l



**Rapport d’Audit de la Sécurité du Système d’Information**

**///Cusotmer + Projet**

**de ${LN}**

**pour l’année ${Y}**

${icon:200:200}

**Expert Auditeur Chargé de la Mission :**

**Signature :**

<Insérer le cachet>

|  |  |  |
| --- | --- | --- |
| **Version du document** | **Date** | **Diffusion** |
| 0.1 | ${today} | Version de diffusion |

**SOMMAIRE**

[1. Avant-propos 3](#_Toc106872382)

[1.1. Confidentialité du document 3](#_Toc106872383)

[1.2. Historique des modifications 3](#_Toc106872384)

[1.3. Diffusion du document 3](#_Toc106872385)

[2. Cadre de la mission 4](#_Toc106872386)

[3. Termes et définitions 4](#_Toc106872387)

[4. Références 5](#_Toc106872388)

[5. Présentation de Client X 5](#_Toc106872389)

[6. Champ d’audit 6](#_Toc106872390)

[6.1. Périmètre géographique 6](#_Toc106872391)

[6.2. Description des systèmes d’information 6](#_Toc106872392)

[6.3. Schéma synoptique de l’architecture du réseau 9](#_Toc106872393)

[7. Méthodologie d’audit 9](#_Toc106872394)

[8. Synthèse des résultats de l’audit 12](#_Toc106872395)

[9. Présentation détaillée des résultats de l’audit 14](#_Toc106872396)

[9.1. Résultat par domaine de sécurité 14](#_Toc106872397)

[9.2. Vulnérabilités non acceptable enregistrées 40](#_Toc106872398)

[9.3. Les critères d’audit 41](#_Toc106872399)

[9.4. Détails audit technique 41](#_Toc106872400)

[10. Appréciation des risques 41](#_Toc106872401)

[10.1. La démarche d’appréciation des risques adoptée 41](#_Toc106872402)

[10.2. Présentation du processus d’appréciation du risque en sécurité de l’information 41](#_Toc106872403)

[10.3. Evaluation des Risques 42](#_Toc106872404)

[10.4. Identification des menaces, des vulnérabilités et des impacts des processus traités 51](#_Toc106872405)

[11. Plan d’action 52](#_Toc106872406)

[11.1. Le plan d’action 52](#_Toc106872407)

1. Avant-propos
   1. Confidentialité du document

Le présent document est confidentiel et sa confidentialité consiste à :

* Ne pas divulguer des dites informations confidentielles auprès de la tierce partie,
* Ne pas reproduire des informations dites confidentielles, sauf accord de ${SN},
* Ne pas profiter ou faire profiter tierce partie du contenu de ces informations en matière de savoir-faire,
* Considérer toutes les informations relatives à la production et au système d’information de ${SN} déclarées Confidentielles.
  1. Historique des modifications

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Auteur** | **Modifications** |
| 1.0 | {today} | Equipe Smart SKILLS | Version initiale |

* 1. Diffusion du document

**///GLB\_PIP**

|  |  |  |  |
| --- | --- | --- | --- |
| **Diffusion (coté *Smart SKILLS*)** | | | |
| Nom  Prénom | Titre | Tél | Mail |
| Ayed AKROUT | Chef de projet | 29961666 | Ayed.akrout@smartskills.tn |
| **Diffusion (coté ${SN})** | | | |
| Nom  Prénom | Titre | Tél | Mail |
| ${SPOC\_Tech\_Name} | ${SPOC\_Tech\_Title} | ${SPOC\_Tech\_Tel} | ${SPOC\_Tech\_email} |

1. Cadre de la mission

Dans le cadre de la loi N°17-2023, ${SN} a confié au bureau d’études SMART SKILLS la réalisation d’une mission d’audit réglementaire de la sécurité de son système d’information pour l’année ${Y}. Le référentiel utilisé lors de cette mission est celui de la norme internationale ISO 27002 en sa version 2022, qui décrit les bonnes pratiques pour la gestion de la sécurité de l’information. Cette norme présente 93 mesures pouvant être mises en place pour gérer la sécurité d’un système d’information, et nous sommes attachés à vérifier l’existence et l’efficacité de chacune de ces mesures au niveau du système d’information de ${SN}.

1. Termes et définitions

* **Preuves d'audit**

Durant notre mission d’audit, nous avons exploité les différentes preuves d’audit qualitatives et quantitatives :

* La liste des enregistrements
* Les informations qui se rapportent aux critères d'audit et qui sont vérifiables.

Notre audit se base sur les différentes preuves :

* La preuve physique : c'est ce que l'on voit, constate = observation,
* La preuve testimoniale : témoignages. C'est une preuve très fragile qui doit toujours être recoupée et validée par d'autres preuves,
* La preuve documentaire : procédures écrites, comptes rendus, notes,
* La preuve analytique : résulte de calculs, rapprochements, déductions et comparaisons diverses.
* **Critères d’audit**

Ensemble de politiques, procédures ou exigences déterminées par rapport auxquelles la conformité du système est évaluée (contrôles au niveau de la norme ISO/IEC 27002 :2012).

* **Plan d'audit**

Description des activités et des dispositions nécessaires pour réaliser un audit, préparé par le responsable de l'audit en commun accord entre SMART SKILLS et ${SN} pour faciliter la programmation dans le temps et la coordination des activités d'audit.

* **Champs d'audit**

Étendu et limité d'un audit, le champ décrit généralement les lieux, les unités organisationnelles, les activités et les processus ainsi que la période de temps couverte.

* **Constats d'audit**

Résultats de l'évaluation des preuves d'audit recueillies par rapport aux critères d'audit.

1. Références

Les documents de référence utilisés pour la réalisation de la présente mission d'audit sont :

* Le référentiel d'audit de l'ANSI v1.4
* La norme ISO 27002 :2012

1. Présentation de ${SN} //Cusotmer

|  |  |
| --- | --- |
| **Nom de l’organisme** | ${LN} |
| **Acronyme** | ${SN} |
| **Statut** | ${typeCompany} |
| **Secteur d’activité** | $SecteurActivite} |
| **Catégorie** | ${Categorie} |
| **Site web** | ${siteweb} |
| **Adresse Email** | ${mailadress} |

//[Select](https://md-39.webhostbox.net:2083/cpsess6431293367/3rdparty/phpMyAdmin/url.php?url=https://dev.mysql.com/doc/refman/5.7/en/select.html) Processus\_domaine, [Max](https://md-39.webhostbox.net:2083/cpsess6431293367/3rdparty/phpMyAdmin/url.php?url=https://dev.mysql.com/doc/refman/5.7/en/aggregate-functions.html%23function_max)(D), [Max](https://md-39.webhostbox.net:2083/cpsess6431293367/3rdparty/phpMyAdmin/url.php?url=https://dev.mysql.com/doc/refman/5.7/en/aggregate-functions.html%23function_max)(I), [Max](https://md-39.webhostbox.net:2083/cpsess6431293367/3rdparty/phpMyAdmin/url.php?url=https://dev.mysql.com/doc/refman/5.7/en/aggregate-functions.html%23function_max)(C) from RM\_Processus\_Actifs\_Valeurs [Left](https://md-39.webhostbox.net:2083/cpsess6431293367/3rdparty/phpMyAdmin/url.php?url=https://dev.mysql.com/doc/refman/5.7/en/string-functions.html%23function_left) join RM\_Processus\_domains on RM\_Processus\_Actifs\_Valeurs.ID\_Processus=RM\_Processus\_domains.ID where RM\_Processus\_domains.ID\_ITERATION=1 group by Processus\_domaine;

|  |  |  |  |
| --- | --- | --- | --- |
| **Désignation du processus** | **Exigences des données traitées en (1)** | | |
| **Confidentialité** | **Intégrité** | **Disponibilité** |
| ${process} | ${Process\_C} | ${Process\_I} | ${Process\_D} |

//Projet

**Les principales missions de ${SN} :**

${DescriptionCompany}

//Customer

**Ci-dessous l’organigramme de ${SN}**

|  |
| --- |
| ${organigrame:800:800} |

1. Champ d’audit
   1. Périmètre géographique

La liste des structures à auditer

[SELECT](https://md-39.webhostbox.net:2083/cpsess6431293367/3rdparty/phpMyAdmin/url.php?url=https://dev.mysql.com/doc/refman/5.7/en/select.html) \* FROM `Customer\_sites` WHERE Customer\_ID=1

|  |  |  |
| --- | --- | --- |
|  | **Structure** | **Lieu d’implantation** |
| **{N\_Site}** | {Structure\_Site} | {Lieu\_Site} |

Le choix du périmètre géographique est selon la demande de ${SN} (Le respect du périmètre de la mission d’audit selon le cahier de charge).

* 1. Description des systèmes d’information
* Les composants du système d'information avec justification des exclusions le cas échéant selon le modèle « Description du SI de ${SN} »

**Description du SI Siège de ${SN}**

**// SELECT `Nom`,`field3`,`field4`,`field5`,`dev by`,`URL`,`Number of users` FROM `Audit\_sow` WHERE Type='Application' and `Customer`=1;**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Applications** | | | | | | | |
| Nom (1) | Modules | Description | Environnement de développement | Développée par /Année | Noms ou @IP des  serveurs d’hébergement | Nombre d’utilisateurs | **Incluse au périmètre d’audit (6)** |
| ${App\_Name} | ${App\_Module} | ${App\_Descr} | ${App\_EnvDev} | ${App\_DevPar} | ${App\_IPs} | ${App\_NumberUsers} | Oui |

**SELECT `Nom`,IP\_Host,`field3`,`field4`,`field5` FROM `Audit\_sow` WHERE Type='Serveur' and `Customer`=1;**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Serveurs (par plateforme)** | | | | | |
| Nom (1) | @IP | Type (2) | Système d’exploitation | Rôle/métier (3) | **Inclus au périmètre d’audit (6)** |
| ${Srv\_Name} | ${Srv\_IP} | ${Srv\_Type} | ${Srv\_SE} | ${Srv\_Role} | Oui |

// [SELECT](https://md-39.webhostbox.net:2083/cpsess6431293367/3rdparty/phpMyAdmin/url.php?url=https://dev.mysql.com/doc/refman/5.7/en/select.html) `Nom`,IP\_Host,`field3`,`field4`,`field5` FROM `Audit\_sow` WHERE Type='Infra' [and](https://md-39.webhostbox.net:2083/cpsess6431293367/3rdparty/phpMyAdmin/url.php?url=https://dev.mysql.com/doc/refman/5.7/en/logical-operators.html%23operator_and) `Customer`=1;

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Infrastructure Réseau et sécurité** | | | | | |
| Nature (4) | Marque | Nombre | Administré par : | Observations (5) | **Inclus au périmètre d’audit (6)** |
| ${Infra\_Nature} | ${Infra\_Marque} | ${Infra\_Number} | ${Infra\_ManagedBy} | ${Infra\_Obs} | Oui |

//[SELECT](https://md-39.webhostbox.net:2083/cpsess6431293367/3rdparty/phpMyAdmin/url.php?url=https://dev.mysql.com/doc/refman/5.7/en/select.html) ` field4`,[count](https://md-39.webhostbox.net:2083/cpsess6431293367/3rdparty/phpMyAdmin/url.php?url=https://dev.mysql.com/doc/refman/5.7/en/aggregate-functions.html%23function_count)(field4) FROM `Audit\_sow` WHERE Type='PC' [and](https://md-39.webhostbox.net:2083/cpsess6431293367/3rdparty/phpMyAdmin/url.php?url=https://dev.mysql.com/doc/refman/5.7/en/logical-operators.html%23operator_and) `Customer`=1 group by field4;

|  |  |  |
| --- | --- | --- |
| **Postes de travail** | | |
| Système d’exploitation | Nombre | **Inclus au périmètre d’audit (6)** |
| ${PC\_SE} | {$PC\_Number} | Oui |

(1) : **Nomenclature**

(2) : Type du serveur : MV (Machine Virtuelle) ou MP (Machine Physique).

(3) : Rôle/métier : Base de données (MS SQL Server, Oracle, …), messagerie, application métier, Contrôleur de domaine, Proxy, Antivirus, etc.

(4): Nature: Switch, Routeur, Firewall, IDS/IPS, etc.

(5) Observations : des informations complémentaires sur l’équipement par exemple niveau du switch

(6) : Oui/Non. **Si non, présenter les raisons de l’exclusion. En cas où l’élément n’est pas audité pour des raisons d’échantillonnage, indiquer l’élément échantillonné avec, tout en précisant les critères d’échantillonnage adoptés.**

* 1. Schéma synoptique de l’architecture du réseau

Le schéma de réseau de ${SN}

//Customer table

|  |
| --- |
| ${NetworkDesign:800:800} |

1. Méthodologie d’audit

* La méthodologie d’audit adoptée, comporte 4 étapes principales :
* Audit organisationnel et physique
* Audit technique
* Analyse de risque
* Synthèse de l’audit
* Les domaines de la sécurité des systèmes d’information couverts par la méthodologie d’audit sont détaillés dans la partie ci-dessous :
* La maturité des mesures et contrôles de sécurité mise en place est conforme avec les quatorze (04) domaines dudit référentiel :

**A.5 Mesures organisationnelles**

**A.6 Mesures liées aux personnes**

**A.7 Mesures physiques**

**A.8 Mesures technologiques**

**- Les outils d’audit utilisés**

**//SELECT \* FROM `Audit\_Tools` order by Composante\_SI**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Outils | Version utilisée | License | Fonctionnalités | Composantes du SI objet de l’audit |
| ${tool} | ${tool\_version} | ${tool\_license} | $tool\_features} | ${tool\_sow} |

**- Les check-lists utilisées**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Check List** | **Créer par** | **Equipe** | **Détails** | **Audit** |
| Check List Poste de travail | CIS Benchmark | Equipe SMART SKILLS | https://www.cisecurity.org/benchmark | Audit Poste de travail |
| Check List serveur | CIS Benchmark | Equipe SMART SKILLS | https://www.cisecurity.org/benchmark | Audit des serveurs |
| Check List applicatif | Créer par SMART SKILLS | Equipe SMART SKILLS | Détails des parties audités | Audit des applications |
| Check List firewall | CIS Benchmark | Equipe SMART SKILLS | https://www.cisecurity.org/benchmark | Audit firewall |
| Check List Switch | CIS Benchmark | Equipe SMART SKILLS | https://www.cisecurity.org/benchmark | Audit équipements réseau |
| Check List Router | CIS Benchmark | Equipe SMART SKILLS | https://www.cisecurity.org/benchmark | Audit équipements réseau |

**- L’équipe du projet côté SMART SKILLS**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Nom et Prénom** | **Qualité** | **Qualification** | **Certifié**  **Par l’ANSI** | **Champs d’intervention** |
| AKROUT Ayed | Chef de projet | ISO 27001, 27005, 22301, OSCP, CEH, CISA, CISM, CISSP, 27032 | Oui | AOP, Appréciation des risques |
|  |  |  |  |  |

**- L’équipe du projet côté ${SN}**

**//** [SELECT](http://webapp.smartskills.local/phpmyadmin/url.php?url=https://dev.mysql.com/doc/refman/8.0/en/select.html) \* FROM `glb\_pip` where Customer\_ID=1

|  |  |  |
| --- | --- | --- |
| **Nom Prénom** | **Qualité** | **Fonction** |
| ${SPOC\_Tech\_Name} | ${SPOC\_Tech\_Title} | ${SPOC\_Tech\_Title} |

Le planning réel d’exécution de la mission d’audit de la sécurité du SI de ${SN}

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Composant** | | **Équipe intervenante** | **Date(s) de réalisation** | **Durée en Hommes/jours pour chaque intervenant** | |
| **Phase** | **Objet de la sous phase** | **Sur Site** | **Totale** |
| **Réunion d’ouverture et sensibilisation** | Réunion d’ouverture et sensibilisation |  |  |  |  |
| **AOP** | Audit Org. et Physique |  |  |  |  |
| Audit Org. et Physique |  |  |  |  |
| Audit Org. et Physique |  |  |  |  |
| Audit Org. et Physique |  |  |  |  |
| **AT** | Audit Technique |  |  |  |  |
| Audit Technique (Poste de travail) |  |  |  |  |
| Audit serveurs |  |  |
| Audit applicatif |  |  |  |  |
| Audit réseaux |  |  |  |  |
| **Appréciation des risques** | Appréciation des risques |  |  |  |  |
| **Synthèse et recommandations** | Synthèse et recommandations |  |  |  |  |
| **Réunion de clôture et sensibilisation post audit** | Réunion de clôture et sensibilisation |  |  |  |  |
| **Durée totale de la mission (en Homme/jour)** | | | | |  |

1. Synthèse des résultats de l’audit

* **Les critères et les standards/référentiels par rapport auxquels l’audit a été réalisé,**

D’une façon globale, le niveau de maturité de la sécurité du système d’information de ${SN} est ${acceptablility} ${raison\_decision}.

Un constat important est que d’après l’appréciation de risque, il y a ${nbr\_risk\_critique} scénarios de risque jugés vitale au niveau de ${SN}, il y a ${nbr\_risk\_critique} scénarios de risque jugés majeurs.

* **Les critères et les standards/référentiels par rapport auxquels l’audit a été réalisé,**

ISO 27002 / ISO 27005

* **Les types et nature de test réalisés pour établir ces résultats,**

      Scans de vulnérabilités et de configuration, Observations, réunions de travail, interviews, revue    documentaire, workshops.

* **Evaluation du dernier plan d’action**

**//** SELECT \* FROM `audit\_previousaudits\_ap` WHERE `ID\_Projet`=3 Order by `ProjetNumero`,`ActionNumero`

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Projet** | **Action** | **Criticité** | **Chargé de**  **l’action** | **Charge**  **(H/J)** | **Taux de**  **réalisation** | **Evaluation** (**1)** |
| **Projet 1 :** | **Action 1.1 :** |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
| **Projet 2 :** | **Action 2.1 :** |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |  |

(1) Evaluation des mesures qui ont été adoptées depuis le dernier audit réalisé et aux insuffisances enregistrées dans l’application de ses recommandations, avec un report des raisons invoquées par les responsables du système d’information et celles constatées, expliquant ces insuffisances.

* **Etat de maturité de la sécurité du système d’information de ${SN}**
* **par rapport à la norme ISO 27002 (les détails sont dans la section 9 du présent rapport)**

SELECT `Clause\_name`, `controle\_name`, round(sum( 5\*`rm\_questions`.`P`\* rm\_answers.Answer)/sum( `rm\_questions`.`P`),1) FROM `standards\_controls`

LEFT JOIN rm\_questions on standards\_controls.ID=`rm\_questions`.`Standard\_Control\_id`

LEFT Join rm\_answers on rm\_answers.ID\_Question=rm\_questions.ID

group by `Clause`, `controle` order by `Clause`, `controle` ASC

|  |  |  |  |
| --- | --- | --- | --- |
| **Domaine** | **Critère d’évaluation** | **Valeur attribuée** | **Commentaires** |
| ${Domain} | ${Mesures} | {Value} |  |

Les valeurs à attribuer pour chaque règle de sécurité invoquée seront entre 0 et 5 :

N/A - Non applicable

0 - Pratique inexistante

1 - Pratique informelle : Actions isolées

2 - Pratique répétable et suivie : Actions reproductible

3 - Processus définis : Standardisation des pratiques

4 - Processus contrôlés : des mesures quantitatives

5 - Processus continuellement optimisés

* **Les indicateurs de sécurité selon le modèle « Indicateurs de sécurité :**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Classe/Indicateur** | | **Exp de valeur** | **Valeur** | **Commentaires** |
| **Organisation** | **Nomination officielle RSSI** | 0/1 |  |  |
| **Fiche de poste RSSI** | 0/1 |  |  |
| **Rattachement RSSI** | DG/DSI/Direction Administrative/Direction Audit Interne/Direction Risques |  |  |
| **Existence officielle Cellule Sécurité** | 0/1 |  |  |
| **Existence officielle Comité Sécurité** | 0/1 |  |  |
| **PSSI** | **Existence formelle PSSI** | 0/1 |  |  |
| **Portée** | Partielle/Totale |  |  |
| **Communication** | 0/1 |  |  |
| **Maintien de la PSSI** | 0/1 |  |  |
| **Gestion de la continuité d'activité** | **Existence formelle PCA** | 0/1 |  |  |
| **Existence formelle PRA** | 0/1 |  |  |
| **Maintien du PCA** | 0/1 |  |  |
| **Maintien du PRA** | 0/1 |  |  |
| **Organisation de crise en cas de sinistre** | 0/1 |  |  |
| **Site Secours** | 0/1 |  |  |
| **Gestion des actifs** | **Inventaire complet** | 0/1 |  |  |
| **Procédure formelle de classification** | 0/1 |  |  |
| **Mise en place de la classification** | 0/1 |  |  |
| **Gestion des risques SI Métier** | **Existence formelle de la gestion des risques** | 0/1 |  |  |
| **Couverture totale du Métier** | 0/1 |  |  |
| **Réalisée une seule fois** | 0/1 |  |  |
| **Fréquence Réalisation Périodique** | 0/1 |  |  |
| **En cas de changement majeur** | 0/1 |  |  |
| **Gestion des incidents** | **Procédure formelle de gestion des incidents** | 0/1 |  |  |
| **Existence d'une cellule de gestion des incidents** | 0/1 |  |  |
| **Gestion des sauvegardes** | **Politique formelle de sauvegarde** | 0/1 |  |  |
| **Couverture des données métier** | Absence/Totale/ Partielle |  |  |
| **Couverture des données de serveurs de support** | Absence/Totale/ Partielle |  |  |
| **Couverture des données des PCs utilisateurs sensibles** | Absence/Totale/Partielle |  |  |
| **Couverture des running-config des équipements de sécurité &réseau** | Absence/Totale/Partielle |  |  |
| **Couverture Clonage OS des serveurs** | Absence/Totale/Partielle |  |  |
| **Couverture des codes sources et des paramètres de configuration des applications et des logiciels de base** | Absence/Totale/Partielle |  |  |
| **Maintien de la solution de sauvegarde** | 0/1 |  |  |
| **Tests de restauration périodiques** | 0/1 |  |  |
| **Sécurité physique des copies de sauvegarde** | 0/1 |  |  |
| **Existence des copies à un site distant** | 0/1 |  |  |
| **Contrôle d’accès** | **Politique formelle de contrôle d’accès** | 0/1 |  |  |
| **TdB SSI** | **Existence d'un Tableau de bord SSI** | 0/1 |  |  |
| **Portée : indicateurs opérationnels** | 0/1 |  |  |
| **Portée : indicateurs stratégiques** | 0/1 |  |  |
| **Audit interne de la sécurité** | **Existence de l'Audit interne de la sécurité** | 0/1 |  |  |
| **Réalisation périodique de l'Audit interne** | 0/1 |  |  |
| **Réalisation suite à un incident** | 0/1 |  |  |
| **Réalisation suite à la mise en place d’un nouveau système** | 0/1 |  |  |
| **Portée: uniquement aspects techniques** | 0/1 |  |  |
| **Portée: aspects tech, org et phys** | 0/1 |  |  |
| **Démarche de conformité** | **Existence d'une démarche de conf** | 0/1 |  |  |
| **Nature** | exemples: ISO 27001/ PCI/DSS |  |  |
| **Etape** | certifié/projet en cours/planifié |  |  |
| **Protection antivirale** | **Existence d'une solution antivirale** | 0/1 |  |  |
| **MAJ périodique de la Sol Antivirale** | 0/1 |  |  |
| **Couverture des serveurs** | Absence/Partielle/Totale |  |  |
| **Couverture des PCs** | Absence/Partielle/Totale |  |  |
| **Dépl auto des patchs et correctifs Séc OS** | **Existence Dép auto patchs&cor Séc OS** | 0/1 |  |  |
| **MAJ périodique de la Sol Antivirale** | Absence/Partielle/Totale |  |  |
| **Couverture des serveurs** | Absence/Partielle/Totale |  |  |
| **Couverture des PCs** | 0/1 |  |  |
| **Processus MAJ des firmwares Equips Sécurité** | **Existence** | Absence/Partielle/Totale |  |  |
| **Couverture** | 0/1 |  |  |
| **Processus MAJ des firmwares Equips Réseau** | **Existence** | 0/1 |  |  |
| **Couverture** | Absence/Partielle/Totale |  |  |
| **Remplacement des produits dont la date EoL ou EoS expiré** | **Remp OS Serveurs EoL EoS** | Total/Partiel/Planifié/Absence |  |  |
| **Remp OS PCs EoL EoS** | Total/Partiel/Planifié/Absence |  |  |
| **Remp Produits Sécurité EoL EoS** | Total/Partiel/Planifié/Absence |  |  |
| **Remp Produits Réseau EoL EoS** | Total/Partiel/Planifié/Absence |  |  |
| **Contrôle d'accès logique** | **Utilisation Contrôleur de domaines** | 0/1 |  |  |
| **Utilisation d'une Solution IAM** | 0/1 |  |  |
| **Utilisation Proxy Accès Internet** | 0/1 |  |  |
| **Matrice de Flux Réseau MFR formelle** | 0/1 |  |  |
| **Implémentation règles de filtr -Equips frontaux- cf MFR** | 0/1 |  |  |
| **Implémentation Filtrage inter-VLAN cf MFR** | 0/1 |  |  |
| **Réseau d’administration** | **Existence d'un réseau d'admin** | 0/1 |  |  |
| **Isolé du réseau production et Internet** | 0/1 |  |  |
| **Admin qu’à partir des machines de ce réseau** | 0/1 |  |  |
| **Utilisation protocoles admin chiffrés** | Absence/Partielle/Totale |  |  |
| **Séparation des environnements** | **Sép infras dév, test et exploitation** | 0/1 |  |  |
| **Sécurité des partages** | **Désactiv des partages rés sur les serveurs** | 0/1 |  |  |
| **Désactiv des partages rés sur les PCs** | 0/1 |  |  |
| **Utilisation des serveurs de fichier** | 0/1 |  |  |
| **Système de détection/Prévention d’intrusion** | **Existence** | 0/1 |  |  |
| **Déf politique de détection et de prévention d’intrusion** | 0/1 |  |  |
| **Configuration par défaut des alertes** | 0/1 |  |  |
| **Configuration cf à la politique des IDS/IPS** | 0/1 |  |  |
| **Processus de suivi des alertes générées** | 0/1 |  |  |
| **Solution SIEM** | **Existence** | 0/1 |  |  |
| **Portée: Serveurs** | 0/1 |  |  |
| **Portée: Equips Séc** | 0/1 |  |  |
| **Portée: Equips Rés** | 0/1 |  |  |
| **Synchronisation des horloges** | 0/1 |  |  |
| **Contrats de maintenance** | **Couverture des Serveurs** | Absence/Partielle/Totale |  |  |
| **Couverture des applications métier** | Absence/Partielle/Totale |  |  |
| **Couverture des SGBDs** | Absence/Partielle/Totale |  |  |
| **Couverture des équips sécurité** | Absence/Partielle/Totale |  |  |
| **Couverture des équips réseau** | Absence/Partielle/Totale |  |  |
| **Local Data-center** | **Existence** | 0/1/2/3+ |  |  |
| **Classification** | Non-classé/Tier1/Tier2/Tier3/Tier4 |  |  |
| **Zones d'emplacement** | Forts Risques/Faibles Risques |  |  |
| **Contrôle d’accès au Data-Center** | Exemples: Clé/Carte magnétique/Biométrie |  |  |
| **Secours électrique** | **Couverture onduleurs Serveurs** | Absence/Partielle/Totale |  |  |
| **Couverture onduleurs Equips rés & séc** | Absence/Partielle/Totale |  |  |
| **Couverture onduleurs PCs** | Absence/Partielle/Totale |  |  |
| **Existence Groupe électrogène** | 0/1 |  |  |
| **Test régulier du groupe électrogène** | 0/1 |  |  |
| **Sécurité de la climatisation DC** | **Système de climatisation adéquate** | 0/1 |  |  |
| **Redondance** | 0/1 |  |  |
| **Contrat de maintenance** | 0/1 |  |  |
| **Sécurité Câblage** | **Chemins de câbles dédiés et séparés** | 0/1 |  |  |
| **Etiquetage** | 0/1 |  |  |
| **Plans de chemins de câblage** | 0/1 |  |  |
| **Sécurité périmétrique DC** | **Solution de détection d’intrusion** | 0/1 |  |  |
| **Système de vidéo-surveillance** | 0/1 |  |  |
| **Murs résistants aux intrusions physiques et aux incendies et dépourvus de fenêtres** | 0/1 |  |  |
| **Sécurité Incendie DC** | **Détecteurs de fumée** | 0/1 |  |  |
| **Extincteurs automatiques** | 0/1 |  |  |
| **Porte Data Center Coupe-feu** | 0/1 |  |  |
| **Sécurité contre les dégâts des eaux** | **Détecteurs d’humidité** | 0/1 |  |  |
| **Système d’alerte** | 0/1 |  |  |
| **Dispositif Anti-foudre** | **Dispositif Anti-foudre** | 0/1 |  |  |

* **Les vulnérabilités très critiques détectées et jugées être d’un intérêt particulier pouvant affecter la sécurité du cyber espace national :**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Vulnérabilité** | **Référence de la vulnérabilité** | **Actifs impactés** | **Impact d’exploitation réussie de la vulnérabilité** | **Probabilité d’exploitation réussie de la vulnérabilité** | **Recommandation / Mesure de traitement** |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

1. Présentation détaillée des résultats de l’audit
   1. Résultat par domaine de sécurité

// [SELECT](http://webapp.smartskills.local/phpmyadmin/url.php?url=https://dev.mysql.com/doc/refman/8.0/en/select.html) `standards\_controls`.`Clause`, `standards\_controls`.`controle`, rm\_answers.Answer, `rm\_questions`.`Bonne pratique`, `rm\_questions`.`Vulnérabilité` FROM `standards\_controls` [LEFT](http://webapp.smartskills.local/phpmyadmin/url.php?url=https://dev.mysql.com/doc/refman/8.0/en/string-functions.html" \l "function_left) JOIN rm\_questions on standards\_controls.ID=`rm\_questions`.`Standard\_Control\_id` [LEFT](http://webapp.smartskills.local/phpmyadmin/url.php?url=https://dev.mysql.com/doc/refman/8.0/en/string-functions.html" \l "function_left) Join rm\_answers on rm\_answers.ID\_Question=rm\_questions.ID WHERE LENGTH(`rm\_questions`.`Vulnérabilité`) > 5 order by `Clause`, `controle`,`rm\_questions`.`Question\_numero` ASC;

|  |  |  |  |
| --- | --- | --- | --- |
| **Domaine** | **Critères d’audit** | **Résultats de l’audit (constats)** | **Description des vérifications effectuées (tests, conditions de test, etc)** |
| **5 Mesures de sécurité organisationnelles** | **5.${Controle} ${controle\_name}** | **Bonnes pratiques identifiées** |  |
| ${5\_BestPractice} |
| **Vulnérabilités enregistrées** |
| ${5\_Vuln} |
| **6 Mesures de sécurité applicables aux personnes** | **6.${6\_Mesures\_id} ${6\_Mesures}** | **Bonnes pratiques identifiées** |  |
| ${6\_BestPractice} |
| **Vulnérabilités enregistrées** |
| ${6\_Vuln} |
| **7 Mesures de sécurité physique** |  | $BestPractice |  |
| **8 Mesures de sécurité technologiques** |  | **Vulnérabilités enregistrées** |  |
|  |  |  |  |
|  |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **Domaine** | **Critères d’audit** | **Résultats de l’audit (constats)** | **Description des vérifications effectuées (tests, conditions de test, etc)** |
| **5.** Principes pour les mesures organisationnelles | **5. 1** Appr?ciation des ?v?nements li?s ? la s?curit? | **Bonnes pratiques identifiées** |  |
| Présence d'une politique de sécurité de l'inform |
| **Vulnérabilités enregistrées** |
| $Vuln |
| **5. 2** Fonctions et responsabilit?s li?es ? la s?curit? d... | **Bonnes pratiques identifiées** |  |
| Présence d'une structure opérationnelle d |
| **Vulnérabilités enregistrées** |
| $Vuln |
| **Other Domains are here** | **Same as previous one** | | |

* 1. Vulnérabilités non acceptable enregistrées

|  |
| --- |
| **Référence de la vulnérabilité:**  ${Vuln\_ref} |
| **Description :**  ${Vuln\_desc} |
| **Preuve(s) d’audit :**  ${Vuln\_proof} |
| **Composante(s) du SI impactée(s) :**  ${Vuln\_si} |
| **Recommandation :**  ${Vuln\_recom} |

* 1. **Détails audit technique**

Description dans les Rapports d’audit Technique.

1. Appréciation des risques
   1. La démarche d’appréciation des risques adoptée

Nous nous proposons d’effectuer une analyse des risques menaçant la sécurité du système d’information du **${SN}** Méhari.

Méhari est une méthode harmonisée d’analyse de risques, développée par le CLUSIF (Club de la Sécurité de l'Information Français) depuis 1995 et elle est dérivée des méthodes Melissa et Marion. Elle a été initialement conçue pour aider les DSI dans leur tâche de management de la sécurité de l’information. Cette présentation générale leur est ainsi principalement destinée, mais elle s’adresse également aux auditeurs ou aux gestionnaires de risques qui partagent, dans une large mesure, les mêmes préoccupations. L’objectif de Méhari est donc de fournir une gamme d’outils adaptés au management de la sécurité. Or, ceux-ci se concrétisent par un ensemble d’actions qui ont chacune des objectifs particuliers. Parmi les actes de management, nous citons :

* L’élaboration de plans de sécurité, ou de schémas directeurs
* La mise en place de règle ou politiques de sécurité ;
* La conduite de diagnostics, rapides ou approfondis sur l’état de la sécurité ;
* L’évaluation et le management des risques ;
* La gestion de la sécurité dans la conduite de projets de développement ;
* La sensibilisation ((La bonne utilisation des mots des passes, la défense contre l’attaque de phishing, les Ransomwares, le bureau propre et l’écran verrouillé, etc…) et la formation à la sécurité ;
* Le pilotage de la sécurité et le contrôle des actions décidées.

Ces différents actes de management et leurs variantes ne sont pas exclusifs mais au contraire des actions pouvant être menées simultanément ou successivement, par des entités distinctes ou par la même entité, en fonction des besoins ponctuels ou permanents, indépendamment ou faisant partie d’un programme d’ensemble.

En outre, les mêmes actes de management peuvent être conduits différemment selon

* La maturité de l’entreprise de son personnel en termes de sécurité,
* La volonté d’impliquer plus ou moins fortement les managers opérationnels dans les prises de décision concernant la sécurité de l’information
* La culture de l’entreprise : hiérarchique ou, au contraire, décentralisée et responsabilisant.
  1. Présentation du processus d’appréciation du risque en sécurité de l’information

L’appréciation du risque se découpe en deux activités :

L’analyse de risque, elle-même segmentée en deux sous-activités (l’identification et l’estimation des risques) et l’évaluation du risque.

* En premier lieu, l’identification des risques définit les actifs : ceux primaires, c’est-à-dire les activités métier et l’information, et ceux secondaires, comme un serveur, avec pour chacun son propriétaire et sa valeur selon une échelle commune.
* Ensuite, on recherche les menaces, les vulnérabilités et les conséquences, c’est-à-dire les dommages possibles quand une menace exploite une vulnérabilité sur les actifs.
* Enfin, on liste les mesures de sécurité existantes.
* L’estimation des risques consiste à évaluer les conséquences et les probabilités d’occurrence des menaces, analyse - de risques.

L’évaluation du risque correspond à la prise de décision par comparaison des niveaux de risque.



**Processus d’Appréciation du Risque en Sécurité de l’Information**

* 1. Evaluation des Risques

En partant de la méthodologie Méhari stipulant que la sécurité est mise en œuvre à travers de Services de sécurité (Contrôle d’accès par exemple), l’analyse des vulnérabilités consiste alors à faire un diagnostic de la qualité des services de sécurité.

L’analyse que nous nous proposons d’effectuer est orientée scénarios. Un scénario de risque est la description d’un dysfonctionnement et de la manière dont ce dysfonctionnement peut survenir. Le dysfonctionnement comprend lui-même un sinistre, c'est-à-dire des détériorations directes et des conséquences indirectes de ce sinistre. Dans notre démarche, nous utilisons la base de connaissance de scénarios de risque proposée par la méthodologie Méhari.

L'objectif de l’analyse d’un scénario de risque est d’évaluer deux paramètres caractéristiques du risque encouru par l’organisme dans l'hypothèse d'occurrence d'un tel scénario. Ces paramètres sont:

* **La potentialité du risque** qui représente, en quelque sorte, sa probabilité d'occurrence, bien que cette occurrence ne soit pas modélisable en termes de probabilité. Cette potentialité est en fonction du contexte et des mesures de sécurité mises en place.
* **L'impact du risque** sur l'organisme, qui représente la gravité des conséquences directes et indirectes qui découlent de l'occurrence du risque. Cet impact est fonction de l'impact maximum ou intrinsèque, défini lors de la classification en termes d'enjeux ou de niveau dans l'échelle de valeurs, éventuellement réduit par la mise en œuvre de mesures de sécurité adaptées.

Afin de quantifier le risque correspondant au scénario analysé, les évaluations de la potentialité et de l’impact seront faites sur une échelle ayant 4 niveaux :

* **Identification des menaces**

Il est important d’identifier les potentielles faiblesses associées à chacun des processus supportant l’information critique de l’organisation. Ces faiblesses peuvent être exploitées par des menaces et avoir un impact négatif sur l’information (divulgation, destruction, etc.).

* **Identification des Impacts**

Le niveau d’impact est défini selon les exigences internes, externes, réglementaires et légales du cadre dans lequel évolue l’organisation. Dans la partie qui suit, nous décrivons ces niveaux d’impacts:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Impact** | 1 | 2 | 3 | 4 |
| **Gravité** | **Non significatif** | **Important** | **Très grave** | **Vitale** |
| **Description** | A ce niveau les dommages encourus n'ont pratiquement pas d'impact sur les résultats de l'entité ni sur son image, même si certaines personnes sont fortement impliquées dans le rétablissement de la situation d'origine. | Important Il s'agit là de sinistres ayant un impact notable au niveau des opérations de l'entité, de ses résultats ou de son image, mais restant globalement supportables | Il s'agit là d'impact très grave au niveau de l'entité, sans que son avenir soit compromis. En termes financiers, cela peut amputer sérieusement le résultat de l'exercice, sans que les actionnaires se dégagent massivement. En termes d'image, on considérera souvent à ce niveau une perte d'image dommageable qu'il faudra plusieurs mois à remonter, même si l'impact financier ne peut être évalué avec précision. Des sinistres conduisant à une désorganisation notable de l'entreprise pendant une durée de plusieurs mois seront aussi souvent évalués à ce niveau. | A ce niveau l'impact est extrêmement grave et met en danger l'existence même ou la survie de l'entité ou de l'une de ses activités majeures. En cas de survie de l'entreprise ou de l'organisme, les séquelles sont importantes et durables. |
| **Financier** | Perte négligeable | Perte importante | Perte majeure | Perte vitale |
| **Engagement vis à vis parties intéressées** | Faible nuisance | Dégradation du service vis-à-vis parties intéressées | Blocage d’un système ou Perte d’une donnée des parties intéressées | Blocage des systèmes ou Perte de la totalité des données des parties intéressées. |
| **Juridique** | Faible impact | Non-respect de la réglementation nationale | Infraction majeure à la législation | Sanction judiciaire |
| **Sécurité des personnes** | Impact marginal | Inconfort pour un individu | Risque pour la sécurité d’un individu | Risque pour la sécurité d'un groupe de personnes |

* **Identification de la Potentialité**

La gravité du risque ne dépend pas seulement du niveau de son impact sur la Confidentialité, l’Intégrité et la Disponibilité des actifs, mais aussi de sa Potentialité.

**La Potentialité (P):** C’est la probabilité qu'un événement se produise avec un impact indésirable. Si l’événement est très probable, alors le niveau du risque va être plus élevé. Le niveau de potentialité devrait se baser sur l’historique de l'occurrence de l'événement indésirable ou à partir de statistiques disponibles. Ce facteur est essentiel pour la poursuite de l’analyse du risque car il permet de déterminer la gravité du risque.

|  |  |  |
| --- | --- | --- |
| **Description** | **Durée** | **Valeur** |
| **Très peu probable** | 1 fois tous les 5 ans et plus | **1** |
| **Peu probable** | 1 à 2 fois tous les 2 ans | **2** |
| **Probable** | 2 mois < 1 fois < 6 mois | **3** |
| **Très probable** | > 1 fois tous les deux mois | **4** |

* **Maturité des contrôles existants**

Le but de cette phase est d’analyser la maturité des contrôles déjà existants, afin de minimiser la probabilité de l’exploit d’une vulnérabilité ou réduire son impact. Les contrôles existants à analyser doivent couvrir :

Les méthodes organisationnelles et opérationnelles, attestées par un plan d’exploitation, des manuels de procédures, des documents ou des directives de politiques de sécurité.

Les méthodes techniques tels que la segmentation des réseaux par les VLANs, les ACLs sur les routeurs, les Firewalls périmétriques ou de zones, les Systèmes de Détection d’Intrusion (IDS), les techniques cryptographiques et les VPNs, la vidéosurveillance, le contrôle d’accès etc.

Il y a 8 domaines utilisés au niveau de Mehari Standard 2.1 du 10 Aout 2022 à savoir:

1. Organisation de la sécurité
2. Sécurité des Sites
3. Sécurité des systèmes et de leur architecture
4. Exploitation et administration des systèmes
5. Sécurité applicative et continuité de l'activité
6. Protection des postes de travail utilisateurs
7. Sécurité des projets et développements applicatifs
8. Conformité aux exigences légales et contractuelles

* **Calcul de risque**

Avec la méthode Méhari, après avoir calculé l’impact et la potentialité intrinsèques ainsi que la maturité des contrôles existants (pas de formule générale mais pour chaque risque il y aura une formule dédiée suivant le nombre des mesures de réduction de risque possible et leurs type (Dissuasive, Préventive, Confinement, Palliative). Une fois l’impact et la potentialité calculés, le risque sera comme suit :

Risque calculé sera en fonction de deux facteurs I et P calculé suivant la grille suivante :

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Impact** | | |  | |
|  |  | |  | |
| **4** | **2** | **3** | **4** | **4** |
| **3** | **2** | **3** | **3** | **4** |
| **2** | **1** | **2** | **2** | **3** |
| **1** | **1** | **1** | **1** | **2** |
|  | **1** | **2** | **3** | **4** |
|  | **Potentialité** | | | |

* **Résultats globaux de l’appréciation des risques :**

Sur 212 scénarios de risque, on constate :

* ${risk\_4\_nbr} scénarios de gravité 4
* ${risk\_3\_nbr} scénarios de gravité 3
* ${risk\_2\_nbr} scénarios de gravité 2
* ${risk\_1\_nbr} scénarios de gravité 1

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Panorama des risques** | | | | | |
|  | **Impact** | | |  | |
|  | 4 | ${R41} | ${R42} | ${R43} | ${R44} |
|  | 3 | ${R31} | ${R32} | ${R33} | ${R34} |
|  | 2 | ${R21} | ${R22} | ${R23} | ${R24} |
|  | 1 | ${R11} | ${R12} | ${R13} | ${R14} |
|  | | 1 | 2 | 3 | 4 |
|  | |  | | **Potentialité** | |

* **Panorama des gravités de scénarios par rapport à DIC**

MET ICI screenshot de **Panorama des gravités de scénarios par rapport à DIC**

* **Evaluation des impacts intrinsèques et choix des processus :**

Nous avons sélectionné pour cette appréciation les processus mentionnés dans les tableaux T1 et T2.

Pour chaque processus, on définit l’impact intrinsèque sur les actifs de type données (Tableau T1) utilisées par ce processus puis sur les services (Tableau T2)

MET ICI screenshot de **T1**

Tableau 1: Classifications des données

MET ICI screenshot de **T2**

Tableau 2: Classifications des Services

Ce qui donne le tableau récapitulatif d’impact intrinsèque suivant

MET ICI screenshot de tableau de classification

Tableau 3: tableau récapitulatif des impacts intrinsèques

**Qualité de service de réduction des risques (Vue d’ensemble)**

|  |  |  |
| --- | --- | --- |
| **N°** | **Domaine** | **Note** |
| 1 | Organisation de la sécurité (1 Org) |  |
| 2 | Sécurité physique (2 Phy) |  |
| 3 | Sécurité des systèmes et de leur architecture (3 Sys) |  |
| 4 | Exploitation des systèmes d'information et de communication (4 Ope) |  |
| 5 | Sécurité applicative et continuité de l'activité (5 App) |  |
| 6 | Protection des postes de travail utilisateurs (6 Mic) |  |
| 7 | Sécurité des projets et développements applicatifs (7 Dev) |  |
| 8 | Conformité aux exigences légales et contractuelles (8 CEX) |  |

* **Exposition naturelle aux différents types des événements :**

On adoptera les valeurs de l’exposition naturelle standard de CLUSIQ:

|  |  |  |  |
| --- | --- | --- | --- |
| **Tableau des événements : types et exposition naturelle** | | |  |
| ***Type*** | ***Code type*** | ***Événement*** | ***Exposition naturelle standard CLUSIQ*** |
| Absence de personnel | AB.P | Absence accidentelle de personnel interne ou de partenaire |  |
| Absence ou indisponibilité accidentelle de service | AB.S | Absence de service : Énergie |  |
| Absence de service : défaillance ou indisponibilité du fournisseur d'accès à Internet |  |
| Absence de service : Impossibilité d'accès aux locaux |  |
| Absence de maintenance ou maintenance impossible |  |
| Accident grave d'environnement | AC.E | Incendie, Inondation, foudroiement, … |  |
| Accident matériel | AC.M | Panne d'équipement |  |
| Panne d'équipement de servitude |  |
| Erreur matérielle ou de comportement du personnel | ER.P | Perte ou oubli de document ou de media |  |
| Erreur de manipulation ou dans le suivi d'une procédure |  |
| Erreur de saisie ou de frappe |  |
| Incident dû à l'environnement | IC.E | Dégât dû au vieillissement ou à la pollution |  |
| Dégât externes divers : dégâts des eaux, surcharge électrique, etc. |  |
| Incident logique ou fonctionnel | IF.L | Incident d'exploitation |  |
| Bug bloquant dans un logiciel système, middleware, applicatif ou un progiciel |  |
| Logiciel malveillant ou virus |  |
| Malveillance menée par voie logique ou fonctionnelle | MA.L | Attaque en blocage de comptes |  |
| Effacement volontaire ou pollution massive de configurations systèmes |  |
| Effacement volontaire direct de supports logiques ou physiques |  |
| Falsification logique (données ou fonctions) |  |
| Création de faux (messages ou données) |  |
| Rejeu de transaction |  |
| Saturation malveillante d'équipements informatiques ou réseaux |  |
| Destruction logique totale (fichiers et leurs sauvegardes) |  |
| Détournement logique de fichiers ou données (téléchargement ou copie) |  |
| Malveillance menée par voie physique | MA.P | Manipulation ou falsification matérielle d'équipement |  |
| Terrorisme |  |
| Vandalisme |  |
| Vol physique |  |
| Procédures non conformes | PR.N | Procédures inadéquates |  |
| Procédures inappliquées par manque de moyens |  |
| Procédures inappliquées par méconnaissance |  |
| Procédures inappliquées volontairement |  |

* **Vue détaillée de risques les plus critiques**

MET ICI liste de tableau des scéanrios de risque(max Top 20)

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ID risque | ***LIBELLÉ*** | **Sélection** | **Type AEM** | **Type DICE** | **Impact Intrins.** | **Exposition** | **Grav. Intrins.** | **Dissuasion** | **Prévention** | **Confinement** | **Palliation** | **I calculé** | **P calculée** | **Gravité calculée** |
|  |  | | | | | | | | | | | | | |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  | | | | | | | | | | | | | |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  | | | | | | | | | | | | | |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

* 1. Identification des menaces, des vulnérabilités et des impacts des processus traités

Le tableau suivant fournit :

* L’impact/conséquences d’exploitation des vulnérabilités associées
* La complexité d’exploitation des vulnérabilités associées
* La probabilité d’occurrence des menaces associées
* Une estimation de la gravité du risque (la gravité du risque étant une résultante des facteurs suscités)

|  |
| --- |
| **Scénario du risque :** |
| **Description :** |
| **Référence(s) de(s) la vulnérabilité(s) :** |
| **Composante(s) du SI impactée(s) :** |
| **Impact(s)/Conséquence(s) d’exploitation des vulnérabilités associées :** |
| **Complexité d’exploitation de(s)s vulnérabilité(s) :** |
| **Gravité du risque :** |
| **Recommandation :** |
| **Complexité de mise en œuvre de la recommandation :** |

1. Plan d’action

Durant le reste de ce rapport, nous allons préparer et de mettre en œuvre une stratégie de sécurité cohérente et ciblée. Ce rapport sera mis à jour lors des audits de la seconde et de la troisième année tenant compte du taux de réalisation des mesures qui ont été adoptées depuis le dernier audit réalisé et des insuffisances enregistrées dans l’application de ses recommandations, ainsi que des résultats de l’audit de l’année en cours,

**Plan d’action cadre s’étalant sur trois (03) années**

Nous allons présenter dans cette partie les actions à mener en urgence pour la sécurisation du SI de l’ XXXXX

|  |  |
| --- | --- |
| Très urgente | A réaliser dans la 1ère année |
| Urgente | A réaliser dans la 2ème année |
| Normale | A réaliser dans la 3ème année |

* 1. Le plan d’action

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Projet** | **Action** | **Priorité** | **Responsable de l’action** | **Charge (H/J)** | **Planification** |
| **Projet 1 : Organisation de la sécurité** | **Action 1.1 :** Faire des formations poussées pour le RSSI et l’équipe IT dans le domaine de la sécurité des systèmes d'information et la continuité d’activité, sur le plan organisationnel et technique. | **Urgente** | **Interne** | **5** |  |
| **Action 1.2 :** Planifier des sessions de sensibilisation consacrées à la sécurité informatique pour tous le personnel. | **Urgente** | **Interne** | **5** |  |
| **Action 1.3 :** Elaborer une politique de sécurité de l’information (PSI). | **Urgente** | **Interne** | **2** |  |
| **Action 1.4 :** Mettre en place un plan de continuité d’activité (PCA) | **Urgente** | **Interne** | **2** |  |
| **Action 1.5 :** Réaliser le test régulier du PCA (test backup, site de secours). | **Très Urgent** | **Interne** | **10** |  |
| **Action 1.8 :** Forcer les sessions de communication pour les textes et veille réglementaire. | **Urgente** | **Interne** | **5** |  |
| **Action 1.9 :** Etablir la cartographie des risques et registre des DCP. | **Urgente** | **Interne** | **5** |  |
| **Action 1.11 :** Mettre en place un schéma directeur de SI. | **Très Urgent** | **Interne** | **10** |  |
| **Projet 2 : Améliorer la Sécurité opérationnelle** | **Action 2.1 :** Réaliser des scans de vulnérabilité régulière (chaque 3 mois) | **Très Urgent** | **Interne** | **10** |  |
| **Action 2.2 :**  Réaliser des tests de d’intrusion. | **Très Urgent** | **Interne** | **10** |  |
| **Action 2.3 :**  Mettre en place une solution de patch management. | **Très Urgent** | **Interne** | **10** |  |
| **Action 2.4 :** Mettre en place un SIEM. | **Très Urgent** | **Interne** | **5** |  |
| **Action 2.5 :** Assurer la revue régulier des accès direct réseaux, systèmes et aux Bases de données. | **Très Urgent** | **Interne** | **5** |  |
| **Action 2.6 :** Mise en place d’un système permettant de détecter toute modification ou suppression d'un enregistrement qui permet de déclencher une alerte immédiate auprès d'un responsable. (DLP) | **Très Urgente** | **Interne plus un consultant externe** | **15** |  |
| **Action 2.7 :** Il est recommandé de suivre la bonne pratique de CIS Benchmark pour la Configuration des (PCs, serveurs, réseaux). | **Très Urgent** | **Interne** | **5** |  |
| **Action 2.8 :** Migrer vers un Système d’Exploitation supporté par l’éditeur | **Très Urgent** | **Interne** | **5** |  |