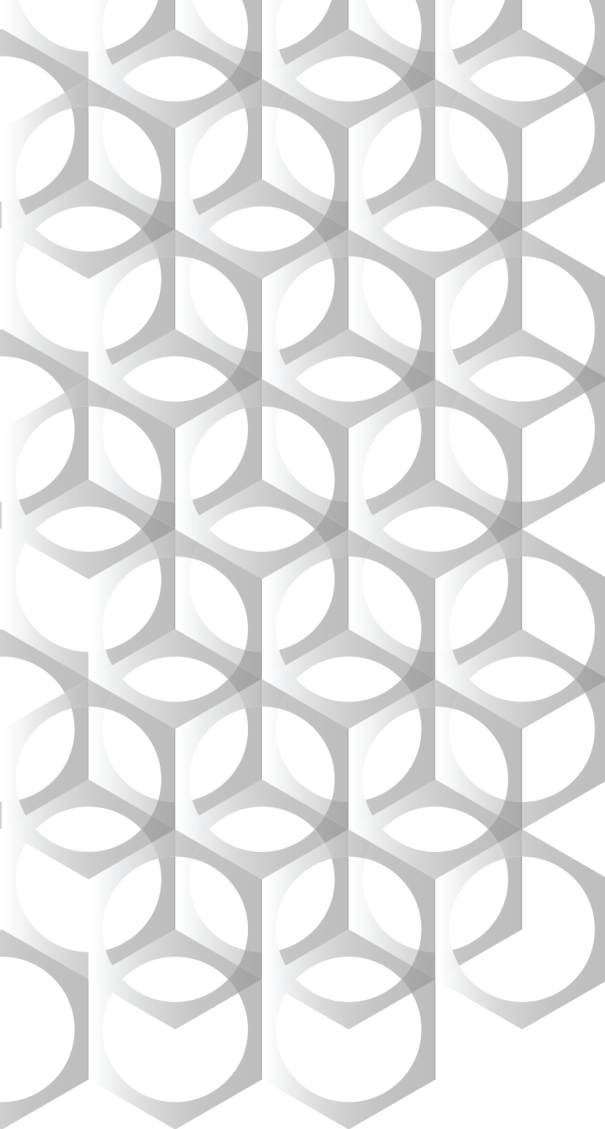


|  |
| --- |
|  |
| **Réalisation d’un audit portant sur l’évaluation de la conformité de la sécurité du système d’information de {CLIENT} à la {NORME}**  Rapport d’audit |
|  |
| **DOCUMENT STRICTEMENT CONFIDENTIEL** |



|  |  |  |  |
| --- | --- | --- | --- |
| **REDACTION DU DOCUMENT** | | | |
|  | **Nom** | **Fonction** | **Contact** |
| **Ecrit par :** | {auditeur} | Consultante en Sécurité SI | {auditeurEmail} |
| **Relu par :** |  | Consultant Expert en Sécurité SI |  |
| **Relu par** | {manager} | Chef de projet | {managerEmail} |

|  |  |
| --- | --- |
| **DIFFUSION DU DOCUMENT** | |
| **Nom** | **Entité / Fonction** |
| M. {clientChef} | Responsable de la Sécurité SI - {CLIENT} |
|  |  |

**Sommaire**

[1. Introduction 4](#_Toc179454844)

[2. Objectif et démarche 5](#_Toc179454845)

[2.1 Objectifs 5](#_Toc179454846)

[2.2 Démarche méthodologique 5](#_Toc179454847)

[2.3 Définition du référentiel 6](#_Toc179454848)

[3. Préambule 7](#_Toc179454849)

[3.1 Engagement 7](#_Toc179454850)

[3.2 Confidentialité 7](#_Toc179454851)

[4. Synthèse 8](#_Toc179454852)

[4.1 synthèse des conformités 9](#_Toc179454853)

[4.2 Synthèse des actions d’amélioration 10](#_Toc179454854)

[5. Audit organisationnel selon la {NORME} 11](#_Toc179454855)

[5.1 Politique de sécurité 12](#_Toc179454856)

[5.2 Organisation de la sécurité des systèmes d’information 12](#_Toc179454857)

[5.3 Sécurité des ressources humaines 13](#_Toc179454858)

[5.4 Gestion des actifs informationnels 15](#_Toc179454859)

[5.5 Contrôle d’accès 17](#_Toc179454860)

[5.6 Cryptographie 19](#_Toc179454861)

[5.7 Sécurité physique et environnementale 20](#_Toc179454862)

[5.8 Sécurité liée à l’exploitation 22](#_Toc179454863)

[5.9 Sécurité des communications 25](#_Toc179454864)

[5.10 Acquisition, développement et maintenance des systèmes d’information 27](#_Toc179454865)

[5.11 Relations avec les fournisseurs 28](#_Toc179454866)

[5.12 Gestion des incidents de cybersécurité 29](#_Toc179454867)

[5.13 Gestion de la continuité de l’activité 31](#_Toc179454868)

[5.14 Conformité 32](#_Toc179454869)

[6. Annexes 34](#_Toc179454870)

[6.1 Notation 34](#_Toc179454871)

# Introduction

{CLIENT}, conscient des enjeux liés à la sécurité de l’information, procède à un audit de sécurité qualifié par un prestataire PASSI dans le but d’évaluer l’efficacité des mesures de sécurité organisationnelles/physiques déployées et ce, afin de proposer des actions correctives et de pallier les dysfonctionnements et carences identifiées.

En se référant à la nouvelle version de la norme ({NORME}) et aux bonnes pratiques nationales et internationales, cet audit vise la détection des éventuels écarts et non-conformités liés aux différents processus de gestion et d’organisation de la sécurité au sein {CLIENT}.

Le présent rapport présente le niveau de maturité du Système d’Information {CLIENT}. Il décrit les résultats de l’analyse de conformité par rapport aux différentes règles et mesures édictées par la nouvelle version de la {NORME}. Le rapport présente également des recommandations et des projets à mettre en œuvre afin de lever les différentes anomalies détectées.

# Objectif et démarche

## Objectifs

Le présent document constitue le rapport de l’audit organisationnel et physique. Il répond aux objectifs ci-après :

* Disposer d’une vue globale du niveau de maturité de la sécurité du système d’information adopté par {CLIENT} relativement à la {NORME} v2 ;
* Faire ressortir les différentes insuffisances et dysfonctionnements liés à la sécurité de l’information ;
* Vérifier la conformité, la pertinence et l’application des mesures déployées par rapport aux politiques de sécurité {CLIENT} à la {NORME} v2 et aux procédures en vigueur.

Ce document présente ainsi :

* Une synthèse des points marquants ressortant de cet audit ;
* Un bilan détaillé de l’état des lieux réalisé et des recommandations.

## Démarche méthodologique

L’audit organisationnel et physique {CLIENT} est réalisé en se référant à la {NORME} v2.

La démarche adoptée par Near Secure dans le cadre de cette mission suivra les bonnes pratiques de l’audit édictées par les standards nationaux et internationaux. Elle est basée en premier lieu sur une analyse documentaire de différents éléments de référence mis à la disposition des auditeurs de Near Secure par {CLIENT} et sur une série d’entretiens planifiés et réalisés avec les parties prenantes.

L’audit physique et environnemental a été réalisé en effectuant des visites aux sites et aux locaux {CLIENT} ainsi qu’une revue de la documentation fournie relative à ce volet.

Les résultats détaillés dans ce document présentent :

* L’évaluation du niveau de sécurité de l’organisation de la sécurité de l’information ;
* L'identification des écarts et conformités recensés par rapport à la {NORME}.

## Définition du référentiel

Le référentiel choisi pour l’audit organisationnel est la Directive Nationale de Sécurité des Systèmes d’Information V2 ({NORME} v2). Cet audit s’est articulé autour des chapitres suivants :

|  |  |
| --- | --- |
| **Chapitre {NORME}** | **Description** |
| **{#chapitres}{number}** | {title}**{/chapitres}** |

# Préambule

## Engagement

NearSecure s’est engagée à exécuter cette mission en respectant l’ensemble des dispositions légales et réglementaires en vigueur.

En tout état de cause, Nearsecure ne sera pas autorisée à diffuser, reproduire ou transférer les données auxquelles elle aurait pu avoir accès.

## Confidentialité

Nos auditeurs s’engagent à respecter la confidentialité des informations et documents auxquels ils ont eu accès dans le cadre de leur mission.

# Synthèse

Le présent rapport a pour objectif d’évaluer la conformité {CLIENT} aux exigences de la {NORME} V2.

Les entretiens menés ainsi que la revue et l’analyse documentaire réalisée ont permis de situer le **niveau de maturité global** **{CLIENT} par rapport à la {NORME} v2 à un niveau de Moyen Perfectible.**

Maturité globale selon la {NORME}

{%chartImage}

|  |  |  |  |
| --- | --- | --- | --- |
| **Conformité par rapport à la {NORME}** | **Nbre de questions** | **Niveau de maturité 2023** | **Niveau de maturité cible** |
| **{#conformite}{title}** | **{nbreQuestions}** | {maturiteNiveau  } | {maturiteCible}{/conformite} |
| **Total des questions** | **{TotalPc**  **}** | **{avConformite}** | **80%** |

## synthèse des conformités

{CLIENT} a déployé de grands efforts dans l’instauration et l’amélioration de la sécurisation de son système d’information. En effet, l’audit a recensé plusieurs points forts détaillés ci-après :

* L’engagement de la Direction Générale et des parties prenantes par rapport à l’amélioration du niveau de sécurité de l’information

## Synthèse des actions d’amélioration

Malgré les différentes actions menées pour assurer une maturité de la Sécurité de l’Information {CLIENT}, la mission a constaté l’existence de plusieurs écarts notamment :

# Audit organisationnel selon la {NORME}

Ce chapitre présente les éléments de revue organisationnelle {CLIENT}. Ces éléments sont présentés selon les chapitres de la nouvelle version de la Directive Nationale de la Sécurité des Systèmes d’Information :

{#chapitres}

* {title}

{/chapitres}

Pour chaque thématique, un bilan des non-conformités constatées est présenté, ainsi que la cotation globale pour cette thématique de l’écart constaté avec les exigences du référentiel d’audit et les recommandations associées.

{#CONTROLPOINTTABLES}

## {CHAPTERTITLE}

|  |  |  |  |
| --- | --- | --- | --- |
|  | | | |
| **Constats** | | **Niveau de maturité** | **{#showConformite}Conformité {NORME}{/showConformite}** |
| **Détail** | **{#controlPoints} {detail}:**  {constats} | **{maturite}** | **{#showConformite} {conformite}{/showConformite}** |
| **Recommandations** | | **Niveau d’urgence** | |
| **Il convient de : {#recommandations}**  {courtTerme} | | C.T | |
| **{**moyenTerme} | | M.T | |
| {longTerme} | | L.T**{/recommandations}{/controlPoints}** | |

{/CONTROLPOINTTABLES}

# Annexes

## Notation

|  |  |
| --- | --- |
| **Niveau de maturité** | **Description** |
| **N/A** | La règle est non applicable. |
| **Aucun** | Aucun processus/documentation en place. |
| **Initial** | Le processus est caractérisé par la prédominance d'interventions ponctuelles, voir chaotiques. Il est très peu défini et la réussite dépend de l'effort individuel. |
| **Reproductible** | Une gestion élémentaire de la sécurité est définie pour assurer le suivi des couts, des délais et de la fonctionnalité. L'expertise nécessaire au processus est en place pour reproduire la même action. |
| **Défini** | Le processus de sécurité est documenté, normalisé et intégré dans les processus standards de l'entité ou de l'IIV. |
| **Maitrisé** | Des mesures détaillées sont prises en ce qui concerne le déroulement du processus et la qualité générée. Le processus et le niveau de qualité sont connus et contrôlés quantitativement. |
| **Optimisé** | Une amélioration continue du processus est mise en œuvre par une rétroaction quantitative émanant du processus lui-même et par l'application d'idées et de technologies innovatrices. |

|  |  |
| --- | --- |
| **Niveau de conformité** | **Niveau de maturité** |
| **Non\_conforme** | **Aucun** |
| **Initial** |
| **Partielle** | **Reproductible** |
| **Défini** |
| **Totale** | **Maitrisé** |
| **Optimisé** |
| N/A | La règle est non applicable. |

|  |  |
| --- | --- |
| **Niveau** | **Priorité des recommandations** |
| **Court terme**  **(C.T)** | Ce sont les actions à lancer au cours des 6 premiers mois  [0- 6 mois] |
| **Moyen terme**  **(M.T)** | Ce sont les actions à lancer sous 18 mois  [6 - 18 mois] |
| **Long terme**  **(L.T)** | Ce sont les actions à lancer sous 21 mois  [18mois – 36 mois] |