vulnérabilités actuelles du système d'information et la nécessité d'améliorer la sécurité et la fiabilité constituent les principales motivations de cette recherche. Cette étude se concentre sur une analyse exhaustive des dispositifs de sécurité du système d'information de la [CAGD](#), visant à identifier ses insuffisances.

Afin de garantir que le système d'information respecte les exigences recommandées, un audit interne de sécurité a été commandité. Les résultats de cet audit permettront de formuler des recommandations concrètes pour renforcer la sécurité du [SI](#), ainsi que de sensibiliser les acteurs concernés aux enjeux de sécurité inhérents à leur quotidien.

2 Problématique

La problématique centrale de cette étude réside dans l'analyse approfondie des dispositifs de sécurité du système d'information de la [CAGD](#) pour identifier les vulnérabilités et proposer des mesures de sécurité efficaces. Quelles sont les vulnérabilités spécifiques auxquelles elle est exposée, et quelles stratégies peut-elle mettre en place pour renforcer sa résilience face aux cyberattaques ?

Notre travail est donc d'auditer la sécurité du système d'information et de proposer des mesures adaptées pour renforcer sa protection. L'enjeu est de taille, car il s'agit de garantir un environnement de travail sûr et sécurisé pour les employés, tout en préservant la confidentialité des données et en prévenant d'éventuelles attaques. Cette étude se positionne donc comme une contribution significative à la sécurité des systèmes d'information de la [CAGD](#), en offrant une perspective approfondie et une approche proactive pour relever les défis actuels et futurs.

3 Objectifs de l'étude

Objectif général

L'objectif général de notre travail est d'évaluer et de renforcer la sécurité du système d'information de la Caisse Autonome de Gestion de la Dette (CAGD).

Objectifs spécifiques

Pour atteindre cet objectif, les objectifs spécifiques suivants seront poursuivis :

- Vérifier si le système d'information de la [CAGD](#) respecte les exigences définies par la Politique de Sécurité des Systèmes d'Information de l'État et la norme ISO 27001.
- Détecter les failles de sécurité potentielles dans le système d'information, y compris les vulnérabilités techniques et organisationnelles.
- Proposer des mesures correctives pour remédier aux non-conformités et renforcer la posture de sécurité du système d'information.
- Prendre en compte les dites recommandations.
- Éduquer les parties prenantes sur les bonnes pratiques en matière de sécurité et les risques potentiels identifiés au cours de l'audit.

4 Organisation du mémoire

Le présent mémoire se divise en trois chapitres. Le premier chapitre est une revue de littérature qui explore les concepts généraux par rapport aux audits et les systèmes de management de la sécurité de l'information (SMSI). Le deuxième chapitre se concentre sur notre méthodologie d'évaluation. Le troisième chapitre traite des résultats obtenus et des recommandations formulées.

Revue de littérature

Introduction

Ce chapitre offre un aperçu des principes clés des audits de sécurité des systèmes d'information, en mettant en avant leur importance, leur objectif et leur mise en œuvre. Nous abordons brièvement les méthodes et normes d'audit telles que la méthode [EBIOS](#), [MEHARI](#) et les normes [ISO](#) et enfin les systèmes de management en sécurité de l'information. En comprenant ces concepts et pratiques, il nous est plus facile de les mettre en place pour protéger les systèmes d'information contre les menaces potentielles.

1.1 Généralités sur les audits

1.1.1 Définition d'un audit

L'audit de sécurité d'un Système d'Information ([SI](#)) est un processus systématique et méthodique visant à évaluer l'efficacité des contrôles de sécurité mis en place pour protéger les actifs informationnels d'une organisation. Il consiste à faire un bilan complet du [SI](#), en analysant ses composants, ses interactions, ses mesures de sécurité et ses risques. C'est un rapport détaillé qui permet à l'entreprise de connaître les zones vulnérables exposées aux cybercriminels.[9]

1.1.2 Rôle et objectif

L'audit de sécurité examine les différents aspects de la sécurité informatique, y compris les politiques de sécurité, les contrôles d'accès, la gestion des identités, la protection des données, la surveillance des systèmes, etc. L'audit, qu'il soit interne ou externe, son but reste de juger la gestion de la sécurité de l'information et l'accomplissement de ses objectifs. En une phrase, il identifie les risques de sécurité, évalue les contrôles en place et recommande des mesures pour renforcer la sécurité du [SI](#) tout en assurant la conformité aux normes et aux réglementations applicables.

1.1.3 Cycle de vie d'un audit de sécurité des systèmes d'information

Le processus d'audit de sécurité est un processus répétitif et perpétuel. Il décrit un cycle de vie schématisé sur la figure suivante :

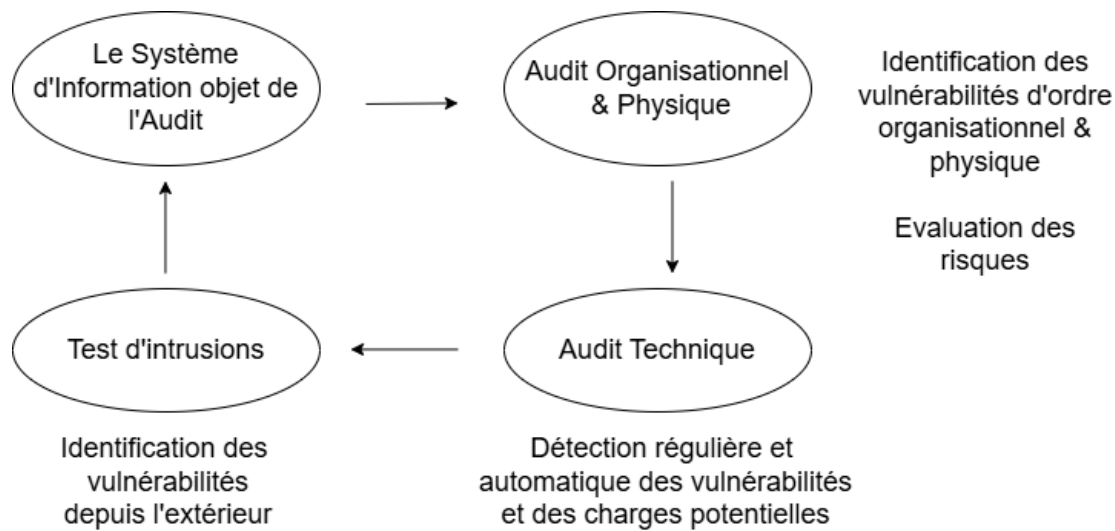


FIGURE 1.1 : Cycle de vie d'un audit de sécurité
[10]

L'audit de sécurité informatique se présente essentiellement suivant deux parties :

- L'audit organisationnel et physique.
- L'audit technique.

Une troisième partie optionnelle peut être également considérée. Il s'agit de l'audit Intrusif (test d'intrusions). A l'issue de ces étapes, un rapport qui présente la synthèse de l'audit est établi. Il contient également les recommandations à mettre en place pour corriger les défaillances organisationnelles ou techniques constatées.

1.1.4 Démarche de réalisation

La démarche va s'appuyer sur un processus général qu'il faut ensuite adapter aux spécificités de chaque mission. L'audit peut être réalisé à l'interne par le personnel de l'organisme ou en ayant recours à des auditeurs externes. Cette démarche comporte cinq (05) différentes phases :

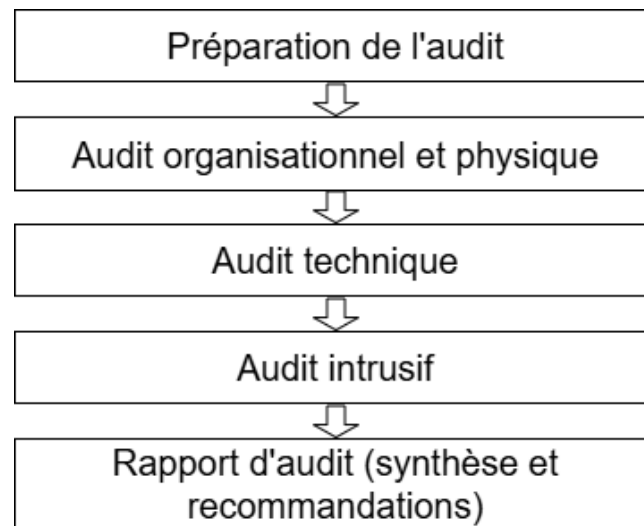


FIGURE 1.2 : Démarche d’audit des systèmes d’informations.

[11]

1.1.4.1 Définition de la charte d’audit

C’est un document de référence permettant au responsable d’audit et à la fonction d’audit interne de s’acquitter efficacement de leurs responsabilités au sein de l’organisation. Elle est souvent établie par le département d’audit interne ou par un comité d’audit indépendant et approuvée par la direction de l’organisation.

1.1.4.2 Préparation de l’audit

C’est une phase qui comprend toutes les activités qui doivent être réalisées avant le début de l’audit. Elle se manifeste par des rencontres entre auditeurs et responsables de l’entité à auditer. Les composantes habituelles comprennent généralement les éléments suivants :[12]

- les objectifs de l’audit;
- la portée de l’audit comprenant les domaines d’activité à évaluer et le niveau de détail de l’évaluation par l’auditeur;
- la façon dont sera documenté l’audit;
- le calendrier d’audit détaillé comprenant les services évalués, sur combien de temps, etc.

Chaque membre de l’équipe informatique d’audit se prépare à l’exécution avec un accès à la liste de contrôle de vérification. Celle-ci permet de guider l’auditeur afin de n’oublier aucun détail à évaluer.

1.1.4.3 Audit organisationnel et physique

Il représente une approche méthodologique basée sur l’identification des vulnérabilités, des lacunes de sécurité, des inefficacités et des risques potentiels liés aux systèmes d’information afin de proposer des recommandations pour les améliorer et les sécuriser. Le jeu de question, qui peut être énoncé, est de type : Qui s’occupe des sauvegardes ? Comment sont-elles planifiées ? Qui a accès à la salle des serveurs ? Qu’est ce qui est prévu en cas de panne de courant ? Ces questions sont classées par thèmes ou par domaine de sécurité à savoir sécurité physique, contrôle d’accès, pannes et erreurs humaines,

etc...

Tout ceci permet d'analyser les politiques et les procédures mises en place par l'organisation dans le but de vérifier leur conformité soit aux contraintes réglementaires de leur marché soit aux exigences de sécurité de l'organisation.

1.1.4.4 Audit technique

Cette phase de l'audit suit celle de l'audit organisationnel. L'audit technique, se base sur les vérifications des configurations du SI (systèmes, équipements réseaux, etc.), les confronte aux politiques de sécurité internes, aux exigences normatives et aux bonnes pratiques des éditeurs.

On distingue trois familles d'audit technique[13] :

- **Audit d'architecture réseau** : Il s'agit de vérifier si l'architecture mise en place répond aux exigences de sécurité de l'entreprise.
- **Audit de configuration des systèmes et réseaux** : Il est important car il permet de voir si ce qui est établi en architecture est effectivement ce qui est mis en place.
- **Audit d'architecture du Système d'Information** : Il évalue les interactions entre sous-systèmes du SI à un niveau « haut niveau », en se concentrant sur la pertinence des échanges et des séparations entre systèmes, plutôt que sur les configurations basiques.

1.1.4.5 Test d'intrusions (Audit intrusif)

Cet audit consiste à se mettre dans la peau d'un pirate (hacker) malveillant et d'essayer de pénétrer une cible donnée qui sera, dans ce cas, le client (audité). La cible peut être de différent type : une adresse IP, une application, un serveur ou encore un réseau complet. Cela permet d'apprécier le comportement du réseau face à des attaques, et de sensibiliser également les acteurs (management, équipe informatique, utilisateurs) par des rapports illustrant les failles décelées.

1.1.4.6 Rapport de mission

Cette phase finale du processus d'audit est consacrée à la production du rapport d'audit. Les éléments de ce rapport doivent nécessairement être appuyés par des preuves consignées dans le dossier d'audit. Le rapport est de fournir aux parties prenantes, telles que la direction générale, les actionnaires et les auditeurs internes ou externes, une évaluation impartiale et détaillée de la sécurité et de la performance des systèmes d'information de l'organisation.

1.2 Méthodes et normes (Référentiels)

1.2.1 Définitions

1.2.1.1 Méthode d'audit

Une méthode d'audit est une démarche, un processus ou un ensemble de principes qui permettent d'appliquer une norme au système d'information de l'entreprise. La plupart des méthodes sont appliquées par des experts en gestion des risques.

1.2.1.2 Référentiels

Les référentiels d'audit constituent l'ensemble des normes, des méthodes et des bonnes pratiques établies par des organismes reconnus et permettant de fournir un moyen d'assurance d'une démarche sécuritaire cohérente.

1.2.2 Quelques méthodologies d'analyse des risques

Parmi les méthodologies d'analyse des risques les plus connues, nous pouvons citer de manière non exhaustive : **EBIOS**, **MEHARI** ou encore **OCTAVE**.

1.2.2.1 La méthode **EBIOS**

EBIOS est l'acronyme de « Expression des Besoins et Identification des Objectifs de Sécurité ».

C'est une méthode publiée par la Direction Centrale de la Sécurité des Systèmes d'Information (**DCSSI**) en France en 1995. Depuis 2018, cette méthodologie a pris un nouveau virage avec une nouvelle version, "**EBIOS** Risk Manager".

La méthode **EBIOS** Risk Manager se distingue par une approche qui réalise une synthèse entre conformité et scénarios. Elle se fonde sur un socle de sécurité solide, construit grâce à une approche par conformité. La démarche par scénarios vient solliciter ce socle face à des menaces particulièrement ciblées ou sophistiquées, qui prennent en compte l'écosystème métier et technique dans lequel l'organisation ciblée évolue.

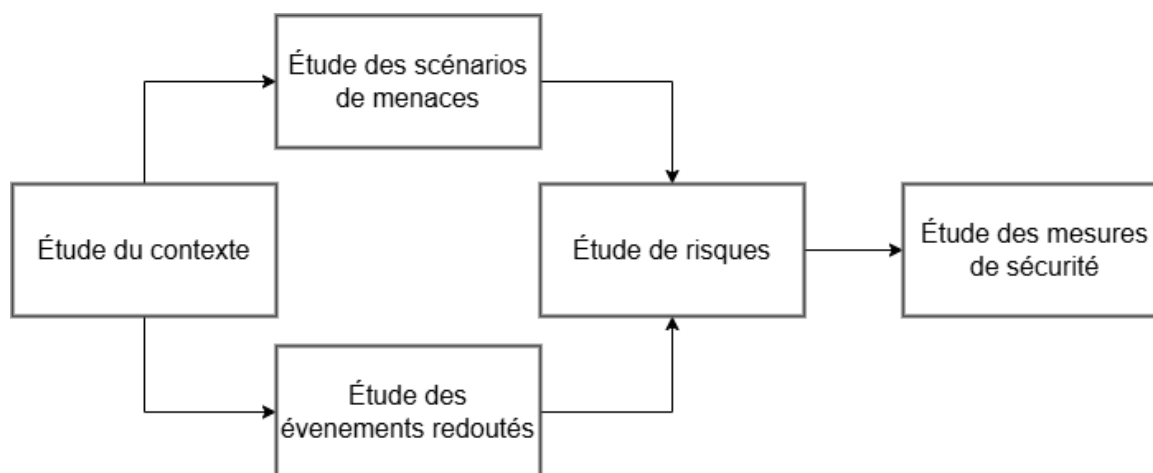


FIGURE 1.3 : Méthodologie **EBIOS** [20]

1.2.2.2 La méthode **MEHARI**

MEHARI est l'acronyme de « Méthode harmonisée d'analyse des risques ».

Elle est développée et maintenue depuis 1995 par le **CLUSIF** (Club de la sécurité de l'information français) et reprend et remplace les méthodes MELISA et MARION.

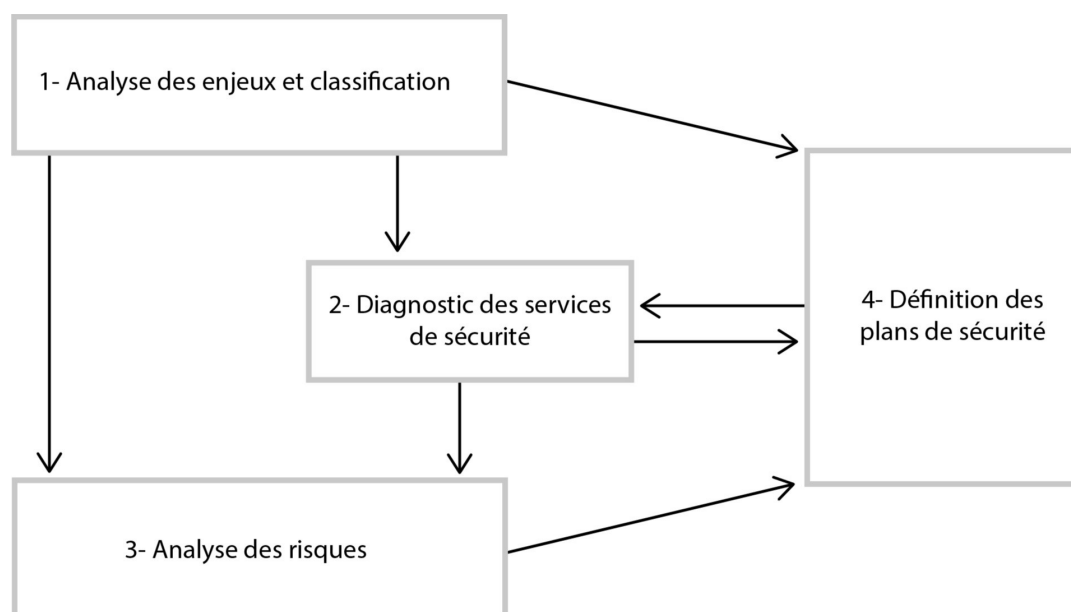


FIGURE 1.4 : Méthodologie MEHARI [20]

1.2.2.3 La méthode OCTAVE

OCTAVE est l'acronyme de « Operationally Critical Threat, Asset and Vulnerability Evaluation ». Elle fut produite par le Software Engineering Institute (SEI) de l'université Carnegie Million de Pittsburgh aux USA en 1999.

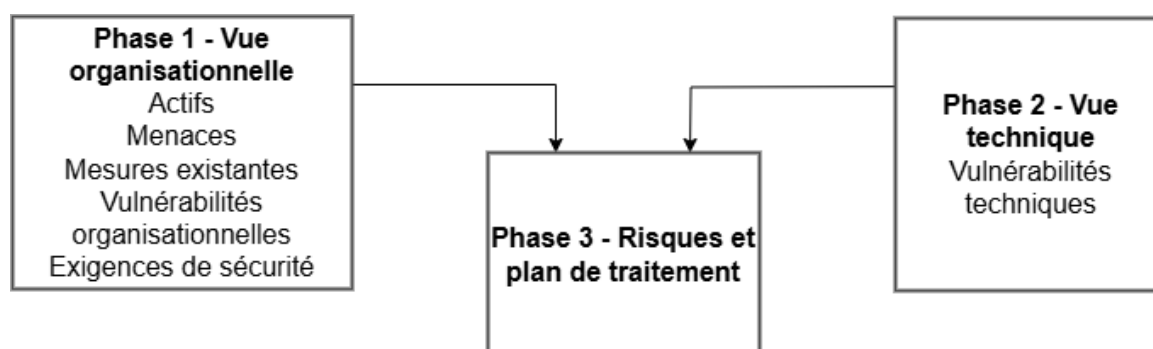


FIGURE 1.5 : Méthodologie OCTAVE [20]

Le tableau ci-dessous peut être utilisé comme référence pour choisir la méthode la plus adaptée en fonction des besoins de l'entreprise.

Ce tableau n'étant pas exhaustif, il existe également d'autres critères de choix possibles, tels que :

- La qualité de la documentation existante ;
- L'origine géographique (la culture d'un pays influe sur le fonctionnement interne de l'organisme) ;
- La langue utilisée (il est primordial de maîtriser parfaitement les concepts employés) ;
- La taille de l'organisme ;
- Les ressources humaines et matérielles nécessaires.

	OCTAVE	MEHARI	EBIOS
Documentation	Disponible en téléchargement gratuit	Disponible en téléchargement gratuit	Disponible en téléchargement gratuit
Outil	Logiciel d'appui à la démarche payant	Manuel de base inclus et gratuit. Outil additionnel développé par le CLUSIF	Logiciel en téléchargement gratuit
Objectif	Analyse de risques	Analyse de risques Tableau de bord Indicateurs Maturité SSI	Analyse de risques Maturité SSI
Complexité d'implémentation	Élevée : Convient aux petites structures, aide externe recommandée	Medium : Demande un logiciel et des feuilles de calcul dédiées	Nulle : Club d'experts et base de connaissances à disposition

TABLE 1.1 : Tableau comparatif de mise en œuvre des trois solutions [EBIOS](#), [MEHARI](#) et [OCTAVE](#)^[20]

1.2.2.4 L'ISO (Organisation Internationale de Normalisation)

L'Organisation Internationale de Normalisation, dont le siège est à Genève, élabore et publie des normes [ISO](#). Elle compte 165 organismes nationaux de normalisation du monde entier. L'objectif des normes [ISO](#) est de définir les meilleures pratiques à suivre, de la fabrication des biens aux processus de gestion. Depuis 1946, elle facilite les échanges et la coopération entre les personnes et les entreprises dans le monde entier. Différents secteurs utilisent les normes [ISO](#) pour adopter des solutions cohérentes aux défis opérationnels. Les documents normalisés [ISO](#) sont séquencés numériquement en « familles ».

1.2.2.5 Les normes

Une norme, selon le guide [ISO/CEI](#), est « un document établi par consensus et approuvé par un organisme reconnu, qui fournit des règles, lignes directrices ou caractéristiques pour des activités ou résultats, garantissant un niveau d'ordre optimal dans un contexte donné ». Comparable à une formule décrivant la meilleure pratique, elle s'applique à la fabrication, la gestion, la prestation de services ou la fourniture de matériel. Les normes, basées sur les connaissances d'experts, répondent aux besoins des fabricants, distributeurs, utilisateurs, associations, consommateurs et organismes de réglementation.

On distingue quatre familles de normes :

- **Les normes fondamentales** qui concernent les règles qui ont trait à la métrologie.
- **Les normes de spécifications** qui traitent des caractéristiques et des seuils de performance d'un produit ou d'un service
- **Les normes d'analyse et d'essais** qui renseignent sur les méthodes et moyens pour la réalisation d'un essai sur un produit
- **Les normes d'organisation** qui décrivent les fonctions et les relations organisationnelles au sein d'un organisme

1.2.2.6 Historique des normes en matière de sécurité de l'information [4]

Au cours des vingt dernières années, les normes liées à la sécurité de l'information ont connu de nombreuses évolutions et remplacements. Ces changements ont parfois rendu la compréhension du cadre normatif complexe. Un rappel historique de ces évolutions permet de mieux appréhender la situation actuelle.

- **Années 1990** : Au début des années 1990, plusieurs grandes entreprises britanniques se sont concertées pour établir des mesures visant à sécuriser leurs échanges commerciaux en ligne. Cette collaboration a produit une référence précieuse pour d'autres entreprises cherchant à mettre en place des mesures similaires. Le Département des Transports et de l'Industrie britannique a soutenu cette initiative en supervisant la rédaction d'un projet de norme de gestion de la sécurité de l'information au format du **BSI**.
- **1991** : Un projet de code de bonnes pratiques, connu sous le nom de « **best practices** », a été lancé. Il recommandait la formalisation d'une politique de sécurité de l'information couvrant au minimum huit points stratégiques et opérationnels, ainsi qu'une mise à jour régulière de cette politique.
- **1995** : Le **BSI** publie la norme **BS7799**, qui rassemble dix chapitres avec plus de 100 mesures détaillées pour la sécurité de l'information. Ces mesures sont adaptées en fonction des besoins spécifiques de chaque organisation.
- **1998** : La norme **BS7799** est modifiée et renommée **BS7799-1**, tandis qu'une nouvelle norme, **BS7799-2**, est introduite. Cette dernière précise les exigences pour la mise en place d'une politique de sécurité de l'information et repose sur une approche de gestion des risques et le management de la sécurité de l'information.
- **2000** : **BS7799-1** est internationalisée sous le nom **ISO/ 17799 :2000**, après avoir suivi un processus de concertation internationale et quelques ajustements. Elle devient la norme de référence pour les organisations cherchant à renforcer leur sécurité de l'information.
- **2002** : Le **BSI** fait évoluer la norme **BS7799-2** en s'inspirant des normes **ISO 9001 :2000** et **ISO 14001 :1996**, adoptant une approche de management de la sécurité de l'information.
- **2005** : L'**ISO** adopte **BS7799-2** sous la nouvelle référence **ISO/ 27001 :2005**, avec des modifications pour se rapprocher du principe de « système de management » des normes **ISO 9001** et **ISO 14001**. **ISO/ 27001 :2005** spécifie les exigences pour la mise en place d'un Système de Management de la Sécurité de l'Information (**SMIS**). À cette époque, la sécurisation des systèmes d'information et la réduction des risques sont devenues cruciales, faisant de **ISO 27001 :2005** l'une des normes les plus prisées de l'**ISO**.
- **2007** : Dans un souci de clarification, l'**ISO** renomme **ISO/CEI 17799 :2005** en **ISO/CEI 27002**, intégrant cette norme à la famille des normes **ISO/CEI 2700x** en développement.

1.2.2.7 La série des normes de la famille **ISO 27000** [4]

La série des normes **ISO 27000** est une série de bonnes pratiques concernant la mise en œuvre, la maintenance et la gestion des Systèmes de Management de la Sécurité de l'Information (**SMIS**). Cette série vise à établir les meilleures pratiques concernant différents aspects liés à la gestion de la sécurité

de l'information, en mettant l'accent sur l'amélioration continue et l'atténuation des risques. Elle comprend les normes de sécurité de l'information publiées conjointement par l'ISO et la CEI.

1.2.2.8 ISO/CEI 27000

Intitulée « Systèmes de management de la sécurité de l'information — Vue d'ensemble et vocabulaire », elle fournit la base et le langage commun pour le reste des normes de la série.

1.2.2.9 ISO/CEI 27001

Intitulée « Systèmes de gestion de sécurité de l'information – Exigences », elle a été publiée en octobre 2005 et mise à jour en octobre 2022 (version que nous utilisons dans le cadre de notre évaluation). Cette norme fournit aux entreprises de toutes tailles et de tous secteurs d'activité des lignes directrices pour la mise en place, la mise en œuvre, la maintenance et l'amélioration continue d'un système de management de la sécurité de l'information.

1.2.2.10 ISO/CEI 27002

Intitulée « Code de bonnes pratiques pour la gestion de la sécurité de l'information », elle a été publiée en 2005 et mise à jour en octobre 2022. L'ISO/CEI 27002 fournit un ensemble de référence de contrôles de sécurité de l'information, de cybersécurité et de protection de la vie privée, y compris des lignes directrices de mise en œuvre basées sur les meilleures pratiques internationalement reconnues.

1.2.2.11 ISO/CEI 27003

Intitulé « Guide de mise en œuvre du système de management de la sécurité de l'information », elle a été mise à jour en octobre 2017. L'ISO/CEI 27003 fournit un guide pour la mise en œuvre correcte d'un SMSI, en se concentrant sur les aspects importants pour une mise en œuvre réussie.

1.2.2.12 ISO/CEI 27004

Intitulé « Management de la sécurité de l'information - Suivi, mesure, analyse et évaluation », elle a été mise à jour en octobre 2016. L'ISO/CEI 27004 établit le suivi et la mesure de la performance en matière de sécurité de l'information; la surveillance et la mesure de l'efficacité d'un système de management de la sécurité de l'information (SMSI), y compris de ses processus et contrôles; l'analyse et l'évaluation des résultats de la surveillance et de la mesure.

1.2.2.13 ISO/CEI 27005

Intitulé « Management du risque de la sécurité de l'information », elle a été publiée en 2008 et mise à jour en 2022. Cette norme définit la manière dont la gestion des risques liés aux systèmes de gestion de l'information doit être effectuée, en se concentrant sur la manière d'établir la méthodologie à utiliser.

1.2.2.14 ISO/CEI 27006

Intitulé « Exigences pour les organismes d'audit et de certification des systèmes de management de la sécurité de l'information », elle a été remise à jour en mars 2024. Cette norme établit les exigences

à respecter par les entreprises qui souhaitent être accréditées pour certifier d'autres entreprises en conformité avec l'ISO/CEI-27001.

1.2.2.15 ISO/CEI 27007

Intitulée « Lignes directrices pour l'audit des systèmes de management de la sécurité de l'information » et mise à jour en octobre 2020, l'ISO/CEI 27007 détaille la gestion des programmes d'audit SMSI, la réalisation des audits et les compétences requises des auditeurs. Elle complète l'ISO 19011 et s'adresse à ceux qui doivent comprendre ou réaliser des audits internes ou externes d'un SMSI ou gérer un programme d'audit.

Norme	Description
ISO/CEI 27000	Vue d'ensemble et vocabulaire pour les systèmes de management de la sécurité de l'information.
ISO/CEI 27001	Exigences relatives aux systèmes de management de la sécurité des informations (SMSI).
ISO/CEI 27002	Mesures de sécurité de l'information.
ISO/CEI 27003	Directives pour l'élaboration d'un plan de mise en œuvre du SMSI.
ISO/CEI 27004	Mesure de la performance du SMSI.
ISO/CEI 27005	Gestion des risques de sécurité de l'information.
ISO/CEI 27006	Exigences pour les organismes fournissant des services d'audit et de certification des SMSI.
ISO/CEI 27007	Directives pour l'audit et la certification des SMSI.

TABLE 1.2 : Tableau récapitulatif de la Famille de la norme ISO/CEI 27k

1.2.3 Autres cadres de sécurité de l'information

En plus des normes ISO 27000, il existe plusieurs autres cadres et référentiels pertinents pour la gestion de la sécurité de l'information. Ces cadres offrent des perspectives variées et peuvent être utilisés pour compléter ou enrichir les pratiques de sécurité en fonction des besoins spécifiques des organisations.

1.2.3.1 NIST Cybersecurity Framework

Le National Institute of Standards and Technology (NIST) a élaboré le Cybersecurity Framework, qui offre un ensemble flexible de recommandations pour améliorer la gestion des risques liés à la cybersécurité. Ce cadre est particulièrement apprécié pour sa capacité à s'adapter aux différents types d'organisations et à intégrer les meilleures pratiques en matière de prévention, détection et réponse aux incidents de sécurité.

1.2.3.2 PCI DSS (Payment Card Industry Data Security Standard)

Le PCI DSS est une norme de sécurité spécifiquement conçue pour protéger les données de cartes de paiement. Elle est essentielle pour les organisations traitant des transactions par carte de crédit et impose des exigences rigoureuses en matière de sécurité des systèmes et de gestion des données de paiement.

1.2.3.3 GDPR (General Data Protection Regulation)

Le Règlement Général sur la Protection des Données (GDPR) est une réglementation européenne qui impose des exigences strictes en matière de protection des données personnelles. Bien qu'il ne soit pas un référentiel de sécurité à proprement parler, sa conformité est cruciale pour la protection des informations personnelles au sein des organisations opérant en Europe.

1.2.3.4 ITIL (Information Technology Infrastructure Library)

ITIL est un ensemble de pratiques pour la gestion des services informatiques qui met l'accent sur l'amélioration continue des services IT. Bien que principalement axé sur la gestion des services, ITIL inclut également des pratiques importantes pour la gestion des risques et la sécurité des informations.

1.2.3.5 La Politique de Sécurité des Systèmes d'Information (PSSI)

Au-delà des normes et référentiels mentionnés, la Politique de Sécurité des Systèmes d'Information (PSSI) joue un rôle central dans la mise en œuvre effective des pratiques de sécurité. Elle établit les objectifs stratégiques en matière de sécurité, définit les rôles et responsabilités, et guide les mesures de sécurité à mettre en place. Elle garantit la conformité aux normes et réglementations, propose des directives pour la gestion des incidents de sécurité et établit des mécanismes pour la révision et l'amélioration continue des pratiques. En définissant clairement les attentes et en fournissant un cadre pour la gestion de la sécurité de l'information, la PSSI soutient l'efficacité des autres référentiels et normes en les intégrant dans une stratégie globale de sécurité.

1.3 Les systèmes de management

Les systèmes de management, représentent un ensemble d'éléments corrélés au sein d'un organisme. Ils sont utilisés pour établir des processus afin atteindre des objectifs. Ces objectifs sont préalablement définis par ou en déclinaison de la politique de l'organisme. Nous pouvons ainsi dire qu'un système de management est un ensemble de mesures organisationnelles et techniques visant à atteindre un objectif. Une fois celui-ci atteint, il s'y tient, voire le dépasser. C'est un ensemble de valeurs, de règles, de normes et de convictions fondamentales, considérées comme justes et susceptibles de servir de base au management de la qualité.

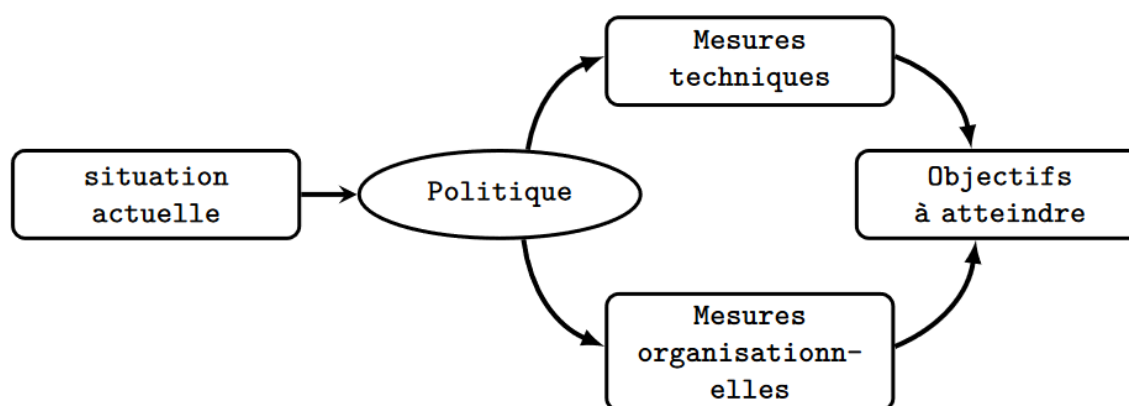


FIGURE 1.6 : Le processus du système de management.

1.3.1 Les principaux systèmes de management

Le tableau ci-après donne un aperçu non exhaustif des principaux référentiels de systèmes de management.

Référentiel	Domaine
ISO 9001	Qualité
ISO 14001	Environnement
ISO 27001	Sécurité de l'information
ISO 20000	Services informatiques
OHSAS 18001	Santé/Sécurité du personnel

TABLE 1.3 : Historique des normes en matière de sécurité de l'information

Nous constatons que la majorité de ces référentiels sont normalisés par l'ISO. Cependant, d'autres organismes privés ou nationaux peuvent proposer leurs propres référentiels. La dernière ligne de cette liste montre, en effet, que l'ISO n'a pas le monopole des systèmes de management, puisque la norme relative à la sécurité du personnel au travail (OHSAS 18001) n'est pas spécifiée par l'ISO.

1.3.2 L'apport des systèmes de management

Toutes les entreprises, quelle que soit leur taille ou leur secteur, bénéficient d'un système de management efficace. Celui-ci répond aux exigences des clients, des parties intéressées et aux enjeux de durabilité, tout en aidant à relever les défis du marché et de la société. Lorsqu'il est appliqué et développé en continu, il permet d'éviter les erreurs, d'identifier opportunités et risques, de satisfaire les parties prenantes et de s'adapter aux évolutions constantes.

Les avantages qu'offrent les systèmes de management

- Des structures uniformes et des responsabilités claires
- Procédures et processus transparents et stables
- Ancrage organisationnel d'un processus d'amélioration continue
- Bonne base d'une culture d'entreprise résiliente et tournée vers l'avenir
- Satisfaction prononcée des clients et des employés

- Réduction notable des coûts grâce à la prévention des erreurs
- Réalisation systématique des objectifs fixés par l'entreprise
- Plus grande sécurité juridique grâce à la réduction des risques
- Amélioration de la réputation et accès plus facile à de nouveaux marchés

Bien que les systèmes de management de la sécurité de l'information (SMSI) offrent de nombreux avantages, il est important de reconnaître qu'ils peuvent également présenter des inconvénients. En voici quelques uns :

- **Temps et ressources** : La mise en œuvre d'un SMSI nécessite du temps et des moyens. Il faut élaborer des politiques, des processus et des procédures, ce qui peut être coûteux en termes de ressources humaines et financières.
- **Complexité documentaire** : La gestion de la sécurité de l'information implique la création et la maintenance de nombreux documents, tels que des politiques, des plans de sécurité, des procédures, etc. Cette paperasserie peut devenir complexe et exigeante.
- **Suivi et maintenance** : Une fois en place, le SMSI nécessite un suivi continu pour s'assurer de sa conformité et de son efficacité. Cela peut également nécessiter des ressources supplémentaires.
- **Rigidité** : Parfois, les organisations peuvent devenir trop rigides dans leur approche de la sécurité de l'information, en suivant aveuglément les obligations formelles. Cela peut entraîner des problèmes si les mesures ne sont pas adaptées aux besoins spécifiques de l'entreprise.
- **Externalités** : L'utilisation d'un SMSI dans une organisation peut avoir des effets sur d'autres systèmes en interaction. Par exemple, des contrôles de sécurité stricts peuvent entraver la productivité des employés.

1.3.3 Les systèmes de management de la sécurité de l'information (SMSI)

[16] Un Système de Management de la Sécurité de l'Information (SMSI), en anglais : Information security management system (ISMS) est un ensemble d'outils, de documents et de méthodes qui vise à fixer et à appliquer une politique de sécurité de l'information adaptée au besoin d'une entreprise . Il permet à l'entreprise de fixer les objectifs, de les atteindre et, finalement, d'évaluer leur effet dans un objectif d'amélioration constante. Un SMSI est défini par :

- des processus,
- des politiques de sécurité,
- des structures de pilotage et de contrôle,
- une démarche d'amélioration continue,
- des outils en sécurité.

C'est un mode d'organisation que l'entreprise doit mettre en place pour préserver la confidentialité, l'intégrité et la disponibilité de l'information. Ce système prend en compte à la fois des facteurs techniques et humains. Un SMSI permet de gérer les risques relatifs à l'information au moyen de processus, et définit les différentes responsabilités. Dans l'optique de la certification, le SMSI sert à découvrir et à résoudre les non-conformités.

1.3.3.1 Les 4 phases de la démarche PDCA selon la norme 27001

La mise en place d'un SMSI opérationnel est exposée dans la norme ISO 27001 et repose sur les principes chers au domaine de la qualité. La démarche, connue sous l'abréviation PDCA, ou principe de la roue de Deming, vise une amélioration continue du système par le déploiement de 4 phases :

1. **Plan** : Création du SMSI en évaluant les risques de sécurité de l'information et en choisissant les méthodes de vérification adaptées ;
2. **Do** : Mise en œuvre des vérifications, cette phase consiste à passer à l'action, c'est la phase opérationnelle qui permet d'avancer vers la cible fixée précédemment.
3. **Check** : Révision et évaluation de la performance (efficacité et efficience) du SMSI
4. **Act** : Modifications, si nécessaires, afin que la performance du SMSI soit optimale.

Le schéma suivant permet de bien en cerner le périmètre :

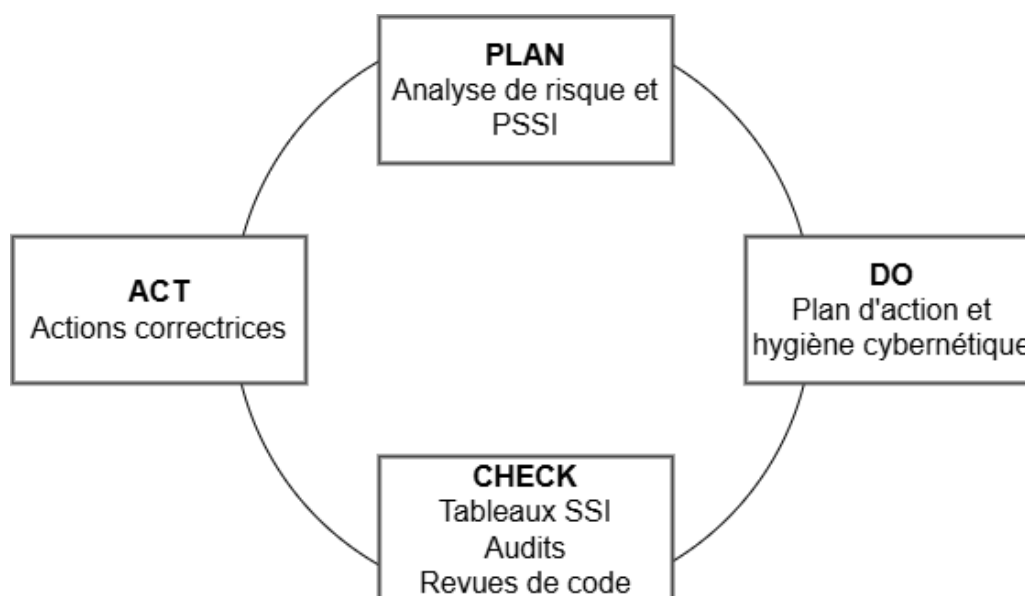


FIGURE 1.7 : La roue de Deming[17]

Phase 1 : Plan

L'objectif de cette première étape est de poser les bases d'un SMSI opérationnel. Si on se réfère au document de référence (la norme ISO 27001), il s'agit de :

- définir la politique et de cadrer le périmètre du SMSI ;
- apprécier les risques et leur traitement des risques ;
- choisir les mesures de sécurité adéquates pour maîtriser les risques.

Phase 2 : Do

L'objectif de cette étape est la mise en place de mesures évoquées dans la phase précédente. Il s'agit de déployer la sécurité de manière opérationnelle. La phase 2 de mise en place d'un SMSI reprend les grandes lignes du plan d'action sécurité de la PSSI. Néanmoins, la mise en place d'un SMSI, au sens de la norme ISO 27001, élargit le périmètre d'application en complétant le plan d'action :

- tout d'abord, des indicateurs clés de performances ou de pilotage sont attachés à chaque mesure, afin d'évaluer leur efficacité et leur conformité. Ce processus n'est pas aisé. Toutefois, la norme [ISO 27004](#) propose une méthodologie pour guider leur élaboration ;
- ensuite, la norme 27001 préconise d'inscrire dans le marbre une formation de sensibilisation des personnels de l'entreprise aux enjeux de la [SSI](#).

Phase 3 : Check

Cette étape est la phase centrale de la démarche [PDCA](#). Elle vise à mettre en œuvre les moyens nécessaires pour **mesurer la conformité des exigences de sécurité** avec le cahier des charges de référence que constitue la norme [ISO 27001](#). La mesure des écarts entre les mesures prises et le niveau de référence, peut être réalisée à travers :

- des **audits internes** planifiés à l'avance ou des contrôles inopinés. Leur objectif est de déterminer, grâce aux indicateurs précédents, l'écart entre la norme et le [SMSI](#) mis en place. Pour les réaliser, on peut procéder en 3 étapes :
 1. Mettre en place une **procédure de feedback** (on parle aussi de retour d'expérience ou de lessons learned) qui permet à chaque responsable de faire part des changements dans son périmètre.
 2. **Évaluer les impacts** sur la version actuelle de la [PSSI](#).
 3. **Animer une réunion de direction** pour entériner les changements.
- des **audits de maturité du SI** qui évaluent les enjeux du système d'information, mesurent l'écart entre les pratiques actuelles et les attentes, et proposent des actions pour une gestion optimale de la [SSI](#).
- des **campagnes de tests d'intrusion** ou des **revues de code**

Phase : Act

Cette dernière phase vise à mettre en place les actions correctrices, préventives ou d'amélioration pour réduire les dysfonctionnements relevés dans la phase précédente. Cette démarche en 4 phases vise une amélioration continue du [SMSI](#), pour tendre vers une conformité maximale aux textes de référence.

Conclusion

L'audit de sécurité des systèmes d'information apparaît comme un processus crucial dans la gestion efficace des risques et des vulnérabilités informatiques. En examinant les différentes étapes du cycle de vie de l'audit, de la définition de la charte d'audit à la rédaction du rapport final, il devient évident que cette pratique permet d'identifier et d'évaluer les faiblesses potentielles dans un environnement informatique. En intégrant les principes des systèmes de management de la sécurité de l'information ([SMSI](#)), les organisations peuvent renforcer leur posture de sécurité et répondre aux défis croissants liés à la cybercriminalité et aux menaces numériques.

Méthodologie d'évaluation

Dans le cadre de l'évaluation de la sécurité du système d'information, il est primordial de bien comprendre le contexte dans lequel l'institution opère. Cette section fournit une présentation détaillée de la **CAGD**, son rôle critique dans la gestion de la dette publique, ainsi que l'impact potentiel des failles de sécurité sur les finances publiques. Par ailleurs, nous aborderons aussi le périmètre et le planning de l'audit, ainsi que les différentes étapes. Cette préparation minutieuse est essentielle pour assurer une évaluation exhaustive et rigoureuse, permettant d'identifier et de traiter les vulnérabilités du système d'information.

2.1 Présentation de la **CAGD**

2.1.1 Historique et cadre juridique

2.1.1.1 Contexte historique

La Caisse Autonome de Gestion de la Dette (**CAGD**), ancienne Caisse Autonome d'Amortissement (**CAA**) a été fondée en 1998 dans le cadre de réformes visant à rationaliser la gestion de la dette publique dans le pays. À l'origine, elle a été créée pour faire face aux défis de la gestion de la dette accumulée par l'État, en apportant une structure centralisée et spécialisée pour la gestion des obligations financières. Depuis sa création, l'institution a évolué significativement, adopté des outils technologiques modernes pour optimiser la gestion de la dette et s'est adaptée aux exigences économiques et réglementaires en constante évolution.

2.1.1.2 Cadre juridique et conformité

Le fonctionnement de la **CAGD** est régi par un cadre juridique bien défini, qui établit les règles et les obligations liées à la gestion de la dette publique. Ce cadre comprend la Loi de Finances gestion 2024, qui fixe les principes de gestion et les limites d'endettement, garantissant ainsi que la dette est gérée de manière prudente et responsable. Les décrets réglementaires complètent cette loi en détaillant les modalités d'application et les responsabilités des acteurs impliqués dans la gestion de la dette. Elle adhère également aux normes internationales établies par la Banque Mondiale et le Fonds Monétaire International, garantissant ainsi une gestion de la dette conforme aux meilleures pratiques et standards mondiaux..

2.1.2 Mission et Objectifs [5]

2.1.2.1 Mission et objectifs généraux

La mission fondamentale de la CAGD est de gérer la dette publique avec une rigueur professionnelle et une transparence totale. Cette mission se traduit par les points suivants :

- **Optimisation de la gestion de la dette :** La CAGD s'efforce de réduire le coût global de la dette tout en minimisant les risques financiers associés.
- **Garantie de la stabilité financière :** En assurant une gestion prudente et efficace des obligations financières, la CAGD contribue à la stabilité économique du pays.
- **Promotion de la transparence :** La CAGD publie régulièrement des rapports détaillés sur la gestion de la dette, favorisant ainsi la transparence et la responsabilité.

2.1.2.2 Rôle dans l'administration financière

Outre sa mission principale, la CAGD joue un rôle central dans l'administration financière du pays. Elle collabore étroitement avec d'autres institutions financières nationales et internationales pour garantir la mise en œuvre efficace des politiques de gestion de la dette. Cette collaboration lui permet également de fournir des analyses et des recommandations qui influencent la formulation des politiques économiques et financières. En assurant une transparence totale dans ses opérations, la CAGD contribue à renforcer la confiance des citoyens et des partenaires internationaux dans la gestion des fonds publics, tout en facilitant la production de rapports financiers détaillés.

2.1.3 Rôle critique dans la gestion de la dette publique

La sécurité des systèmes d'information est essentielle pour la gestion efficace de la dette publique. Les systèmes informatiques de la CAGD traitent des données extrêmement sensibles, notamment des informations financières cruciales et des détails sur les transactions. Assurer la sécurité de ces systèmes est donc primordial pour préserver la confidentialité des informations et garantir leur intégrité. En protégeant ces systèmes contre les accès non autorisés, les modifications malveillantes et les interruptions de service, elle assure la fiabilité des opérations financières et la conformité avec les exigences réglementaires. La sécurité des systèmes d'information joue ainsi un rôle central dans la gestion de la dette, permettant à la CAGD de fonctionner de manière efficace et sécurisée.

2.1.4 Impact des failles de sécurité sur la gestion des finances publiques

Les failles de sécurité peuvent avoir des conséquences graves et étendues sur la gestion des finances publiques. Les violations de sécurité, telles que les cyberattaques ou les fuites de données, peuvent compromettre la confidentialité des informations financières sensibles, entraînant des risques de manipulation ou de divulgation non autorisée. De telles failles peuvent également perturber les opérations de gestion de la dette, causant des retards dans les transactions et des erreurs dans les rapports financiers. Les coûts de réparation des systèmes compromis et les amendes pour non-conformité peuvent être significatifs. Les incidents passés dans le secteur financier démontrent ces risques et soulignent l'importance de mesures de sécurité solides pour protéger les systèmes d'information et préserver la confiance dans la gestion des finances publiques.

Des incidents passés, comme les cyberattaques ciblant des institutions financières, illustrent les dangers potentiels et soulignent l'importance de la mise en œuvre de mesures de sécurité robustes. La gestion proactive des risques de sécurité est donc essentielle pour protéger les systèmes d'information et maintenir la confiance dans la gestion des finances publiques.

2.1.5 Périmètre de l'audit

L'audit de la sécurité du système d'information de la Caisse Autonome de Gestion de la Dette porte sur des éléments critiques pour une évaluation intégrale de la sécurité. Cet audit interne sera réalisé exclusivement sur le siège unique de la CAGD. Le périmètre englobe, sans s'y limiter, les éléments suivants :

- **Infrastructures** : Évaluation des serveurs, bases de données, réseaux et dispositifs de stockage. Analyse de l'efficacité des dispositifs de sécurité (pare-feux, IDS, IPS) et vérification des règles de gestion des identités et des accès.
- **Gestion des données** : Analyse des pratiques liées à la collecte, au stockage, au traitement, et à la protection des données sensibles, incluant l'évaluation des technologies de sécurité telles que le chiffrement et les protocoles de sauvegarde.
- **Politiques, procédures de sécurité et conformité réglementaire** : Révision des politiques de sécurité, des procédures de gestion des incidents, et des plans de continuité et de reprise après sinistre. Vérification de l'alignement avec les cadres légaux et réglementaires applicables.

Chaque composant sera évalué pour s'assurer de sa configuration optimale et de sa conformité avec la PSSIE et la norme ISO 27001. Cette évaluation identifie les vulnérabilités, protège les informations critiques et assure la conformité des pratiques et technologies aux normes de sécurité en vigueur. L'objectif ultime est de renforcer la sécurité globale du système d'information de la CAGD tout en assurant une conformité rigoureuse aux directives établies.

2.1.6 Personnes ressources

Les personnes qui sont amenées à répondre aux questionnaires incluent généralement les profils suivants :

- L'équipe du Département des Systèmes d'Information ;
- Chef Département Administratif et Financier ;
- Responsable des Ressources Humaines ;
- Autres utilisateurs clés du système ;

Ces différentes personnes pourront répondre à des préoccupations durant l'évaluation car elles interagissent avec le système d'information. La liste n'étant pas exhaustive, d'autres intervenants pourraient être consultés au besoin lors du déroulement de la mission.

2.1.7 Planning de la mission

Nous avons élaboré un calendrier afin de dérouler la mission d'audit proprement dite sur 6 mois de la phase de préparation au rapport final. Le planning proposé se retrouve dans le tableau suivant :

Phase	Description	Durée
Phase 1 : Préparation de la mission	- Définition des objectifs et du périmètre évalué - Planification des ressources - Collecte des documents préliminaires	2 semaines
Phase 2 : Control des aspects organisationnels et physiques	- Évaluation de la structure organisationnelle et des politiques de sécurité - Inspection physique du site - Contrôle des accès physiques et logiques aux systèmes	6 semaines
Phase 3 : Contrôle des aspects techniques	- Evaluation des infrastructures technologiques (réseaux, serveurs, etc.) - Test de conformité des logiciels et des applications - Vérification des dispositifs de sécurité (pare-feux, IDS, etc.)	6 semaines
Phase 4 : Conformité Réglementaire	- Analyse des politiques de sécurité existantes - Évaluation de la conformité par rapport à la PSSIE etc.) - Vérification de l'application des contrôles de conformité	6 semaines
Phase 5 : Recommandations et conclusion	- Élaboration des recommandations pour améliorer la sécurité - Préparation et présentation du rapport final	6 semaines
Rédaction du rapport	- Compilation et rédaction du rapport détaillé pour chaque phase - Révisions et validation - Présentation finale aux parties prenantes	Continuellement, tout au long de la mission 25 semaines

TABLE 2.1 : Planning de la mission

2.1.8 Politique de Sécurité des Systèmes d'Information de l'État ([PSSIE](#))

[1] Le Bénin dans sa marche vers un cyberspace sécurisé, a élaboré les documents stratégiques qui définissent les grandes lignes directrices ainsi que les activités à mettre en œuvre pour l'atteinte des objectifs visés. Ainsi, le Gouvernement de la République du Bénin a approuvé par décret N° 2021- 550 du 27 octobre 2021 la [PSSIE](#) qui découle de sa Stratégie Nationale de Sécurité Numérique ([SNSN](#)). Ce document de politique est un condensé d'exigences et de mesures techniques, physiques et organisationnelles pour la sécurité des systèmes d'information des entités et structures de l'État.

2.1.8.1 Objectifs clés de la [PSSIE](#)

Les objectifs de la [PSSIE](#) sont de :

- **Protéger les systèmes d'information de l'État** : Prévenir les violations et les attaques contre les informations sensibles et les infrastructures.
- **Harmoniser les pratiques de sécurité** : Définir des procédures et des normes de gestion de la sécurité des systèmes d'information homogènes dans toutes les institutions publiques.
- **Renforcer les capacités institutionnelles** : Formation et sensibilisation des fonctionnaires aux bonnes pratiques de sécurité informatique, renforcement des compétences techniques dans les administrations.
- **Gestion des incidents de sécurité** : Développer des capacités de détection, de réaction, et de récupération proactives des incidents de sécurité pour limiter leur impact.

2.1.8.2 Déploiement et fonctions

La mise en œuvre de la [PSSIE](#) est assurée par une série d'acteurs clés dans l'État béninois. Chaque ministère, institution, et agence publique est tenu de mettre en œuvre les principes de la [PSSIE](#) dans ses systèmes d'information. En général, un comité de pilotage central a la responsabilité de coordonner les efforts, de conseiller du point de vue technique (au besoin), et de vérifier si les institutions sont conformes aux politiques de sécurité. Les institutions doivent notamment :

- **Élaborer des plans de sécurité** : Toute organisation doit élaborer et maintenir un plan de sécurité des systèmes d'information conjointement avec la [PSSIE](#).
- **Effectuer des audits de sécurité** : Les audits doivent être continus pour identifier les vulnérabilités et vérifier la conformité.
- **Gestion des risques** : Les risques doivent être mesurés et des mesures de gestion appropriées doivent être identifiées.

Étant une institution sous la tutelle du Ministère de l'Économie et des Finances, la [CAGD](#) ne fait pas exception et est tenue de se conformer à la [PSSIE](#).

2.1.8.3 Objectifs et règles de sécurité

La PSSIE fixe des lignes directrices précises pour garantir la confidentialité, l'intégrité et la disponibilité des informations sensibles de l'État, tout en réduisant les vulnérabilités et en renforçant la résilience face aux cybermenaces. En adoptant ces règles, les institutions publiques s'engagent à respecter des standards rigoureux de gestion des risques et à se conformer aux exigences légales et réglementaires, favorisant ainsi une gouvernance sécurisée et un environnement numérique fiable.

1. **Organisation de la sécurité des systèmes d'information** : Établir un cadre de gestion pour engager, puis vérifier la mise en œuvre et le fonctionnement de la sécurité des systèmes d'information au sein de l'entité.
2. **Sécurité des ressources humaines** : Faire des ressources humaines un maillon fort de la sécurité des systèmes d'information.
3. **Gestion des actifs du système d'information** :
 - Identifier les actifs du système d'information de l'entité et s'assurer que les responsabilités sont définies pour la protection des actifs.

- Identifier la sensibilité des actifs du système d'information pour permettre aux utilisateurs d'en faire un bon usage.
 - Maîtriser la sécurité du cycle de vie des actifs.
 - Sécuriser les informations qui sont stockées sur les supports numériques.
4. **Contrôle d'accès logique au système d'information** : Limiter l'accès aux systèmes d'information aux seules personnes autorisées.
 5. **Sécurité physique des locaux abritant les actifs SI** : Empêcher tout accès physique non autorisé, tout dommage ou toute intrusion dans les environnements des SI.
 6. **Protection du matériel** : Empêcher la perte, l'endommagement, le vol ou la compromission des actifs.
 7. **Sécurité des réseaux informatiques** : Garantir la protection de l'information sur les réseaux informatiques de l'entité.
 8. **Sécurité du poste de travail utilisateur** : Fournir aux utilisateurs des postes de travail sécurisés pour leurs activités professionnelles.
 9. **Sécurité des équipements itinérants** : Protéger l'information stockée sur des équipements nomades.
 10. **Sécurité liée à l'exploitation des SI** : Assurer l'exploitation correcte et sécurisée des SI et gérer les actions d'administration du SI.
 11. **Sécurité dans l'acquisition, le développement et la maintenance des SI** : Intégrer la sécurité dans le cycle de vie des systèmes d'information qu'ils soient acquis ou développés par l'entité.
 12. **Sécurité des e-services** : Sécuriser les informations impliquées dans les applications d'e-services.
 13. **Sécurité des applications Web** : Sécuriser les applications exposées sur Internet.
 14. **Mesures cryptographiques** : Garantir l'utilisation correcte et efficace de la cryptographie en vue de protéger la confidentialité, l'authenticité et/ou l'intégrité de l'information.
 15. **Relations avec les fournisseurs** : Garantir la protection des actifs de l'organisation accessibles aux fournisseurs.
 16. **Sécurité du Cloud computing** : Assurer la sécurité des informations hébergées dans une infrastructure cloud.
 17. **Gestion des incidents de sécurité** : Garantir une méthode cohérente et efficace de gestion des incidents liés à la sécurité du SI, incluant la communication des événements et des failles liées à la sécurité.
 18. **Gestion de la continuité de la sécurité du SI** : Faire en sorte que la sécurité des systèmes d'information fasse partie intégrante du processus de continuité d'activité de l'entité.
 19. **Conformité, audit et contrôles de sécurité** :
 - Éviter toute violation des obligations légales, statutaires, réglementaires ou contractuelles relatives à la sécurité de l'information, éviter toute violation des exigences de sécurité.

- Effectuer des contrôles et des exercices réguliers de façon à mesurer les progrès accomplis et corriger les manquements.

2.1.9 Evaluation des aspects organisationnels et physiques

L'audit organisationnel et physique est une phase préliminaire de notre évaluation de sécurité qui a pour objectif de scruter la gestion et l'organisation de la sécurité, en prenant en compte les dimensions organisationnelles, humaines et physiques. L'objectif principal est de fournir une vue d'ensemble qualitative et quantitative des différents facteurs de sécurité du site audité. Cette évaluation permet également d'identifier les points critiques du système d'information qui nécessitent une attention particulière.

Pour réaliser cette étape, une méthodologie rigoureuse est essentielle. Un questionnaire détaillé est élaboré, prenant en compte les spécificités de l'organisme à auditer. Ce questionnaire est conçu pour être flexible et adaptable aux réalités de l'organisation, afin de garantir une évaluation précise et pertinente. Après l'exploitation de ce questionnaire et l'analyse des réponses obtenues, l'auditeur est en mesure d'évaluer les écarts présents, d'apprécier le niveau de maturité en termes de sécurité et de vérifier la conformité de l'organisme avec la norme référentielle de l'audit. Dans le contexte actuel, et suivant les recommandations de l'[ASSI](#), cet audit se référera aux clauses de la Politique de Sécurité des Systèmes d'Information de l'État approuvé par décret N° 2021- 550 le 27 octobre 2021. Notre questionnaire se basera donc sur cette politique.

2.1.10 Evaluation technique

L'audit technique, qui suit l'audit organisationnel, se concentre sur une analyse approfondie de la sécurité des composants techniques du système informatique. Cette phase consiste en des tests pour évaluer la résistance des systèmes face aux attaques, et en une analyse des risques associés aux failles découvertes lors de l'audit. Cette analyse couvre divers environnements, tels que les réseaux d'accès Internet, les réseaux d'interconnexion intersites, ainsi que les serveurs internes et les postes sensibles du [LAN](#).

Le processus d'audit technique se déroule en quatre phases distinctes. La première phase implique un audit de l'architecture du système, au cours de laquelle les caractéristiques du système d'information sont recensées. Cela inclut la reconnaissance du réseau, le sondage des systèmes, des services réseau, et des applications. La deuxième phase consiste en une analyse des vulnérabilités internes, utilisant divers outils automatisés pour identifier les failles et les composants vulnérables du système.

La troisième phase se concentre sur les vulnérabilités externes, en vérifiant les possibilités pour un attaquant de récupérer des informations sur le système depuis l'extérieur. Cette phase implique l'énumération des services et protocoles internes, ainsi que l'élaboration de scénarios d'attaques potentielles. Enfin, la quatrième phase est dédiée à l'évaluation de l'architecture de sécurité existante. Elle vise à évaluer la qualité de l'architecture de sécurité, à identifier les périmètres établis et à analyser la sécurité des flux sensibles et l'administration des outils de sécurité. Cela inclut la politique des mots de passe, la protection contre les attaques par déni de service, ainsi que la configuration des firewalls et des [ACLs](#), etc.

2.1.11 Rapport d'évaluation

La phase finale de l'évaluation de sécurité est consacrée à la rédaction du rapport de synthèse. Ce rapport résume les principales vulnérabilités et insuffisances identifiées au cours de l'audit. Il inclut également une synthèse des solutions et outils de sécurité recommandés, ainsi qu'une série de recommandations pour la mise en œuvre de mesures organisationnelles, physiques et techniques. En outre, le rapport esquisse un plan d'action pour la sécurité, en estimant les budgets nécessaires pour la mise en œuvre des mesures recommandées.

2.2 Description du système d'information

Avant d'entamer l'évaluation organisationnelle et physique il est nécessaire de collecter les informations concernant l'infrastructure, les composants informatiques et réseaux du site à auditer.

2.2.1 Description de l'architecture

Cette architecture réseau en étoile relie plusieurs étages, chacun équipé de postes utilisateurs connectés à des commutateurs Cisco (Catalyst 2960, 2960-X et Small Business). Au 4ème et 3ème étages, les ordinateurs sont connectés à une baie réseau centrale via des commutateurs, reliant ainsi tous les utilisateurs aux ressources du SI. La baie réseau gère la connectivité entre les étages et les serveurs. La baie serveur regroupe plusieurs serveurs critiques, dont des serveurs de domaine, d'applications, de fichiers, de sauvegarde, et des serveurs de virtualisation.

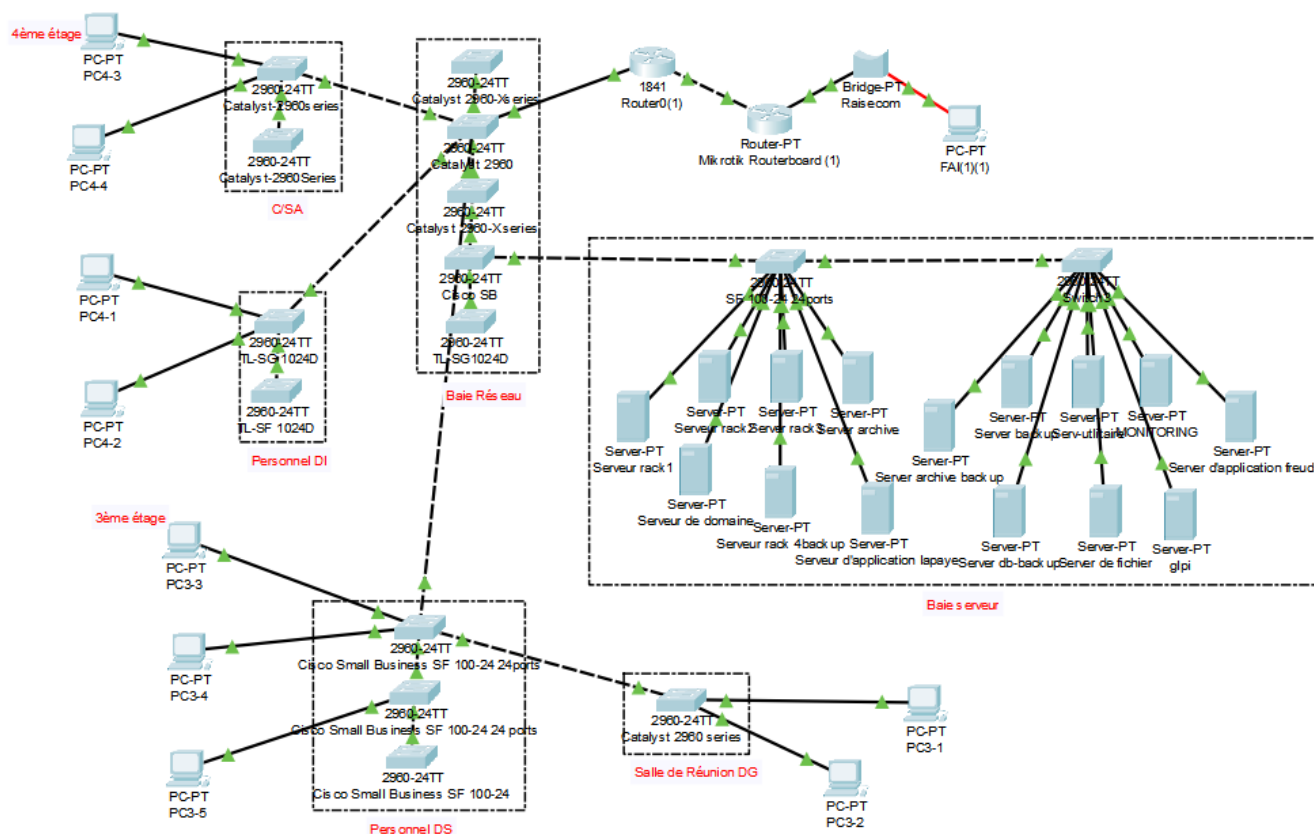


FIGURE 2.1 : Architecture réseau de la CAGD

2.2.2 Mesures de sécurité existantes

2.2.2.1 Sécurité réseaux

L'architecture réseau est sécurisée à son point d'entrée par un pare-feu FortiGate, chargé de filtrer les flux de données. Ce dispositif nécessite un renouvellement de licence annuel. Il arrive parfois que, durant la période de renouvellement, le pare-feu se retrouve sans licence, ce qui entraîne la désactivation de tous les services de sécurité associés. Par ailleurs, aucune solution de détection ou de prévention des intrusions (IDS/IPS) n'est en place pour surveiller l'activité du pare-feu, notamment l'analyse des journaux de sécurité.

2.2.2.2 Sécurité physique

Ces observations mettent en évidence des mesures de sécurité physique déjà en place, tout en pointant des faiblesses importantes. La sécurité physique repose sur les aspects suivants :

- Des agents se chargent de surveiller l'accès aux locaux. Ils contrôlent parfois les entrées et consignent des informations sur chaque visiteur.
- La salle des serveurs est fermée à clé, et seuls les individus autorisés, possédant la clé, peuvent y accéder.
- Tous les serveurs ne sont pas placés dans des armoires sécurisées. Certains sont simplement posés sur une table, ce qui représente une faiblesse dans l'organisation physique du matériel.
- La salle des serveurs est équipée d'un système de climatisation pour maintenir une température adéquate et assurer le bon fonctionnement des équipements.
- Seuls les serveurs et les équipements réseaux critiques sont protégés par des onduleurs, permettant de pallier aux coupures de courant de courte durée. Cependant, des dysfonctionnements ont été observés, aussi bien sur le réseau électrique que sur le groupe électrogène, en cas de coupure prolongée.
- Des extincteurs sont disponibles à chaque étage du bâtiment pour faire face à d'éventuels incendies.
- Il existe une absence de caméras de surveillance dans certaines zones sensibles, ce qui limite la capacité à monitorer ces endroits en cas d'incident.

2.2.2.3 Sécurité logique

La sécurité logique repose sur plusieurs mesures importantes visant à protéger les systèmes et les données :

- Un contrôleur de domaine est mis en place pour centraliser la gestion des accès aux postes de travail des utilisateurs, garantissant un contrôle rigoureux des autorisations et des droits d'accès.
- Le filtrage des accès vers et depuis Internet est assuré par le pare-feu, qui permet de réguler et surveiller les connexions afin d'empêcher les accès non autorisés et de protéger contre les menaces externes.

- Un pare-feu est installé, permettant de configurer des listes de contrôle d'accès pour filtrer les flux réseau selon des règles de sécurité définies, assurant ainsi un contrôle précis des communications internes et externes.
- Un antivirus est également déployé sur les postes de travail et les serveurs, offrant une protection contre les malwares et autres logiciels malveillants, garantissant une surveillance continue des menaces potentielles.

2.2.2.4 Sécurité des machines

La sécurité des machines est assurée par plusieurs mesures importantes, bien que certaines faiblesses soient à noter :

- **Gestion des mises à jour et distribution de correctifs** : La gestion des mises à jour et la distribution des correctifs sont centralisées via l'antivirus. Cependant, plusieurs problèmes subsistent :
 - Certains systèmes d'exploitation ne disposent pas de licences valides, ce qui peut limiter leur capacité à recevoir des mises à jour officielles.
 - Comme observé sur le pare-feu, il existe des périodes d'indisponibilité de licence qui mettent en péril la surveillance du SI.
 - Les switches, routeurs et d'autres équipements réseau ne bénéficient pas de mises à jour régulières, laissant ces équipements vulnérables aux menaces potentielles.
- **Système antiviral** : Un système antivirus centralisé (Kaspersky) est en place pour détecter et éliminer les menaces ainsi que les codes malveillants.
- **Gestion des mots de passe** : Bien que les utilisateurs aient la possibilité de changer leur mot de passe, ce qui leur permet de maintenir un certain niveau de sécurité personnelle, la gestion des mots de passe présente plusieurs lacunes :
 - Il n'existe aucune politique formelle pour la gestion des mots de passe, ce qui peut entraîner des pratiques non sécurisées.
 - Les mots de passe des serveurs ne sont pas modifiés régulièrement, ce qui constitue une faiblesse en matière de sécurité.

Après avoir décrit l'environnement dans lequel s'est déroulée notre mission d'audit et identifié l'architecture réseau ainsi que les principaux serveurs et équipements, nous aborderons, dans le prochain chapitre, la classification des failles organisationnelles et physiques en fonction des exigences.

2.3 Audit organisationnel et physique

2.3.1 Questionnaire d'audit

Pour réaliser une évaluation complète et rigoureuse, nous avons conçu le questionnaire détaillé ci-après, disponible en annexe (AUDIT CONFORMITE). Ce questionnaire est structuré comme suit :

- **CODE** : Ce code sert de référence unique pour chaque exigence d'audit ou règle. Il est généralement sous forme alphanumérique (par exemple, "SEC-001", "POL-002") et permet de structurer et d'indexer les différents éléments de l'audit. Ce système facilite le suivi et la traçabilité des éléments évalués, surtout dans les rapports où des dizaines, voire des centaines de points peuvent être analysés. Cela rend également la communication plus simple entre l'auditeur et l'équipe auditée.
- **EXIGENCES SPÉCIFIQUES** : Cette colonne précise les critères exacts que vous souhaitez auditer. L'exigence doit être décrite de manière précise, permettant ainsi de catégoriser les règles. Par exemple : "Contrôle d'accès logique" ou "Sauvegarde des données". Cela garantit que chaque exigence est bien définie et alignée avec les objectifs de l'audit.
- **RÈGLES** : Cette section décrit les règles ou directives que les équipes doivent suivre pour se conformer à la politique. Ces règles sont souvent issues des meilleures pratiques, des standards de l'industrie, ou des réglementations. Par exemple, si l'exigence concerne la gestion des mots de passe, la règle pourrait être : "Les mots de passe doivent comporter au moins 12 caractères, inclure des majuscules, minuscules, chiffres, et symboles." Cela aide à préciser ce qui est attendu pour chaque point, facilitant l'évaluation de la conformité.
- **POIDS** : Cette colonne indique la criticité de l'exigence ou du contrôle évalué :
 - **N = Normal** : L'exigence est importante mais son non-respect ne présente pas un risque immédiat ou critique.
 - **C = Critique** : L'exigence est cruciale, et toute non-conformité représente un risque majeur pour la sécurité ou la conformité réglementaire.

MATURITÉ : Cette colonne évalue le degré de maturité des processus ou des mesures de sécurité mises en place. Elle s'appuie sur une échelle de 0 à 5, inspirée du modèle de maturité des capacités ([CMMI](#)) :

- **0 : Inexistant** : Aucun processus ou contrôle n'est en place.
- **1 : Initial (ad hoc et désorganisés)** : Les contrôles existent, mais ils sont informels, non standardisés, ou appliqués de manière incohérente.
- **2 : Répétitif (modèle répétable)** : Les processus sont en place et peuvent être répétés, mais ils ne sont pas encore documentés ou formalisés.
- **3 : Défini (formalisés et communiqués)** : Les processus sont bien définis, documentés, et communiqués à l'ensemble de l'organisation.
- **4 : Géré (surveillés et mesurés)** : Les processus sont surveillés de manière régulière, avec des indicateurs de performance clairs.
- **5 : Optimisé (automatisé)** : Les processus sont automatisés, optimisés, et soumis à une amélioration continue.

Cette échelle permet d'identifier le niveau de sophistication et de fiabilité des mesures de sécurité mises en place, ce qui peut influencer les priorités de correction.

ÉVALUATIONS ET CONCLUSIONS "CONFIRMATIONS" : Cette colonne permet de noter nos observations finales après l'évaluation. Il s'agit de synthétiser les conclusions basées sur l'analyse des preuves collectées, telles que l'efficacité des contrôles de sécurité, la conformité avec les règles, et le niveau de maturité atteint. Nous pouvons aussi consigner s'il y a des écarts par rapport aux attentes ou des points à améliorer.

PREUVES (Documentation, Enregistrement, Configuration, Image, ...) : Cette colonne détaille les preuves tangibles recueillies au cours de l'audit pour soutenir les conclusions. Les preuves peuvent prendre différentes formes :

- **Documentation :** Politiques de sécurité, manuels d'utilisation, manuels procédures, etc.
- **Enregistrement :** Journaux d'événements (logs), rapports de monitoring, etc.
- **Configuration :** Paramètres des systèmes ou des réseaux, captures d'écran, etc.
- **Image :** Photos d'équipement, captures d'écran de configurations, etc.

Cette colonne nous permet de fournir des preuves concrètes renforce la crédibilité des conclusions de l'audit et garantit la transparence du processus.

PROCÉDURES DE TEST UTILISÉES : Cette colonne précise les méthodes et techniques utilisées pour évaluer chaque exigence spécifique. Les principales méthodes comprennent :

- **Observation directe :** Observer les opérations et les pratiques de sécurité en temps réel.
- **Entretien :** Dialoguer avec le personnel pour obtenir des informations sur leurs pratiques et leur compréhension des politiques de sécurité.
- **Revue documentaire :** Examiner les documents, les politiques, et les procédures pour vérifier leur conformité.
- **Vérifications techniques :** Utiliser des outils automatisés (scans de vulnérabilités, tests de pénétration) pour détecter les failles de sécurité.
- **Analyse d'échantillon :** Sélectionner un échantillon représentatif de données, configurations ou processus pour les analyser en profondeur.
- **Corroboration :** Croiser les informations de différentes sources pour s'assurer de la validité des observations.

Cette étape permet d'assurer que les évaluations sont complètes et fondées sur des méthodes rigoureuses. La liste n'étant pas exhaustive, d'autres procédures pourraient être utilisées.

RECOMMANDATIONS : Après évaluation, cette colonne propose des actions correctives ou des recommandations d'amélioration. Ces recommandations visent à combler les lacunes identifiées et à renforcer les processus ou les mesures de sécurité. Elles doivent être claires, applicables et réalistes, par exemple : "Mettre à jour le système de gestion des accès pour inclure l'authentification multifactorielle."

CONFORMITÉ : Cette colonne évalue si l'exigence spécifique est respectée ou non.

- **0 : Non applicable :** L'exigence ne s'applique pas à ce contexte ou à ce système particulier.
- **1 : Non conforme :** L'exigence n'est pas respectée, ce qui peut représenter un risque de sécurité.

- **2 : Conforme** : L'exigence est respectée, signifiant que le contrôle ou le processus est bien en place.

Cette classification aide à comprendre rapidement l'état de conformité du [SI](#) par rapport aux exigences.

Il est important de noter que les colonnes CODE, EXIGENCES SPÉCIFIQUES, RÈGLES et POIDS ont été remplies en conformité avec la [PSSIE](#). Elles sont identiques aux directives de la [PSSIE](#) pour garantir que les contrôles de sécurité et que les exigences réglementaires soient correctement évalués.

Conclusion

L'audit étant effectué, les constats sont alarmants et justifient la nécessité d'une refonte en profondeur des stratégies de sécurité de la [CAGD](#). Dans le chapitre suivant, nous présenterons les résultats de l'audit ainsi que des recommandations visant à pallier les insuffisances observées. Ces recommandations couvriront les volets organisationnels, techniques et procéduraux, en soulignant les bonnes pratiques à adopter pour rehausser le niveau de sécurité global. Enfin, nous aborderons la stratégie de mise en œuvre des recommandations et le suivi de leur efficacité, afin de garantir une amélioration continue du système de sécurité de l'information.

Résultats & Recommandations

Ce chapitre vise à présenter les résultats obtenus et à formuler des recommandations visant à renforcer la sécurité des systèmes d'information. Ces orientations permettront de pallier les faiblesses identifiées suite à l'audit.

3.1 Présentation des résultats

Dans le cadre de l'évaluation de conformité réalisé auprès de la Caisse Autonome de Gestion de la Dette, les résultats obtenus mettent en lumière une situation préoccupante. Avec une conformité globale de seulement **11,56%** aux exigences de la Politique de Sécurité des Systèmes d'Information de l'État et de **09,50%** pour la norme ISO 27001, l'institution se trouve bien en deçà des standards requis pour garantir la sécurité et l'intégrité de ses systèmes d'information. Ce faible niveau de conformité souligne des lacunes profondes, non seulement dans la mise en œuvre des mesures de sécurité de base, mais aussi dans la capacité de l'institution à répondre aux risques grandissants liés à la cybercriminalité et aux menaces internes. Cette situation expose directement l'institution à des risques critiques, tant pour la protection de ses données sensibles que pour la continuité de ses opérations stratégiques. À une époque où la gestion de la dette publique dépend d'infrastructures numériques sécurisées, cette faible conformité met en lumière un écart significatif entre les pratiques actuelles et les exigences essentielles pour protéger les actifs numériques de l'institution.

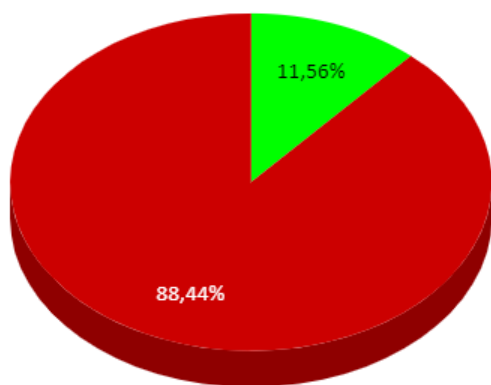


FIGURE 3.1 : Taux de maturité global PSSIE

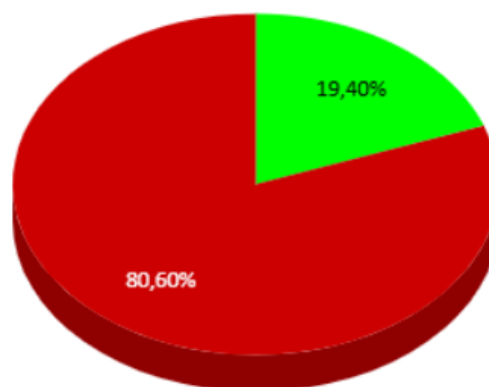


FIGURE 3.2 : Taux de maturité global ISO 27001

Les résultats détaillés qui suivront fourniront une vue d'ensemble des zones critiques nécessitant une action rapide et rigoureuse pour aligner les pratiques existantes sur les standards imposés.

Les tableaux suivants présentent le récapitulatif des niveaux de maturité.

Objectifs de sécurité	Niveau de maturité
Sécurité des e-services	0%
Sécurité du cloud computing	0%
Gestion de la continuité de la sécurité du SI	3%
Mesures cryptographiques	4%
Sécurité des équipements itinérants	5%
Organisation de la sécurité des SI	6%
Gestion des incidents de sécurité	6%
Relations avec les fournisseurs	8%
Conformité, audit et contrôles de sécurité	8%
Sécurité des réseaux informatiques	10%
Sécurité du poste de travail utilisateur	11%
Sécurité physique des locaux abritant les actifs SI	13%
Sécurité des applications Web	13%
Gestion des actifs du système d'information	18%
Sécurité des ressources humaines	19%
Sécurité liée à l'exploitation des SI	19%
Sécurité dans l'acquisition, le développement et la maintenance des SI	19%
Contrôle d'accès logique au système d'information	23%
TOTAL	11,56%

FIGURE 3.3 : Tableau récapitulatif des niveaux de maturité PSSIE.

Objectifs de sécurité	Niveau de maturité
5. Mesures de sécurité organisationnelles	14%
6 Mesures de sécurité applicables aux personnes	20%
7 Mesures de sécurité physique	28%
8 Mesures de sécurité technologiques	16%
TOTAL	19,40%

FIGURE 3.4 : Tableau récapitulatif des niveaux de maturité ISO.

3.2 Présentation des objectifs de sécurité et leur niveau de maturité

3.2.1 Sécurité des e-services (0%)

Le score de 0% pour la sécurité des e-services est alarmant mais compréhensible. Bien que la CAGD n'ait actuellement pas implémenté d'e-services, il est crucial de préparer une stratégie proactive pour

leur sécurisation à mesure que l'institution évolue. Cela inclut l'identification des futurs besoins en services numériques, l'évaluation des risques potentiels et la mise en place de politiques de sécurité adaptées. En anticipant ces besoins, la [CAGD](#) pourra éviter des vulnérabilités critiques au moment de l'introduction de ces services. Les e-services ne sont pas utilisés par l'institution. Cet objectif de sécurité est alors non-applicable et n'est pas pris en compte dans le calcul du niveau de maturité total.

3.2.2 Sécurité du cloud computing (0%)

Le cloud computing est aujourd'hui un pilier fondamental des infrastructures [IT](#) modernes. Un score de 0% dans cette catégorie reflète un manque total de stratégies de sécurité pour la gestion des données dans le cloud. L'institution est exposée à des risques comme la perte de données, les violations de confidentialité, ou l'exploitation non autorisée des ressources cloud. Ce niveau de maturité peut s'expliquer par une adoption tardive des solutions cloud ou une absence de gouvernance claire pour la sécurité des services externalisés. Il est urgent de développer des politiques de gestion des risques spécifiques au cloud, comme l'utilisation de solutions de chiffrement dans le cloud et la mise en place d'accords de niveau de service ([SLA](#)) avec les fournisseurs. Les services cloud ne sont pas utilisés par l'institution. Cet objectif de sécurité est alors non-applicable et n'est pas pris en compte dans le calcul du niveau de maturité total.

3.2.3 Gestion de la continuité de la sécurité du [SI](#) (3%)

Avec un niveau de maturité de seulement 3%, la gestion de la continuité de la sécurité des systèmes d'information est quasiment inexistante. Ce score bas reflète l'absence de plans de secours à jour ou de stratégies efficaces de reprise après sinistre, éléments essentiels en cas de cyberattaque ou de défaillance majeure. Cette lacune expose l'institution à des interruptions prolongées des activités, compromettant ainsi sa résilience opérationnelle. Bien que la [CAGD](#) dispose d'un Plan de Continuité Informatique ([PCI](#)), celui-ci est très ancien et n'a pas été mis à jour depuis longtemps, ce qui le rend inefficace face aux menaces actuelles. Il est impératif de revoir ce [PCI](#) pour qu'il prenne en compte les dernières évolutions technologiques et les risques émergents. La mise en place de sauvegardes redondantes, d'exercices de simulation réguliers et de tests de continuité permettra d'assurer la disponibilité des systèmes en toutes circonstances.

3.2.4 Mesures cryptographiques (4%)

Les mesures cryptographiques assurent la confidentialité et l'intégrité des données, mais avec un score de 4%, l'institution ne protège presque pas les informations sensibles. Ce faible niveau pourrait s'expliquer par l'absence de solutions de chiffrement des données au repos et en transit, ou par une non-application des bonnes pratiques de gestion des clés de chiffrement. En conséquence, les données confidentielles de l'institution peuvent être vulnérables aux attaques de type interception ou vol. L'adoption de normes de chiffrement, et l'utilisation de certificats numériques pour authentifier les échanges doivent être des priorités.

3.2.5 Sécurité des équipements itinérants (5%)

Les équipements itinérants (smartphones, ordinateurs portables) sont souvent des vecteurs d'attaques en raison de leur mobilité. Un score de 5% dans ce domaine signifie que très peu de mesures

de protection sont en place pour ces équipements, ce qui les rend vulnérables au vol physique ou aux attaques via des réseaux non sécurisés. Le faible niveau de maturité pourrait s'expliquer par l'absence de gestion de la mobilité, de chiffrement des disques ou de politiques de verrouillage automatique. Il est essentiel de mettre en place des outils pour gérer et protéger ces appareils, comme le chiffrement des données, le suivi à distance, et des politiques de sécurité rigoureuses.

3.2.6 Organisation de la sécurité des SI (6%)

Le score de 6% montre que la sécurité des systèmes d'information n'est pas suffisamment organisée. Cela peut être dû à une absence de structure claire, où les rôles et responsabilités en matière de sécurité ne sont pas définis. Ce manque de clarté et de coordination dans la gestion de la sécurité affaiblit la capacité de l'institution à réagir face aux menaces. Il est indispensable de définir une gouvernance claire, avec des responsables désignés, des procédures formalisées et un cadre de gestion des risques, pour permettre une amélioration rapide dans ce domaine.

3.2.7 Gestion des incidents de sécurité (6%)

La gestion des incidents de sécurité est également très faible avec un score de 6%. Cela signifie que l'institution ne dispose ni de processus de détection ni de réponse efficace aux incidents de sécurité. En cas de cyberattaque ou d'incident majeur, l'institution pourrait subir des interruptions prolongées et des pertes de données importantes. Ce niveau de maturité reflète probablement l'absence d'une équipe dédiée à la réponse aux incidents ou de procédures automatisées pour détecter et signaler les anomalies. La mise en place d'un centre d'opérations de sécurité (SOC) ou de systèmes de détection des intrusions améliorera considérablement ce score.

3.2.8 Relations avec les fournisseurs (8%)

Les relations avec les fournisseurs en matière de sécurité sont insuffisantes, avec un score de 8%. L'institution n'a pas mis en place de contrôles stricts sur la manière dont ses fournisseurs gèrent les informations sensibles ou accèdent à son infrastructure. Ce niveau de maturité faible peut s'expliquer par un manque de contrats de sécurité avec les tiers ou l'absence de processus de vérification continue de la sécurité chez les fournisseurs. L'institution doit renforcer ses contrats avec ses partenaires, en incluant des clauses spécifiques sur la sécurité, et s'assurer que des audits de sécurité soient réalisés régulièrement sur ses fournisseurs.

3.2.9 Conformité, audit et contrôles de sécurité (8%)

La conformité et l'audit de sécurité sont des piliers essentiels pour assurer une gestion proactive des risques, mais avec un score de 8%, l'institution montre qu'elle ne respecte pas pleinement les normes de sécurité. Cela indique aussi un manque de mécanismes pour vérifier l'efficacité des contrôles de sécurité en place. Des audits réguliers permettraient de révéler les failles et de s'assurer que les politiques sont respectées. Il est essentiel de formaliser un programme d'audit régulier et de veiller à ce que l'institution respecte les cadres de conformité pertinents.

3.2.10 Sécurité des réseaux informatiques (10%)

Avec un niveau de maturité de 10%, la sécurité des réseaux informatiques est un domaine où certaines mesures existent, mais elles restent insuffisantes pour assurer une protection adéquate contre

les cybermenaces modernes. Ce faible niveau peut s'expliquer par une absence de segmentation réseau, de surveillance proactive ou de pare-feu correctement configuré. Une mauvaise gestion des règles de sécurité sur les équipements réseau ou un manque d'investissements dans des solutions de détection et de prévention des intrusions sont souvent des causes de ces faiblesses. Des améliorations dans la modernisation, la surveillance des réseaux et le renforcement des contrôles d'accès sont essentiels pour augmenter ce score.

3.2.11 Sécurité du poste de travail utilisateur (11%)

Le score de 11% dans ce domaine reflète que la sécurité des postes de travail, bien qu'étant légèrement supérieure aux autres domaines, est toujours insuffisante pour garantir une protection solide contre les menaces courantes. Cela peut être dû à des lacunes dans la mise à jour des logiciels, des configurations de sécurité mal gérées ou un manque de contrôle sur l'installation de logiciels non autorisés. Les utilisateurs, souvent maillon faible de la chaîne de sécurité, peuvent être mieux protégés grâce à un programme de sensibilisation combiné à des solutions telles que l'authentification à deux facteurs et une gestion efficace des correctifs.

3.2.12 Sécurité physique des locaux abritant les actifs SI (13%)

La sécurité physique des locaux montre une meilleure maturité avec un score de 13%. Cela signifie que l'institution a mis en place certaines mesures pour protéger ses installations, telles que des contrôles d'accès physiques, mais que ces protections sont encore trop basiques ou mal appliquées. Par exemple, l'absence de caméras de surveillance à des endroits importants, de procédures de vérification des accès peut exposer les installations à des intrusions. Renforcer les mesures de contrôle d'accès physique et mettre en place une surveillance 24/7 peuvent améliorer considérablement ce niveau de maturité.

3.2.13 Sécurité des applications Web (13%)

La sécurité des applications Web est essentielle pour protéger les interfaces de l'institution contre les cyberattaques. Avec un score de 13%, les mesures en place ne sont pas suffisantes pour contrer des menaces telles que les injections [SQL](#) ou les attaques par script intersite ([XSS](#)). Ce manque de maturité peut provenir de l'absence de tests réguliers de sécurité sur les applications, ou d'une non-application des pratiques de développement sécurisé. La formation des développeurs et l'intégration d'outils d'analyse de vulnérabilités dans le cycle de développement sont des étapes clés pour améliorer ce score.

3.2.14 Gestion des actifs du système d'information (18%)

Avec un score de 18%, l'institution démontre une meilleure gestion de ses actifs informatiques. Cependant, il est probable que l'inventaire des actifs ne soit pas exhaustif ou que leur gestion soit encore partiellement manuelle, augmentant ainsi les risques de pertes d'information ou de mauvaise gestion des actifs critiques. L'adoption d'une solution d'inventaire automatisé, couplée à une gouvernance stricte des cycles de vie des actifs, améliorerait la gestion, la traçabilité et la protection des ressources critiques.

3.2.15 Sécurité de la gestion des habilitations (18%)

La gestion des habilitations, avec un score de 18%, montre que des efforts ont été faits pour gérer les droits d'accès aux ressources sensibles. Cependant, ce niveau de maturité laisse supposer que des failles existent, comme la non-révocation rapide des accès des utilisateurs quittant l'institution ou l'absence de politiques de droits minimaux. L'institution doit adopter une approche de gestion des accès basée sur les rôles et respecter le principe du moindre privilège, avec des processus rigoureux pour octroyer, modifier et révoquer les droits d'accès.

3.2.16 Sécurité des ressources humaines (19%)

La sécurité des ressources humaines est relativement plus avancée que les autres domaines avec un score de 19%. Cela inclut probablement une formation initiale en matière de cybersécurité pour les nouveaux employés, mais des lacunes peuvent subsister dans la formation continue et la sensibilisation aux menaces émergentes. Par ailleurs, des procédures de gestion des accès pour les employés et les sous-traitants doivent être renforcées, notamment pour garantir que les accès sont révoqués dès la fin des contrats ou des missions. L'institution doit aussi mettre en place des programmes de sensibilisation réguliers pour renforcer la vigilance des employés face aux attaques de phishing, et instaurer une culture de la sécurité proactive. La réalisation de vérifications approfondies des antécédents des employés avant leur embauche, ainsi que l'intégration de clauses de sécurité dans les contrats des prestataires, contribuerait à améliorer la sécurité globale de l'organisation.

3.2.17 Sécurité liée à l'exploitation des systèmes d'information (19%)

Avec un niveau de maturité de 19%, la sécurité liée à l'exploitation des SI montre que certaines pratiques sont mises en place, mais elles ne sont pas encore suffisantes pour garantir une protection adéquate des infrastructures informatiques. Cela peut inclure des lacunes dans la gestion des correctifs de sécurité, des mises à jour logicielles non régulières, ou encore l'absence de surveillance proactive des systèmes pour détecter des comportements anormaux. L'institution devrait se concentrer sur la mise en place de processus automatiques de mise à jour, l'intégration d'outils de surveillance et de détection d'intrusions ([IDS/IPS](#)), ainsi que des mécanismes de gestion des vulnérabilités. En outre, des tests de pénétration réguliers doivent être effectués pour identifier et corriger les failles avant qu'elles ne soient exploitées.

3.2.18 Sécurité dans l'acquisition, le développement et la maintenance des SI (19%)

Avec un score de 19%, il est clair que la sécurité dans l'acquisition, le développement et la maintenance des systèmes d'information n'est pas encore pleinement intégrée dans le cycle de vie des projets informatiques. L'absence d'une approche « sécurité dès la conception » (Security by Design) signifie que les systèmes développés ou acquis peuvent être vulnérables à des failles dès leur déploiement. De plus, des audits de sécurité doivent être réalisés après chaque phase de développement et avant la mise en production pour garantir que les exigences de sécurité sont respectées. Une formation spécifique aux équipes techniques sur les meilleures pratiques de sécurité dans le développement logiciel est également recommandée pour prévenir les failles courantes comme l'injection [SQL](#) ou les attaques [XSS](#) sans oublier de mentionner la sécurité des réseaux, infrastructures etc...

3.2.19 Contrôle d'accès logique au système d'information (23%)

Le contrôle d'accès logique au système d'information affiche un score de 23%, indiquant que l'institution a mis en place des mécanismes de base pour gérer les accès aux systèmes d'information. Cependant, ce score montre que ces mécanismes ne sont pas suffisamment robustes pour protéger efficacement les données sensibles et les systèmes critiques. Il est possible que l'authentification repose encore sur des méthodes obsolètes, ou que le principe du moindre privilège ne soit pas correctement appliqué. L'institution doit renforcer ses politiques de gestion des accès en mettant en œuvre des solutions modernes d'authentification multi-facteurs (MFA), et en s'assurant que les accès sont revus régulièrement pour éviter les comptes dormants ou sur-privilégiés. Il est également crucial d'automatiser ou de mieux organiser la gestion des droits d'accès pour s'assurer que les utilisateurs quittant l'organisation voient leurs privilèges révoqués immédiatement.

3.3 Recommandations formulées

3.3.1 Définir et faire valider une politique de sécurité

Le côté formel d'une politique de sécurité est aujourd'hui une obligation pour tout organisme intéressé par la sécurité de son SI, c'est pourquoi il est nécessaire que cette politique soit écrite et mise à disposition de tout le personnel. Il s'agira de :

- Rédiger une politique de sécurité qui définit clairement les objectifs en termes de sécurité ;
- Définir des procédures documentées de gestion des incidents de sécurité, sauvegarde des données, gestion de la continuité, gestion de l'authentification des utilisateurs du réseau ;
- S'assurer que la politique soit validée et accompagnée par la Direction Générale ;
- Désigner un comité qui aura pour mission le suivi de l'état de sécurité et de prendre les décisions nécessaires,
- Définir une organisation informatique formelle dotée de manuels, de guides de procédures, de politiques et des chartes d'utilisation,
- Définir les responsabilités (en termes de sécurité) de chaque utilisateur du SI à travers les fiches de poste.

3.3.2 Classifier les ressources

Pour optimiser la gestion des ressources et prévenir les menaces associées à leur usage, nous conseillons vivement de :

- Adopter une charte de bon usage des ressources informatiques.
- Mettre en place une classification des informations sensibles de l'institution. Cette classification doit reposer sur les trois piliers de la sécurité de l'information : Disponibilité, Intégrité et Confidentialité, afin de leur attribuer le niveau de protection adéquat.

3.3.3 Définir une charte de confidentialité

L'utilisation des ressources du SI peut affecter négativement sa robustesse face aux failles de sécurité. Pour remédier à cette situation, nous recommandons de :

- Diffuser à l'ensemble du personnel ayant accès au SI une charte de sécurité relative à l'utilisation des ressources informatiques, et s'assurer du respect de cette charte. Il est possible de profiter de cette occasion pour aussi fournir/rappeler toute documentation utile (Reglement Interieur, Plan Stratégique etc)
- Intégrer une clause de confidentialité dans les contrats de chaque utilisateur, y compris les contractuels et les stagiaires. Les nouveaux utilisateurs du SI doivent être informés de la politique de sécurité de l'institution dès leur prise de fonction.

3.3.4 Instaurer l'auto-évaluation comme une pratique fondamentale

Ce travail constitue une première pour le Département des Systèmes d'Information, marquant ainsi la réalisation de sa toute première auto-évaluation en matière de sécurité. Cette démarche novatrice met en lumière l'importance cruciale de l'évaluation régulière des systèmes et de la mise en conformité avec les normes de sécurité. Afin de garantir la pérennité et la robustesse de nos infrastructures, il est recommandé d'instaurer l'audit comme une pratique standard et récurrente. Cela permet non seulement d'identifier les vulnérabilités potentielles, mais aussi d'adopter une approche proactive pour renforcer la sécurité de manière continue. Nous recommandons de planifier des audits de manière régulière (au moins une fois par an) afin de mesurer le niveau de sécurité de l'organisation et de s'assurer de l'efficacité des procédures de gestion des risques. Il est également judicieux de faire appel au Département de l'Audit Interne et de la Conformité pour accompagner ces évaluations, garantir une meilleure coordination et assurer le suivi des actions correctives.

3.3.5 Sensibiliser et former l'ensemble du personnel

Les mesures mises en place pour sécuriser le Système d'Information (SI) ne seront pleinement efficaces que si l'ensemble du personnel est conscient de l'importance de la sécurité et capable d'identifier les bonnes pratiques qui protègent le SI des diverses menaces. À cet effet, nous recommandons de :

- Sensibiliser et former le personnel aux menaces potentielles, telles que les intrusions dans le système d'information, et à l'importance cruciale de la sécurité pour protéger l'organisation.
- Planifier des cycles de formation spécifiques et approfondis en sécurité pour tout le service informatique.
- Encourager les responsables du service informatique à renforcer leurs connaissances, notamment en favorisant les programmes de formation continue et les cycles de certification.

3.3.6 Protéger les ressources et les actifs

La protection physique des ressources constitue l'un des enjeux majeurs en matière de sécurité. Nous recommandons les mesures suivantes :

- S'assurer que les actifs les plus critiques sont protégés contre tout risque potentiel, tels que les fuites d'eau, l'humidité, et les surtensions électriques. Il est également nécessaire de remettre la salle serveurs aux normes de sécurité recommandées.
- Les supports contenant les sauvegardes de secours doivent être conservés dans des armoires ignifuges et fortement sécurisés. De plus, ils ne doivent pas être stockés dans le même lieu que les versions originales pour éviter tout risque de perte simultanée.
- Prévoir des mesures spécifiques pour garantir une alimentation électrique continue. Nous avons remarqué que certaines pannes électriques répétées rendent indisponible les infrastructures critiques de l'insitution.

3.3.7 Contrôle de l'abandon et de la destruction des supports

L'abandon des supports physiques et logiques ne fait actuellement l'objet d'aucun contrôle. Il est donc vivement recommandé de définir une politique claire pour la destruction des équipements sensibles ainsi que pour l'élimination des supports contenant des informations confidentielles. Afin de garantir que les informations critiques ne puissent être récupérées ou divulguées, nous préconisons l'acquisition d'un dispositif de démagnétisation, qui permet de détruire définitivement les anciens disques durs.

3.3.8 Modernisation de l'architecture du réseau

Une architecture réseau fiable est essentielle pour garantir le succès d'un organisme ainsi que la sécurité de son Système d'Information (SI). Pour améliorer l'architecture actuelle, nous recommandons les mesures suivantes :

- Créer une zone [DMZ](#) pour protéger les actifs critiques.
- Sécuriser les accès distants entre les serveurs via une authentification par certificat et l'utilisation de canaux de communication sécurisés ([SSH](#), [IPsec](#)).
- Créer une zone d'administration permettant aux responsables de contrôler le réseau de manière sécurisée et efficace.
- Développer des procédures de configuration sécurisée pour les équipements informatiques du réseau
- Définir et mettre à jour les listes de contrôle d'accès ([ACL](#)) sur ces équipements.
- Mettre en place une solution de redondance pour ces équipements ainsi que les actifs critiques.

3.3.9 Amélioration de la méthodologie d'administration

Au cours de notre mission, nous avons observé que la méthodologie d'administration actuelle manque de flexibilité et que certaines tâches administratives sont lourdes à gérer. Nous proposons les actions suivantes :

- Pour les ressources critiques (comme les serveurs), appliquer la stratégie de « restriction totale » puis n'accorder l'accès qu'aux personnes autorisées.

- Le compte administrateur ne doit être utilisé qu'en cas d'extrême nécessité. Pour se connecter au serveur chaque utilisateur autorisé devra obligatoirement utiliser son compte domaine.
- Normaliser et standardiser les postes de travail
- Limiter l'abus des privilèges utilisateurs : interdire l'installation de clients [P2P](#), le streaming, etc.,
- Mettre en place des solutions de contrôle des applications installées sur les postes utilisateurs.

3.3.10 Formalisation de la gestion des utilisateurs

La gestion des utilisateurs n'est actuellement pas formalisée. Il est essentiel de définir une méthodologie claire pour standardiser cette gestion. Nous recommandons la création d'un document décrivant les droits d'accès pour les différents systèmes de l'organisation. Par conséquent, il est nécessaire de formaliser au minimum les procédures suivantes :

- La création d'un nouvel utilisateur sur les systèmes d'exploitation et les applications.
- La modification d'un profil utilisateur en cas de changement d'affectation.
- La gestion de l'identification des utilisateurs,
- Le départ d'un utilisateur (démission, congé ou départ à la retraite, etc).
- La revue ou l'audit de la sécurité logique des systèmes et des applications.
- Définir une politique stricte d'expiration automatique des mots de passe non renouvelés.

3.3.11 Mise en place d'une plateforme de support technique

La création d'une plateforme de support technique est recommandée pour gérer efficacement les requêtes des utilisateurs, que ce soit pour le support technique, le dépannage ou les améliorations. [GLPI](#) étant présent, nous recommandons de l'adopter pour une gestion efficace des tickets. Une telle solution offre les avantages suivants :

- Un classement efficace des requêtes,
- Une adhésion à une démarche claire pour le traitement des demandes,
- Un suivi détaillé des actions en cours,
- Des statistiques sur les problèmes récurrents, leurs sources et les solutions possibles.

3.4 Plan d'action

3.4.1 Élaboration d'un plan d'implémentation

L'élaboration d'un plan d'implémentation structuré est essentielle pour garantir que les recommandations issues de l'évaluation soient correctement appliquées et que les objectifs de sécurité soient

atteints. Ce plan doit inclure une approche méthodique permettant de piloter l'exécution des mesures, tout en prenant en compte les ressources disponibles et les contraintes de l'organisme.

Dans ce cadre, plusieurs sujets spécifiques ont été attribués à différents collaborateurs, chacun travaillant dessus comme des projets indépendants. Ces sujets couvrent des aspects divers tels que l'amélioration de l'architecture réseau, la révision des procédures de gestion des utilisateurs, ou encore le renforcement de la politique de sécurité. Chaque projet, bien que supervisé globalement, est géré de manière autonome, ce qui permet une spécialisation et un suivi plus rigoureux.

Le plan d'implémentation propose une série d'étapes claires à suivre, comprenant la définition des tâches à accomplir, l'assignation des responsabilités aux parties prenantes, la définition des délais de réalisation, ainsi que le suivi régulier des progrès. Nous avons également prévu une évaluation périodique de la mise en œuvre des recommandations afin de corriger les écarts et garantir l'atteinte des résultats attendus.

3.4.1.1 Assignation des responsabilités

La réussite de la mise en œuvre des recommandations de sécurité repose en grande partie sur une assignation claire des responsabilités à chaque acteur impliqué dans le processus. Il est crucial de définir un rôle précis pour chaque membre du personnel, en fonction de ses compétences, de son niveau d'autorité, et de son domaine d'expertise. Pour ce faire, nous avons procédé de la manière suivante :

- Identifier les personnes ou les départements responsables de la mise en œuvre des actions de sécurité (par exemple, le Département des Systèmes d'Information, le Responsable de la Sécurité Informatique, etc.).
- Désigner un chef de projet ou un coordinateur chargé de superviser l'exécution du plan et de s'assurer que les différentes actions sont bien alignées.
- Clarifier les rôles des équipes techniques, des gestionnaires de projet, et des autres parties prenantes, en précisant leurs responsabilités respectives, notamment en matière de gestion des risques, d'application des correctifs, et de formation des utilisateurs.
- Intégrer le Département d'Audit Interne et de Conformité pour un suivi continu et une évaluation objective des progrès réalisés.
- Veiller à ce que les sujets pris en charge en tant que projets indépendants soient coordonnés de manière globale, tout en assurant une gestion autonome de chaque volet par les équipes dédiées.
- Établir un échéancier global pour l'implémentation des mesures, en tenant compte des priorités identifiées lors de l'audit. Les actions liées aux failles critiques doivent être réalisées en priorité.
- Fixer des jalons intermédiaires afin de mesurer les progrès et d'assurer que les actions sont bien avancées. Ces jalons permettent également de réajuster les délais en cas d'obstacles ou de retards imprévus.

3.5 Discussions

L'audit de la sécurité mené au sein de la [CAGD](#) a révélé un certain nombre de vulnérabilités importantes. Les mesures techniques, telles que la segmentation du réseau, la mise à jour des systèmes obsolètes et bien d'autres sujets, sont en cours d'implémentation. Toutefois, les résultats montrent que la pleine efficacité de ces actions dépendra de la rapidité avec laquelle elles seront réalisées et de la capacité à les intégrer dans une démarche globale de sécurité.

Le processus de mise en œuvre des recommandations a fait face à plusieurs défis. Premièrement, la résistance au changement de certains utilisateurs, particulièrement en ce qui concerne l'application des nouvelles politiques de sécurité. Ensuite, le manque de flexibilité et la lourdeur administrative limite considérablement la rapidité d'exécution de certaines actions critiques, telles que l'acquisition d'équipements de protection avancés (pare-feu, onduleurs, etc.).

Les recommandations proposées à l'issue de l'audit se sont révélées globalement pertinentes et réalistes compte tenu du contexte de la [CAGD](#). Pour améliorer la sécurité de manière pérenne, il est crucial de renforcer l'engagement de la Direction Générale et de prévoir un budget spécifique pour la sécurité informatique. La mise en place d'audits réguliers, combinée à des mécanismes de surveillance continue, garantira une évaluation en temps réel des mesures prises et permettra de réagir rapidement en cas de nouvelles menaces. De plus, l'intégration de nouveaux outils de gestion des incidents et la formation des équipes sur des technologies émergentes contribueront à renforcer la résilience du SI face à des cyberattaques de plus en plus sophistiquées.

Conclusion

En conclusion, cet audit représente une étape essentielle dans la sécurisation du système d'information de la [CAGD](#). Grâce à une analyse approfondie, il a permis d'identifier les vulnérabilités critiques et de proposer des recommandations concrètes pour renforcer la sécurité sur les plans organisationnel, technique et physique. Les efforts fournis ont permis de jeter les bases d'une gouvernance de la sécurité structurée, notamment à travers la formalisation des processus, la modernisation de l'infrastructure et la mise en place de politiques adaptées.

Cependant, la réussite de cette démarche repose sur la mise en œuvre effective des recommandations, soutenue par un engagement fort de la Direction Générale et une allocation adéquate des ressources financières et humaines. La résistance au changement, observée chez certains utilisateurs, doit être traitée par des actions de sensibilisation et une communication transparente, afin d'instaurer une culture de sécurité partagée au sein de l'institution.

La prise en compte des recommandations dans les délais prévus représente un enjeu majeur pour garantir l'efficacité des actions correctives proposées. Respecter ces échéances permettra à la [CAGD](#) de réduire rapidement les vulnérabilités identifiées, tout en renforçant la résilience de son système d'information. Cette démarche doit s'appuyer sur une planification rigoureuse et un suivi régulier des progrès, afin de s'assurer que chaque mesure est mise en œuvre conformément au calendrier défini.

Ainsi, cet audit ne doit pas être perçu comme une fin, mais comme le point de départ d'une démarche d'amélioration continue. La [CAGD](#) se positionne ainsi sur la voie de la modernisation et de la pérennité de sa sécurité, garantissant à la fois la protection de ses actifs et la confiance de ses Partenaires Techniques et Financiers.

Bibliographie

- [1] Décret n° 2021-550 du 20 octobre 2021 portant approbation de la Politique de Sécurité des Systèmes d'Information de l'État en République du Bénin. Secrétariat Général du Gouvernement. Disponible en ligne : <https://sgg.gouv.bj/doc/decret-2021-550/download>

Webographie

- [2] <https://www.deessi.si/audit-de-systeme-dinformation-4-bonnes-pratiques-de-pilotage/> consulté le 05/04/2024
- [3] <https://www.globalsuitesolutions.com/fr/iso-27000-et-l-ensemble-de-normes-de-securite-de-la-information/> consulté le 05/04/2024
- [4] <https://wikimemoires.net/2012/11/iso-et-historique-des-normes-en-matiere-de-securite-de-linformation/#:~:text=En%202000%2C%20la%20norme%20BS7799,ISO%2FIEC%2017799%3A%202000.> consulté le 20/12/2024
- [5] <https://www.cagd.bj/missions-attributions/> consulté le 20/12/2024
- [6] <https://cdn.standards.iteh.ai/samples/41933/cb9ac91928514170941c5bdeabe2cc36/ISO-IEC-27000-2009.pdf> consulté le 05/04/2024
- [7] <https://www.iso.org/fr/standards.html> consulté le 05/04/2024
- [8] <https://www.iso27001security.com/html/27004.html> consulté le 05/04/2024
- [9] <https://www.google.com/search?client=firefox-b-d&q=definition+audit+de+securit%C3%A9+d%27un+syst%C3%A8me+d%27information> consulté le 05/04/2024
- [10] <https://dln7iqsz6ob2ad.cloudfront.net/document/pdf/54a6749569414.pdf> consulté le 05/04/2024
- [11] <https://docplayer.fr/781230-Memoire-de-stage-de-fin-d-etude-audit-de-securite-du-systeme-informatique-de-mtic.html> consulté le 05/04/2024
- [12] <https://carrieres.groupeozitem.com/blog/auditer-systeme-information> consulté le 06/04/2024
- [13] <https://pro-it-consulting.com/audit-technique-systeme-dinformation> consulté le 06/04/2024
- [14] <https://www.iso.org/fr/about-us.html> consulté le 06/04/2024
- [15] https://www.utc.fr/master-qualite/public/publications/MQ_M2/2017-2018/MIM_projets/qpo12_2018_gr08_secu_info/index.html consulté le 06/04/2024

-
- [16] <https://feelagile.com/quest-ce-quun-smsi/> consulté le 08/04/2024
- [17] <https://openclassrooms.com/fr/courses/1734201-definissez-la-politique-de-securite-de-votre-entreprise/6206511-apprehendez-la-mise-en-place-d-un-smsi> consulté le 08/04/2024
- [18] <https://www.cairn.info/audit-interne-et-referentiels-de-risques--9782100819683-page-173.htm> consulté le 09/04/2024
- [19] <https://www.l-expert-comptable.com/a/529542-la-methodologie-d-audit.html> consulté le 09/04/2024
- [20] <https://openclassrooms.com/fr/courses/1734211-analysez-et-gerez-des-risques-si/6477061-identifiez-le-cadre-normatif-de-l-analyse-de-risques-si> consulté le 16/04/2024
- [21] <https://www.pqb.fr/platform.php?i=&if=222&ch=6472> consulté le 17/04/2024

Table des matières

Dédicace	ii
.....	ii
Remerciements	iii
Résumé/Abstract	iv
Liste des Figures	vi
Liste des Tableaux	vii
Sigles et Abréviations	viii
Introduction	1
1 Revue de littérature	3
Introduction	3
1.1 Généralités sur les audits	3
1.1.1 Définition d'un audit	3
1.1.2 Rôle et objectif	3
1.1.3 Cycle de vie d'un audit de sécurité des systèmes d'information	4
1.1.4 Démarche de réalisation	4
1.1.4.1 Définition de la charte d'audit	5
1.1.4.2 Préparation de l'audit	5
1.1.4.3 Audit organisationnel et physique	5
1.1.4.4 Audit technique	6
1.1.4.5 Test d'intrusions (Audit intrusif)	6
1.1.4.6 Rapport de mission	6
1.2 Méthodes et normes (Référentiels)	6
1.2.1 Définitions	6
1.2.1.1 Méthode d'audit	6
1.2.1.2 Référentiels	7
1.2.2 Quelques méthodologies d'analyse des risques	7
1.2.2.1 La méthode EBIOS	7
1.2.2.2 La méthode MEHARI	7
1.2.2.3 La méthode OCTAVE	8
.....	8
1.2.2.4 L'ISO (Organisation Internationale de Normalisation)	9
1.2.2.5 Les normes	9

1.2.2.6	Historique des normes en matière de sécurité de l'information [4]	10
1.2.2.7	La série des normes de la famille ISO 27000 [4]	10
1.2.2.8	ISO/CEI 27000	11
1.2.2.9	ISO/CEI 27001	11
1.2.2.10	ISO/CEI 27002	11
1.2.2.11	ISO/CEI 27003	11
1.2.2.12	ISO/CEI 27004	11
1.2.2.13	ISO/CEI 27005	11
1.2.2.14	ISO/CEI 27006	11
1.2.2.15	ISO/CEI 27007	12
1.2.3	Autres cadres de sécurité de l'information	12
1.2.3.1	NIST Cybersecurity Framework	12
1.2.3.2	PCI DSS (Payment Card Industry Data Security Standard)	13
1.2.3.3	GDPR (General Data Protection Regulation)	13
1.2.3.4	ITIL (Information Technology Infrastructure Library)	13
1.2.3.5	La Politique de Sécurité des Systèmes d'Information (PSSI)	13
1.3	Les systèmes de management	13
1.3.1	Les principaux systèmes de management	14
1.3.2	L'apport des systèmes de management	14
1.3.3	Les systèmes de management de la sécurité de l'information (SMSI)	15
1.3.3.1	Les 4 phases de la démarche PDCA selon la norme 27001	16
Conclusion		17
2	Méthodologie d'évaluation	18
2.1	Présentation de la CAGD	18
2.1.1	Historique et cadre juridique	18
2.1.1.1	Contexte historique	18
2.1.1.2	Cadre juridique et conformité	18
2.1.2	Mission et Objectifs [5]	19
2.1.2.1	Mission et objectifs généraux	19
2.1.2.2	Rôle dans l'administration financière	19
2.1.3	Rôle critique dans la gestion de la dette publique	19
2.1.4	Impact des failles de sécurité sur la gestion des finances publiques	19
2.1.5	Périmètre de l'audit	20
2.1.6	Personnes ressources	20
2.1.7	Planning de la mission	21
2.1.8	Politique de Sécurité des Systèmes d'Information de l'État (PSSIE)	21
2.1.8.1	Objectifs clés de la PSSIE	21
2.1.8.2	Déploiement et fonctions	22
2.1.8.3	Objectifs et règles de sécurité	22
		22
2.1.9	Evaluation des aspects organisationnels et physiques	24
2.1.10	Evaluation technique	24
2.1.11	Rapport d'évaluation	25
2.2	Description du système d'information	25

2.2.1	Description de l'architecture	25
2.2.2	Mesures de sécurité existantes	26
2.2.2.1	Sécurité réseaux	26
2.2.2.2	Sécurité physique	26
2.2.2.3	Sécurité logique	26
2.2.2.4	Sécurité des machines	27
2.3	Audit organisationnel et physique	27
2.3.1	Questionnaire d'audit	27
3	Résultats & Recommandations	31
3.1	Présentation des résultats	31
3.2	Présentation des objectifs de sécurité et leur niveau de maturité	32
3.2.1	Sécurité des e-services (0%)	32
3.2.2	Sécurité du cloud computing (0%)	33
3.2.3	Gestion de la continuité de la sécurité du SI (3%)	33
3.2.4	Mesures cryptographiques (4%)	33
3.2.5	Sécurité des équipements itinérants (5%)	33
3.2.6	Organisation de la sécurité des SIs (6%)	34
3.2.7	Gestion des incidents de sécurité (6%)	34
3.2.8	Relations avec les fournisseurs (8%)	34
3.2.9	Conformité, audit et contrôles de sécurité (8%)	34
3.2.10	Sécurité des réseaux informatiques (10%)	34
3.2.11	Sécurité du poste de travail utilisateur (11%)	35
3.2.12	Sécurité physique des locaux abritant les actifs SI (13%)	35
3.2.13	Sécurité des applications Web (13%)	35
3.2.14	Gestion des actifs du système d'information (18%)	35
3.2.15	Sécurité de la gestion des habilitations (18%)	36
3.2.16	Sécurité des ressources humaines (19%)	36
3.2.17	Sécurité liée à l'exploitation des systèmes d'information (19%)	36
3.2.18	Sécurité dans l'acquisition, le développement et la maintenance des SI (19%)	36
3.2.19	Contrôle d'accès logique au système d'information (23%)	37
3.3	Recommandations formulées	37
3.3.1	Définir et faire valider une politique de sécurité	37
3.3.2	Classier les ressources	37
3.3.3	Définir une charte de confidentialité	38
3.3.4	Instaurer l'auto-évaluation comme une pratique fondamentale	38
3.3.5	Sensibiliser et former l'ensemble du personnel	38
3.3.6	Protéger les ressources et les actifs	38
3.3.7	Contrôle de l'abandon et de la destruction des supports	39
3.3.8	Modernisation de l'architecture du réseau	39
3.3.9	Amélioration de la méthodologie d'administration	39
3.3.10	Formalisation de la gestion des utilisateurs	40
3.3.11	Mise en place d'une plateforme de support technique	40
3.4	Plan d'action	40
3.4.1	Élaboration d'un plan d'implémentation	40

3.4.1.1	Assignment des responsabilités	41
3.5	Discussions	42
Conclusion		43
Bibliographie		44
Webographie		45
Table des matières		47