l

Rapport d’Audit de la Sécurité du Système d’Information ///Cusotmer + Projet

de SOMEF
pour l’année 2023

${icon:200:200}

Expert Auditeur Chargé de la Mission :
Signature :

<Insérer le cachet>

Version du document	Date	Diffusion
0.1	2023-11-09	Version de diffusion

SOMMAIRE

Version	Date	Auteur	Modifications
1.0	2023-11-09	Equipe Smart SKILLS	Version initiale

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 SOMEF)			
Nom Prénom	Titre	Tél	Mail
Nizar KRIAA	DSI	28827103	nizar.kriaa@somef.tn
Jane Smith	Manager	1234567890	jane.smith@example.com
Ahmed ben Bettaieb	React Developper	52212679	benbettaieb@smartskills.tn

Cadre de la mission

Dans le cadre de la loi N°17-2023, SOMEF 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 2023. 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 SOMEF.

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 SOMEF 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.

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

Présentation de SOMEF

//Cusotmer

Nom de l'organisme	SOMEF
Acronyme	SOMEF
Statut	Privé
Secteur d'activité	Industrie
Catégorie	Entreprise
Site web	www.somef.tn
Adresse Email	contact@somef.tn

//Select Processus_domaine, Max(D), Max(I), Max(C) from RM_Processus_Actifs_Valeurs 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**
Fabrication	3	3	4
R&D	3	3	3

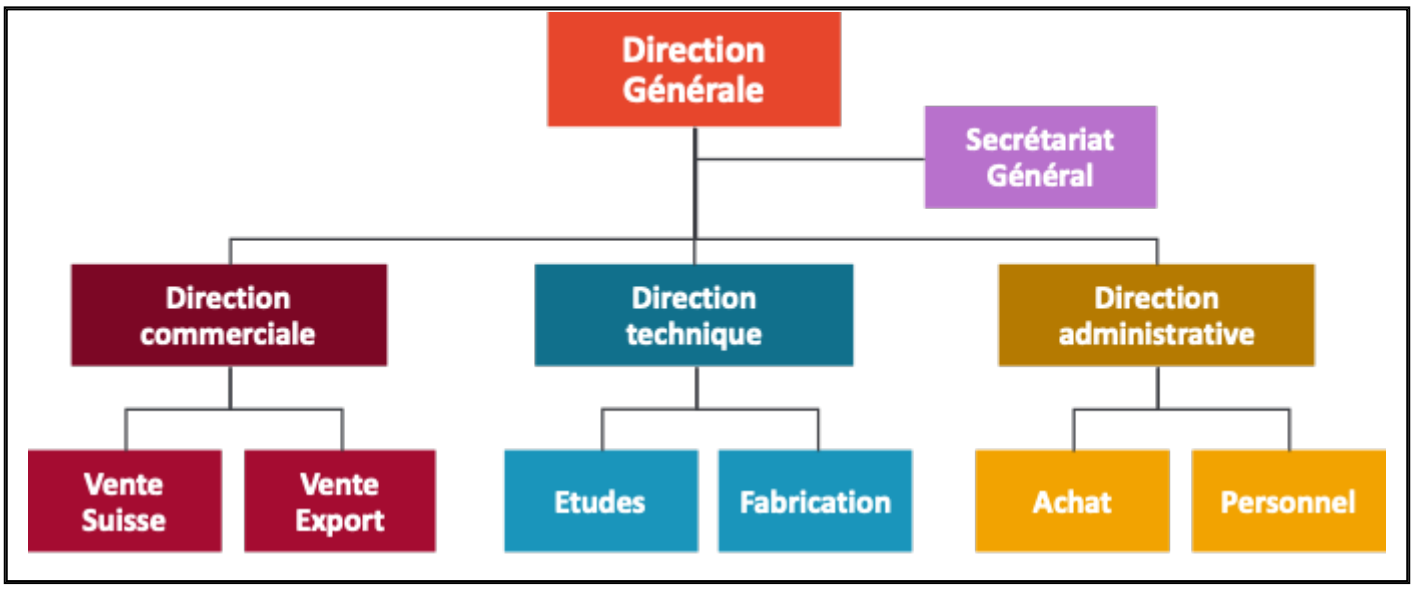
//Projet

Les principales missions de SOMEF :

SOMEF est leader sur le marché tunisien des appareillages électriques, reconnue pour son expertise, la qualité de ses produits et son excellente image de marque. Depuis sa création en 1988, SOMEF a toujours relevé de nouveaux défis, en développant une offre complète de produits et solutions la plus innovante sur le marché. Son expertise, son savoir-faire et l'intégration de nouvelles technologies dans son offre, aussi bien pour le secteur résidentiel que pour le secteur tertiaire, ont rendu son positionnement fort et attractif pour tous ses clients et professionnels. SOMEF a initié depuis des années une stratégie de veille afin d'offrir à ses derniers les solutions les plus adaptées à leurs besoins, et aujourd'hui, ses avantages concurrentiels de leader permettent une expansion aussi bien sur le marché local que celui international

//Customer

Ci-dessous l'organigramme de SOMEF



Champ d'audit
Périmètre géographique

La liste des structures à auditer

SELECT * FROM `Customer_sites` WHERE Customer_ID=1

	Structure	Lieu d'implantation
1	Siège Social	ZI Megrine

Le choix du périmètre géographique est selon la demande de SOMEF (Le respect du périmètre de la mission d'audit selon le cahier de charge).
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 SOMEF »

Description du SI Siège de SOMEF

// 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)**

Microsft Ax 2012 R3	• Gestion financière • Gestion de la chaîne logistique • Gestion de la fabrication • Gestion des services • Les ventes et le marketing	il s'agit du progiciel de gestion intégré (PGI/ERP), cœur de notre métier,	Dynamics AX utilise un environnement de développement intégré nommé MorphX (X++), qui permet de pers	Microsoft/ Version 2012	Client serveur : SRVMASTER port d'écoute 2712. Serveur en répartion de charge sur trois serveur SRVA	Plus que 6	Oui
Maximaint	Gestion de la maintenance	Logiciels de gestion de la maintenance GMAO Industrie - DIMO Maint		DimoMaint	Client serveur vers SRVGMAO	5	Oui
JIRA atlassian	Gestion des projets	Une solution pour la gestion des projets et du clollaboratif		ATLASSIAN			Oui
QualiPro	Gestion de la qualité	Qualipro logiciel qualité SMQ (Système Management Qualité)		SAPHIR CONSULT France	http://192.168.0.23/qualipro/		Oui
Glpi	Gestion du parc informatique		PHP	Teclib' & contributeurs	http://192.168.0.93/glpi/		Oui
Portail RH	Intranet RH		JS et PHP	Interne	http://srvqpro:88/APPMAM/admin/		Oui
AX Somef / PRODPRO	Solution métier suivi de la production et Contrôle de gestion		WINDEV	Interne	Installtion sur les postes clients et pointe vers le serveur SRV-BARCODE		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)**
SRVDB	192.168.0.201	MV	Windows Server 2012 Standard	Serveur BD / Sql Server 2012	Oui
SRV-BARCODE	192.168.0.94	MV	Windows Server 2012 Standard	Application métier	Oui
SRV-RH	192.168.0.20	MV	Windows Server 2012 Standard	Application métier/ Sql server 2014	Oui
SRVGLPI	192.168.0.2	MV	Windows Server 2012 Standard	Application métier	Oui

SRVQPRO	192.168.0.23	MV	Windows Server 2012 Standard	Application métier	Oui
testback	192.168.0.17	MV	Windows Server 2012 Standard	Serveur test/ Sql server 2014	Oui
SRVMASTER	192.168.0.196	MV	Windows Server 2012 Standard	Application métier AX	Oui
SRVAOS1	192.169.0.199	MV	Windows Server 2012 Standard	Application métier AX	Oui
SRVAOS2	192.169.0.193	MV	Windows Server 2012 Standard	Application métier AX	Oui
SRVAOS3	192.169.0.194	MV	Windows Server 2012 Standard	Application métier AX	Oui
SRVAXR3PRE	192.168.0.15	MV	Windows Server 2012 Standard	Serveur test AX/ Sql server 2014	Oui
SRVDEV	192.168.0.2	MV	Windows Server 2012 Standard	Serveur test AX/ Sql server 2015	Oui
SRVREPORT	192.168.0.191	MV	Windows Server 2012 Standard	Reporting Services 2012	Oui
SRV-AD	10.10.0.13	MP	Windows Server 2012 R2 Standard	Contrôleur de domaine	Oui
SRVGMAO	192.168.0.223	MP	Windows Server 2012 R2 Standard	Application métier GMAO	Oui

// SELECT `Nom`,IP_Host,`field3`,`field4`,`field5` FROM `Audit_sow` WHERE Type='Infra' and `Customer`=1;

Infrastructure Réseau et sécurité					
Nature (4)	Marque	Nombre	Administré par :	Observations (5)	**Inclus au périmètre d'audit (6)**
Firewall	192.168.99.2	1	service informatique		Oui
switch niveau 3	192.168.99.254	1	service informatique		Oui

//SELECT ` field4`,count(field4) FROM `Audit_sow` WHERE Type='PC' and `Customer`=1 group by field4;

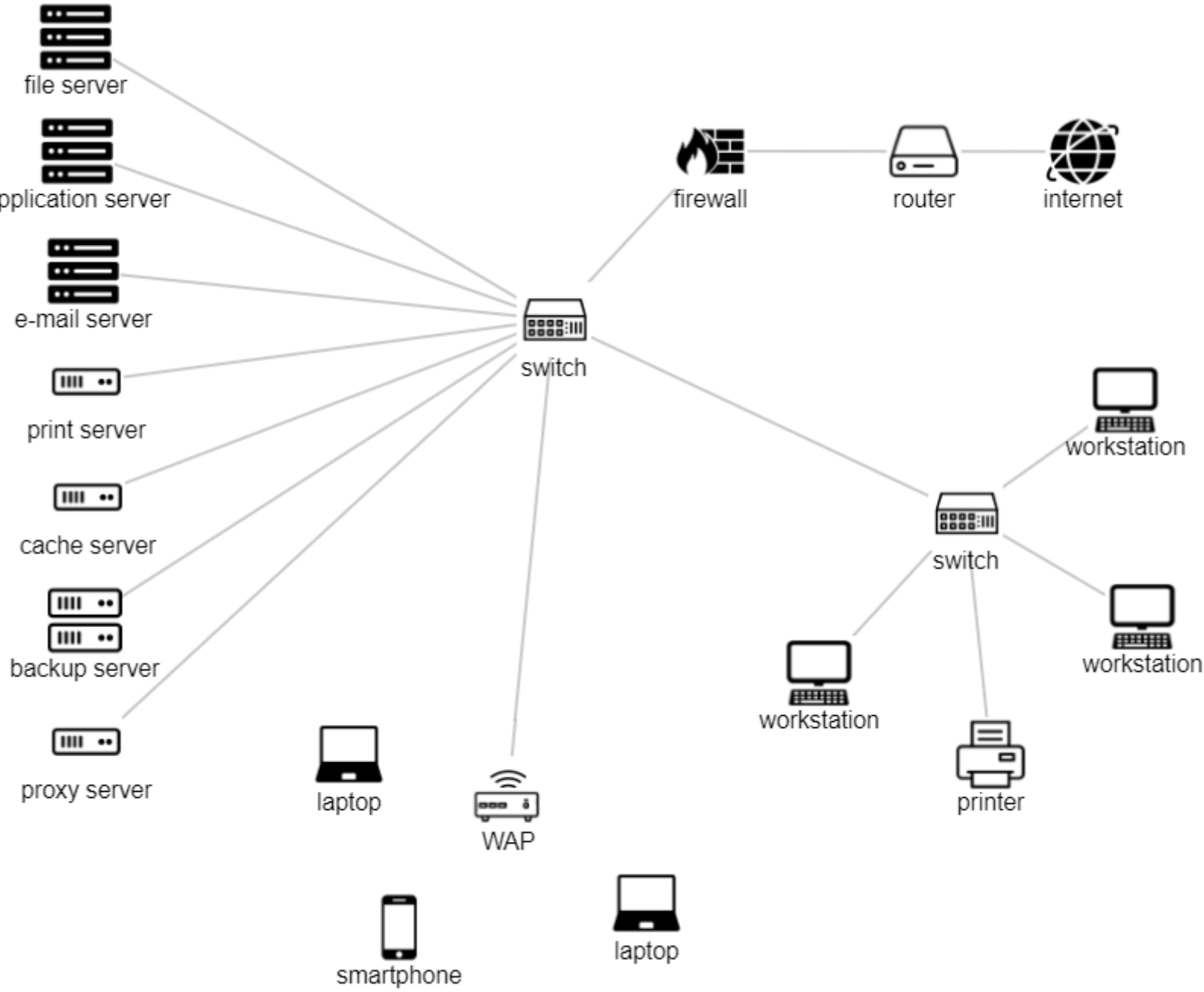
Postes de travail		
Système d'exploitation	Nombre	**Inclus au périmètre d'audit (6)**
192.168.0.0/24	1	Oui
192.168.1.0/24	1	Oui
192.168.2.0/24	1	Oui
192.168.3.0/24	1	Oui
192.168.4.0/24	1	Oui
192.168.5.0/24	1	Oui
192.168.6.0/24	1	Oui
192.168.7.0/24	1	Oui
192.168.8.0/24	1	Oui

(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.**

Schéma synoptique de l'architecture du réseau

Le schéma de réseau de SOMEF

//Customer table



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
OWASP ZAP?	02/11/01	Open source?	OWASP ZAP est un outil pour tester le niveau de s?curit? des applications Web?	Application Web?
Subgraph Vega?	1.0?	Open source?	Vega est un scanner et une plate-forme pour tester le Niveau de s?curit? des applications Web?	Application Web?
Nipper?	02/09/01	Version de test?	Un scanner des configurations r?seau?	Scan ?quipements R?seau?
Nmap?	7.60?	Open source?	Un scanner des ports?	Scan des Ports?
Nessus PRO?	10.0.2?	Version Pro?	Nessus est un outil de scan des vuln?rabilit?s?	Serveur, PC, Application et R?seau?

- 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 SOMEF

// SELECT * FROM `glb_pip` where Customer_ID=1

Nom Prénom	Qualité	Fonction
Nizar KRIAA	DSI	DSI
Jane Smith	Manager	Manager
Ahmed ben Bettaieb	React Developper	React Developper

Le planning réel d'exécution de la mission d'audit de la sécurité du SI de SOMEF

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)					

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 SOMEF 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 SOMEF, 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 SOMEF
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
5.Principes pour les mesures organisationnelles	Appr?ciation des ?v?nements li?s ? la s?curit? de l'information et prise de d?cision	3.6	
5.Principes pour les mesures organisationnelles	Fonctions et responsabilit?s li?es ? la s?curit? de l'information	3	
5.Principes pour les mesures organisationnelles	S?paration des t?ches	0	
5.Principes pour les mesures organisationnelles	Responsabilit?s de la direction	2.5	
5.Principes pour les mesures organisationnelles	Relations avec les autorités	3.3	
5.Principes pour les mesures organisationnelles	Relations avec des groupes de travail spécialisés	5	
5.Principes pour les mesures organisationnelles	Intelligence des menaces	1.2	
5.Principes pour les mesures organisationnelles	Sécurité de l'information dans la gestion de projet	3.8	
5.Principes pour les mesures organisationnelles	Inventaire des informations et des autres actifs associés	1.2	
5.Principes pour les mesures organisationnelles	Utilisation correcte des actifs	3.3	
5.Principes pour les mesures organisationnelles	Restitution des actifs	5	
5.Principes pour les mesures organisationnelles	Classification de l'information	2.5	
5.Principes pour les mesures organisationnelles	Marquage des informations	4	
5.Principes pour les mesures organisationnelles	Transfert de l'information	5	
5.Principes pour les mesures organisationnelles	Contrôle d'accès		
5.Principes pour les mesures organisationnelles	Gestion des identités		
5.Principes pour les mesures organisationnelles	Informations d'authentification		
5.Principes pour les mesures organisationnelles	Droits d'accès		
5.Principes pour les mesures organisationnelles	Sécurité de l'information dans les relations avec les fournisseurs	5	

5.Principes pour les mesures organisationnelles	Prise en compte de la sécurité de l'information dans les accords conclus avec les fournisseurs	0	
5.Principes pour les mesures organisationnelles	Management de la sécurité de l'information dans la chaîne d'approvisionnement TIC	2.5	
5.Principes pour les mesures organisationnelles	Suivi, revue et gestion du changement des services fournisseurs	5	
5.Principes pour les mesures organisationnelles	Sécurité de l'information dans l'utilisation de services en Nuage	0	
5.Principes pour les mesures organisationnelles	Responsabilités et préparation de la gestion des incidents liés à la sécurité de l'information		
5.Principes pour les mesures organisationnelles	Appréciation des événements liés à la sécurité de l'information et prise de décision		
5.Principes pour les mesures organisationnelles	Réponse aux incidents liés à la sécurité de l'information		
5.Principes pour les mesures organisationnelles	Tirer des enseignements des incidents liés à la sécurité de l'information		
5.Principes pour les mesures organisationnelles	Recueil de preuves		
5.Principes pour les mesures organisationnelles	Sécurité de l'information durant une perturbation	5	
5.Principes pour les mesures organisationnelles	Préparation des TIC pour la continuité d'activité	5	
5.Principes pour les mesures organisationnelles	Identification des exigences légales, statutaires, réglementaires et contractuelles		
5.Principes pour les mesures organisationnelles	Droits de propriété intellectuelle		
5.Principes pour les mesures organisationnelles	Protection des enregistrements		
5.Principes pour les mesures organisationnelles	Vie privée et protection des DCP		
5.Principes pour les mesures organisationnelles	Revue indépendante de la sécurité de l'information		
5.Principes pour les mesures organisationnelles	Conformité aux politiques et normes de sécurité de l'information		
5.Principes pour les mesures organisationnelles	Procédures d'exploitation documentées		
6 Principes pour les mesures liées aux personnes	Présélection	2	
6 Principes pour les mesures liées aux personnes	Conditions générales d'embauche	1.7	
6 Principes pour les mesures liées aux personnes	Sensibilisation, apprentissage et formation à la sécurité de l'information	5	
6 Principes pour les mesures liées aux personnes	Processus disciplinaire	2	

6 Principes pour les mesures liées aux personnes	Responsabilités consécutivement à la fin ou à la modification du contrat de travail	3.3	
6 Principes pour les mesures liées aux personnes	Engagements de confidentialité ou de non-divulgation	5	
6 Principes pour les mesures liées aux personnes	Travail à distance	5	
6 Principes pour les mesures liées aux personnes	Signalement des événements liés à la sécurité de l'information		
7 Principes pour les mesures physiques	Périmètre de sécurité physique		
7 Principes pour les mesures physiques	Contrôles physiques des accès		
7 Principes pour les mesures physiques	Sécurisation des bureaux, des salles et des équipements		
7 Principes pour les mesures physiques	Surveillance de la sécurité physique		
7 Principes pour les mesures physiques	Protection contre les menaces extérieures et Environnementales		
7 Principes pour les mesures physiques	Travail dans les zones sécurisées		
7 Principes pour les mesures physiques	Bureau propre et écran vide		
7 Principes pour les mesures physiques	Emplacement et protection du matériel		
7 Principes pour les mesures physiques	Sécurité du matériel et des actifs hors des locaux		
7 Principes pour les mesures physiques	Supports de stockage		
7 Principes pour les mesures physiques	Services généraux		
7 Principes pour les mesures physiques	Sécurité du câblage		
7 Principes pour les mesures physiques	Maintenance du matériel		
7 Principes pour les mesures physiques	Mise au rebut ou recyclage sécurisé(e) du matériel		
8 Principes pour les mesures technologiques	Terminaux utilisateurs	3.8	
8 Principes pour les mesures technologiques	Privilèges d'accès		
8 Principes pour les mesures technologiques	Restriction d'accès à l'information		
8 Principes pour les mesures technologiques	Accès au code source		
8 Principes pour les mesures technologiques	Authentification sécurisée		
8 Principes pour les mesures technologiques	Dimensionnement		
8 Principes pour les mesures technologiques	Protection contre les programmes malveillants		
8 Principes pour les mesures technologiques	Gestion des vulnérabilités techniques		
8 Principes pour les mesures technologiques	Gestion de la configuration	5	

8 Principes pour les mesures technologiques	Suppression d'information		
8 Principes pour les mesures technologiques	Masquage des données	2.5	
8 Principes pour les mesures technologiques	DLP	3.8	
8 Principes pour les mesures technologiques	Sauvegarde des informations		
8 Principes pour les mesures technologiques	Redondance des moyens de traitement de l'information		
8 Principes pour les mesures technologiques	Journalisation		
8 Principes pour les mesures technologiques	Activités de surveillance		
8 Principes pour les mesures technologiques	Synchronisation des horloges		
8 Principes pour les mesures technologiques	Utilisation de programmes utilitaires à privilèges		
8 Principes pour les mesures technologiques	Installation de logiciels sur des systèmes en exploitation		
8 Principes pour les mesures technologiques	Mesures liées aux réseaux	3.3	
8 Principes pour les mesures technologiques	Sécurité des services en réseau	2	
8 Principes pour les mesures technologiques	Cloisonnement des réseaux	2	
8 Principes pour les mesures technologiques	Filtrage Internet		
8 Principes pour les mesures technologiques	Utilisation de la cryptographie	2.5	
8 Principes pour les mesures technologiques	Cycle de vie de développement sécurisé		
8 Principes pour les mesures technologiques	Exigences de sécurité des applications		
8 Principes pour les mesures technologiques	Principes d'ingénierie et d'architecture système sécurisée		
8 Principes pour les mesures technologiques	Codage sécurisé		
8 Principes pour les mesures technologiques	Tests de sécurité dans le développement et l'acceptation		
8 Principes pour les mesures technologiques	Développement externalisé		
8 Principes pour les mesures technologiques	Séparation des environnements de développement, de test et de production		
8 Principes pour les mesures technologiques	Gestion des changements		
8 Principes pour les mesures technologiques	Informations relatives aux tests		
8 Principes pour les mesures technologiques	Protection des systèmes d'information en cours d'audit et de test		

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**

Présentation détaillée des résultats de l'audit
Résultat par domaine de sécurité

Domaine	**Critères d'audit**	**Résultats de l'audit (constats)**	**Description des vérifications effectuées (tests, conditions de test, etc)**
5 Mesures de sécurité organisationnelles	**5.1 Appr?ciation des ?v?nements li?s ? la s?curit? de l'information et prise de d?cision**	**Bonnes pratiques identifiées**	
		Présence d'une politique de sécurité de l'information ainsi des documents plus détaillés de politiques de sécurité par théme	
		bbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbb	
		Vulnérabilités enregistrées	

5 Mesures de sécurité organisationnelles	**5.2 Fonctions et responsabilit?s li?es ? la s?curit? de l'information**	**Bonnes pratiques identifiées** Présence d'une structure opérationnelle détaillé et d'une organisation de la gestion de la sécurité : RSSI et correspondants ou responsables locaux, réles et responsabilités respectifs et vis-é-vis des responsables opérationnels. **Vulnérabilités enregistrées**	
5 Mesures de sécurité organisationnelles	**5.3 S?paration des t?ches**	**Bonnes pratiques identifiées** **Vulnérabilités enregistrées** Absence de la prise en compte dans la définition des réles et des responsabilités, de la séparation des téches pour des domaines de responsabilité incompatibles avec l'objectif de réduire le risque de fraude, d'erreur et de contournement des mesures de sécurité de l'information.	
5 Mesures de sécurité organisationnelles	**5.4 Responsabilit?s de la direction**	**Bonnes pratiques identifiées** **Vulnérabilités enregistrées** Absence de demandes explicites é tous les salariés et contractants déappliquer les régles de sécurité conformément aux politiques et aux procédures en vigueur dans léorganisation et absence de mesures visant é s'assurer que tout le personnel soit sensibilisé aux responsabilités liées é la sécurité de l'information et qu'il assume ces responsabilités.	
5 Mesures de sécurité organisationnelles	**5.5 Relations avec les autorités**	**Bonnes pratiques identifiées** **Vulnérabilités enregistrées**	

Absence de contacts avec les autorités compétentes afin d'assurer la bonne circulation de l'information é l'égard de la sécurité, entre l'organisation et les autorités légales, réglementaires et de surveillance compétentes.			
5 Mesures de sécurité organisationnelles	**5.6 Relations avec des groupes de travail spécialisés**	**Bonnes pratiques identifiées** Existance de relations avec des groupes de travail spécialisés ou des forums spécialisés dans la sécurité et avec des associations professionnelles, afin d'assurer la bonne circulation de l'information é l'égard de la sécurité. **Vulnérabilités enregistrées**	
5 Mesures de sécurité organisationnelles	**5.7 Intelligence des menaces**	**Bonnes pratiques identifiées** Présence d'un systéme destiné é recueillir les informations relatives aux menaces pour la sécurité de l'information et de les analyser pour produire une intelligence des menaces. **Vulnérabilités enregistrées**	
5 Mesures de sécurité organisationnelles	**5.8 Sécurité de l'information dans la gestion de projet**	**Bonnes pratiques identifiées** La sécurité de l'information est intégrée aux activités de gestion de projet de l'organisation. **Vulnérabilités enregistrées**	
5 Mesures de sécurité organisationnelles	**5.9 Inventaire des informations et des autres actifs associés**	**Bonnes pratiques identifiées** Présence d'inventaire documenté, identifiant les actifs et définissant leurs types. **Vulnérabilités enregistrées**	
5 Mesures de sécurité organisationnelles	**5.10 Utilisation correcte des actifs**	**Bonnes pratiques identifiées** **Vulnérabilités enregistrées**	

Absence des régles d'utilisation correcte et des procédures de traitement de l'information et des autres actifs associés.			
5 Mesures de sécurité organisationnelles	**5.11 Restitution des actifs**	**Bonnes pratiques identifiées** présence de procédures necessaires afin queé le personnel et les autres parties intéressées, au besoin, restituent tous les actifs de l'organisation qui sont en leur possession en cas de modification ou de rupture de leur relation de travail, contrat de travail ou engagement. **Vulnérabilités enregistrées**	
5 Mesures de sécurité organisationnelles	**5.12 Classification de l'information**	**Bonnes pratiques identifiées** Présence d'une classification des informations conformément aux besoins de l'organisation en termes de sécurité de l'information sur le plan de la confidentialité, de l'intégrité, de la disponibilité et des exigences des parties intéressées. Cette classification a pour but d'assurer l'identification et la compréhension des besoins de protection de l'information en fonction de l'importance de celle-ci pour l'organisation. **Vulnérabilités enregistrées**	
5 Mesures de sécurité organisationnelles	**5.13 Marquage des informations**	**Bonnes pratiques identifiées** **Vulnérabilités enregistrées** Absence de procédures pour le marquage de léinformation, conformément au plan de classification de léinformation adopté par léorganisation.	
5 Mesures de sécurité organisationnelles	**5.14 Transfert de l'information**	**Bonnes pratiques identifiées**	

Presence de régles, procédures ou accords de transfert de l'information, aussi bien au sein de l'organisation qu'entre l'organisation et des tierces parties, pour tous les types de fonctions de transfert			
Vulnérabilités enregistrées			
5 Mesures de sécurité organisationnelles	**5.15 Contrôle d'accès**	**Bonnes pratiques identifiées**	
		${5_BestPractice#15}	
		Vulnérabilités enregistrées	
		${5_Vuln#15}	
5 Mesures de sécurité organisationnelles	**5.16 Gestion des identités**	**Bonnes pratiques identifiées**	
		${5_BestPractice#16}	
		Vulnérabilités enregistrées	
		${5_Vuln#16}	
5 Mesures de sécurité organisationnelles	**5.17 Informations d'authentification**	**Bonnes pratiques identifiées**	
		${5_BestPractice#17}	
		Vulnérabilités enregistrées	
		${5_Vuln#17}	
5 Mesures de sécurité organisationnelles	**5.18 Droits d'accès**	**Bonnes pratiques identifiées**	
		${5_BestPractice#18}	
		Vulnérabilités enregistrées	
		${5_Vuln#18}	
5 Mesures de sécurité organisationnelles	**5.19 Sécurité de l'information dans les relations avec les fournisseurs**	**Bonnes pratiques identifiées**	
		Présence de processus et procédures pour gérer les risques de sécurité de l'information qui sont associés é l'utilisation des produits ou services des fournisseurs.	
		Vulnérabilités enregistrées	
5 Mesures de sécurité organisationnelles	**5.20 Prise en compte de la sécurité de l'information dans les accords conclus avec les fournisseurs**	**Bonnes pratiques identifiées**	
		Vulnérabilités enregistrées	
		Absence d'exigences applicables liées é la sécurité de l'information dans les accords avec les fournisseurs ayant accés é l'information de l'organisation.	

5 Mesures de sécurité organisationnelles	**5.21 Management de la sécurité de l'information dans la chaîne d'approvisionnement TIC**	**Bonnes pratiques identifiées** Présence des processus et procédures destinés é traiter les risques de sécurité de l'information associés aux services informatiques et de télécommunication et é la chaéne d'approvisionnement des produits informatiques ou de télécommunication. **Vulnérabilités enregistrées**	
5 Mesures de sécurité organisationnelles	**5.22 Suivi, revue et gestion du changement des services fournisseurs**	**Bonnes pratiques identifiées** Présence de la surveillance réguliére, la revue, l'évaluation et la gestion des changements de pratiques du fournisseur en matiére de sécurité de l'information et de prestation de services, afin de maintenir un niveau convenu de sécurité de léinformation et de prestation de services, conformément aux accords conclus avec les fournisseurs. **Vulnérabilités enregistrées**	
5 Mesures de sécurité organisationnelles	**5.23 Sécurité de l'information dans l'utilisation de services en Nuage**	**Bonnes pratiques identifiées** **Vulnérabilités enregistrées** Absence de processus d'acquisition, d'utilisation, de management et de cessation des services en nuage, conformément aux exigences de sécurité de l'information.é	
5 Mesures de sécurité organisationnelles	**5.24 Responsabilités et préparation de la gestion des incidents liés à la sécurité de l'information**	**Bonnes pratiques identifiées** ${5_BestPractice#24} **Vulnérabilités enregistrées** ${5_Vuln#24}	
5 Mesures de sécurité organisationnelles	**5.25 Appréciation des événements liés à la sécurité de l'information et prise de décision**	**Bonnes pratiques identifiées** ${5_BestPractice#25} **Vulnérabilités enregistrées** ${5_Vuln#25}	

5 Mesures de sécurité organisationnelles	**5.26 Réponse aux incidents liés à la sécurité de l'information**	**Bonnes pratiques identifiées** ${5_BestPractice#26} **Vulnérabilités enregistrées** ${5_Vuln#26}	
5 Mesures de sécurité organisationnelles	**5.27 Tirer des enseignements des incidents liés à la sécurité de l'information**	**Bonnes pratiques identifiées** ${5_BestPractice#27} **Vulnérabilités enregistrées** ${5_Vuln#27}	
5 Mesures de sécurité organisationnelles	**5.28 Recueil de preuves**	**Bonnes pratiques identifiées** ${5_BestPractice#28} **Vulnérabilités enregistrées** ${5_Vuln#28}	
5 Mesures de sécurité organisationnelles	**5.29 Sécurité de l'information durant une perturbation**	**Bonnes pratiques identifiées** Ces Plans de Continuité permettent de maintenir la sécurité de l'information au niveau approprié. **Vulnérabilités enregistrées**	
5 Mesures de sécurité organisationnelles	**5.30 Préparation des TIC pour la continuité d'activité**	**Bonnes pratiques identifiées** Existance d'une planification, d'une mis en éuvre,é d'une gestion et de testes pour la préparation des TIC (Technologies de l'Information et de la Communication) a prpos des objectifs de continuité d'activité et des exigences de continuité des TIC. **Vulnérabilités enregistrées**	
5 Mesures de sécurité organisationnelles	**5.31 Identification des exigences légales, statutaires, réglementaires et contractuelles**	**Bonnes pratiques identifiées** ${5_BestPractice#31} **Vulnérabilités enregistrées** ${5_Vuln#31}	
5 Mesures de sécurité organisationnelles	**5.32 Droits de propriété intellectuelle**	**Bonnes pratiques identifiées** ${5_BestPractice#32} **Vulnérabilités enregistrées** ${5_Vuln#32}	
5 Mesures de sécurité organisationnelles	**5.33 Protection des enregistrements**	**Bonnes pratiques identifiées** ${5_BestPractice#33} **Vulnérabilités enregistrées**	

${5_Vuln#33}			
5 Mesures de sécurité organisationnelles	**5.34 Vie privée et protection des DCP**	**Bonnes pratiques identifiées** ${5_BestPractice#34} **Vulnérabilités enregistrées** ${5_Vuln#34}	
5 Mesures de sécurité organisationnelles	**5.35 Revue indépendante de la sécurité de l'information**	**Bonnes pratiques identifiées** ${5_BestPractice#35} **Vulnérabilités enregistrées** ${5_Vuln#35}	
5 Mesures de sécurité organisationnelles	**5.36 Conformité aux politiques et normes de sécurité de l'information**	**Bonnes pratiques identifiées** ${5_BestPractice#36} **Vulnérabilités enregistrées** ${5_Vuln#36}	
5 Mesures de sécurité organisationnelles	**5.37 Procédures d'exploitation documentées**	**Bonnes pratiques identifiées** ${5_BestPractice#37} **Vulnérabilités enregistrées** ${5_Vuln#37}	
6 Mesures de sécurité applicables aux personnes	**6.1 Présélection**	**Bonnes pratiques identifiées** Vérification des références concernant tous les candidats é l'embauche avant qu'ils n'intégrent l'organisation puis de faéon continue, conformément aux lois, aux réglementations et é l'éthique **Vulnérabilités enregistrées**	
6 Mesures de sécurité applicables aux personnes	**6.2 Conditions générales d'embauche**	**Bonnes pratiques identifiées** Les contrats de travail précisent clairement les responsabilités qui incombent au personnel et é l'organisation en matiére de sécurité de l'information **Vulnérabilités enregistrées**	
6 Mesures de sécurité applicables aux personnes	**6.3 Sensibilisation, apprentissage et formation à la sécurité de l'information**	**Bonnes pratiques identifiées**	

Presence d'une organisation telle que le personnel de l'organisation et les parties intéressées soient sensibilisés et suivent un apprentissage et des formations é la sécurité de l'information adaptés, et qu'ils reéoivent réguliérement les mises é jour des politiques et procédures de l'organisation s'appliquant é leur fonction **Vulnérabilités enregistrées**			
6 Mesures de sécurité applicables aux personnes	**6.4 Processus disciplinaire**	**Bonnes pratiques identifiées** **Vulnérabilités enregistrées** Absence un processus disciplinaire permettant de prendre des mesures é l'encontre du personnel et des autres parties intéressées qui ont commis une violation de la politique de sécurité de l'information.	
6 Mesures de sécurité applicables aux personnes	**6.5 Responsabilités consécutivement à la fin ou à la modification du contrat de travail**	**Bonnes pratiques identifiées** **Vulnérabilités enregistrées** Absence d'une détermination des responsabilités et des missions liées é la sécurité de l'information qui restent valables consécutivement é la fin ou é la modification du contrat de travail.	
6 Mesures de sécurité applicables aux personnes	**6.6 Engagements de confidentialité ou de non-divulgation**	**Bonnes pratiques identifiées** Présence d'engagements de confidentialité ou de non-divulgation, conformément aux besoins de l'organisation en matiére de protection de l'information, afin de gérer la confidentialité de l'information accessible au personnel ou é de tierces parties **Vulnérabilités enregistrées**	
6 Mesures de sécurité applicables aux personnes	**6.7 Travail à distance**	**Bonnes pratiques identifiées**	

présence de mesures de sécurité lorsque le personnel travaille é distance, pour protéger les informations consultées, traitées ou stockées en dehors des locaux de l'organisation			
Vulnérabilités enregistrées			
6 Mesures de sécurité applicables aux personnes	**6.8 Signalement des événements liés à la sécurité de l'information**	**Bonnes pratiques identifiées**	
		${6_BestPractice#8}	
		Vulnérabilités enregistrées	
		${6_Vuln#8}	
7 Mesures de sécurité physique	**1. Périmètre de sécurité physique**	**Bonnes pratiques identifiées**	
		${7_BestPractice#1}	
		Vulnérabilités enregistrées	
		${7_Vuln#1}	
7 Mesures de sécurité physique	**2. Contrôles physiques des accès**	**Bonnes pratiques identifiées**	
		${7_BestPractice#2}	
		Vulnérabilités enregistrées	
		${7_Vuln#2}	
7 Mesures de sécurité physique	**3. Sécurisation des bureaux, des salles et des équipements**	**Bonnes pratiques identifiées**	
		${7_BestPractice#3}	
		Vulnérabilités enregistrées	
		${7_Vuln#3}	
7 Mesures de sécurité physique	**4. Surveillance de la sécurité physique**	**Bonnes pratiques identifiées**	
		${7_BestPractice#4}	
		Vulnérabilités enregistrées	
		${7_Vuln#4}	
7 Mesures de sécurité physique	**5. Protection contre les menaces extérieures et Environnementales**	**Bonnes pratiques identifiées**	
		${7_BestPractice#5}	
		Vulnérabilités enregistrées	
		${7_Vuln#5}	
7 Mesures de sécurité physique	**6. Travail dans les zones sécurisées**	**Bonnes pratiques identifiées**	
		${7_BestPractice#6}	
		Vulnérabilités enregistrées	
		${7_Vuln#6}	
7 Mesures de sécurité physique	**7. Bureau propre et écran vide**	**Bonnes pratiques identifiées**	
		${7_BestPractice#7}	
		Vulnérabilités enregistrées	
		${7_Vuln#7}	
7 Mesures de sécurité physique	**8. Emplacement et protection du matériel**	**Bonnes pratiques identifiées**	

${7_BestPractice#8} **Vulnérabilités enregistrées** ${7_Vuln#8}			
7 Mesures de sécurité physique	**9. Sécurité du matériel et des actifs hors des locaux**	**Bonnes pratiques identifiées** ${7_BestPractice#9} **Vulnérabilités enregistrées** ${7_Vuln#9}	
7 Mesures de sécurité physique	**10. Supports de stockage**	**Bonnes pratiques identifiées** ${7_BestPractice#10} **Vulnérabilités enregistrées** ${7_Vuln#10}	
7 Mesures de sécurité physique	**11. Services généraux**	**Bonnes pratiques identifiées** ${7_BestPractice#11} **Vulnérabilités enregistrées** ${7_Vuln#11}	
7 Mesures de sécurité physique	**12. Sécurité du câblage**	**Bonnes pratiques identifiées** ${7_BestPractice#12} **Vulnérabilités enregistrées** ${7_Vuln#12}	
7 Mesures de sécurité physique	13. Maintenance du matériel	**Bonnes pratiques identifiées** ${7_BestPractice#13} **Vulnérabilités enregistrées** ${7_Vuln#13}	
7 Mesures de sécurité physique	14. Mise au rebut ou recyclage sécurisé(e) du matériel	**Bonnes pratiques identifiées** ${7_BestPractice#14} **Vulnérabilités enregistrées** ${7_Vuln#14}	
8 Mesures de sécurité technologiques	1.Terminaux utilisateurs	**Bonnes pratiques identifiées** Presence d'une politique portant sur le théme de la configuration et de la manipulation sécurisées des terminaux utilisateurs finaux, afin de protéger toute information stockée sur un terminal utilisateur final, traitée par ou accessible via ce type d'appareil **Vulnérabilités enregistrées**	
8 Mesures de sécurité technologiques	2.Privilèges d'accès	**Bonnes pratiques identifiées** ${8_BestPractice#2} **Vulnérabilités enregistrées**	

${8_Vuln#2}			
8 Mesures de sécurité technologiques	3.Restriction d'accès à l'information	**Bonnes pratiques identifiées**	
		${8_BestPractice#3}	
		Vulnérabilités enregistrées	
		${8_Vuln#3}	
8 Mesures de sécurité technologiques	4.Accès au code source	**Bonnes pratiques identifiées**	
		${8_BestPractice#4}	
		Vulnérabilités enregistrées	
		${8_Vuln#4}	
8 Mesures de sécurité technologiques	5.Authentification sécurisée	**Bonnes pratiques identifiées**	
		${8_BestPractice#5}	
		Vulnérabilités enregistrées	
		${8_Vuln#5}	
8 Mesures de sécurité technologiques	6.Dimensionnement	**Bonnes pratiques identifiées**	
		${8_BestPractice#6}	
		Vulnérabilités enregistrées	
		${8_Vuln#6}	
8 Mesures de sécurité technologiques	7.Protection contre les programmes malveillants	**Bonnes pratiques identifiées**	
		${8_BestPractice#7}	
		Vulnérabilités enregistrées	
		${8_Vuln#7}	
8 Mesures de sécurité technologiques	8.Gestion des vulnérabilités techniques	**Bonnes pratiques identifiées**	
		${8_BestPractice#8}	
		Vulnérabilités enregistrées	
		${8_Vuln#8}	
8 Mesures de sécurité technologiques	9.Gestion de la configuration	**Bonnes pratiques identifiées**	
		${8_BestPractice#9}	
		Vulnérabilités enregistrées	
		${8_Vuln#9}	
8 Mesures de sécurité technologiques	10.Suppression d'information	**Bonnes pratiques identifiées**	
		${8_BestPractice#10}	
		Vulnérabilités enregistrées	
		${8_Vuln#10}	
8 Mesures de sécurité technologiques	11.Masquage des données	**Bonnes pratiques identifiées**	
		Vulnérabilités enregistrées	

Absence de procédures de masquage des données conformément é la politique de l'organisation portant sur le théme du contréle d'accés et aux exigences métier, tout en prenant en compte les exigences d'ordre légal.			
8 Mesures de sécurité technologiques	12.DLP	**Bonnes pratiques identifiées**	
		Vulnérabilités enregistrées	
		Absence de mesures de prévention de la fuite de données aux systémes, réseaux et terminaux qui traitent, stockent ou transmettent de l'information sensible.	
8 Mesures de sécurité technologiques	13.Sauvegarde des informations	**Bonnes pratiques identifiées**	
		${8_BestPractice#13}	
		Vulnérabilités enregistrées	
		${8_Vuln#13}	
8 Mesures de sécurité technologiques	14.Redondance des moyens de traitement de l'information	**Bonnes pratiques identifiées**	
		${8_BestPractice#14}	
		Vulnérabilités enregistrées	
		${8_Vuln#14}	
8 Mesures de sécurité technologiques	15.Journalisation	**Bonnes pratiques identifiées**	
		${8_BestPractice#15}	
		Vulnérabilités enregistrées	
		${8_Vuln#15}	
8 Mesures de sécurité technologiques	16.Activités de surveillance	**Bonnes pratiques identifiées**	
		${8_BestPractice#16}	
		Vulnérabilités enregistrées	
		${8_Vuln#16}	
8 Mesures de sécurité technologiques	17.Synchronisation des horloges	**Bonnes pratiques identifiées**	
		${8_BestPractice#17}	
		Vulnérabilités enregistrées	
		${8_Vuln#17}	
8 Mesures de sécurité technologiques	18.Utilisation de programmes utilitaires à privilèges	**Bonnes pratiques identifiées**	
		${8_BestPractice#18}	
		Vulnérabilités enregistrées	
		${8_Vuln#18}	

8 Mesures de sécurité technologiques	19.Installation de logiciels sur des systèmes en exploitation	**Bonnes pratiques identifiées**	
		${8_BestPractice#19}	
		Vulnérabilités enregistrées	
		${8_Vuln#19}	
8 Mesures de sécurité technologiques	20.Mesures liées aux réseaux	**Bonnes pratiques identifiées**	
		Vulnérabilités enregistrées	
		Les réseaux ne sont pas gérés ni contrélés afin de garantir la protection de l'information contenue dans les systémes et les applications	
8 Mesures de sécurité technologiques	21.Sécurité des services en réseau	**Bonnes pratiques identifiées**	
		Vulnérabilités enregistrées	
		Absence de la surveillance des mécanismes de sécurité, des niveaux de service et des exigences de services des services en réseau	
8 Mesures de sécurité technologiques	22.Cloisonnement des réseaux	**Bonnes pratiques identifiées**	
		Vulnérabilités enregistrées	
		Absence de cloisonnement, des groupes de services d'information, d'utilisateurs et de systémes d'information dans les réseaux	
8 Mesures de sécurité technologiques	23.Filtrage Internet	**Bonnes pratiques identifiées**	
		${8_BestPractice#23}	
		Vulnérabilités enregistrées	
		${8_Vuln#23}	
8 Mesures de sécurité technologiques	24.Utilisation de la cryptographie	**Bonnes pratiques identifiées**	
		Présence des régles relatives é l'utilisation de la cryptographie et é la gestion des clés cryptographiques	
		Vulnérabilités enregistrées	
8 Mesures de sécurité technologiques	25.Cycle de vie de développement sécurisé	**Bonnes pratiques identifiées**	
		${8_BestPractice#25}	
		Vulnérabilités enregistrées	
		${8_Vuln#25}	
8 Mesures de sécurité technologiques	26.Exigences de sécurité des applications	**Bonnes pratiques identifiées**	

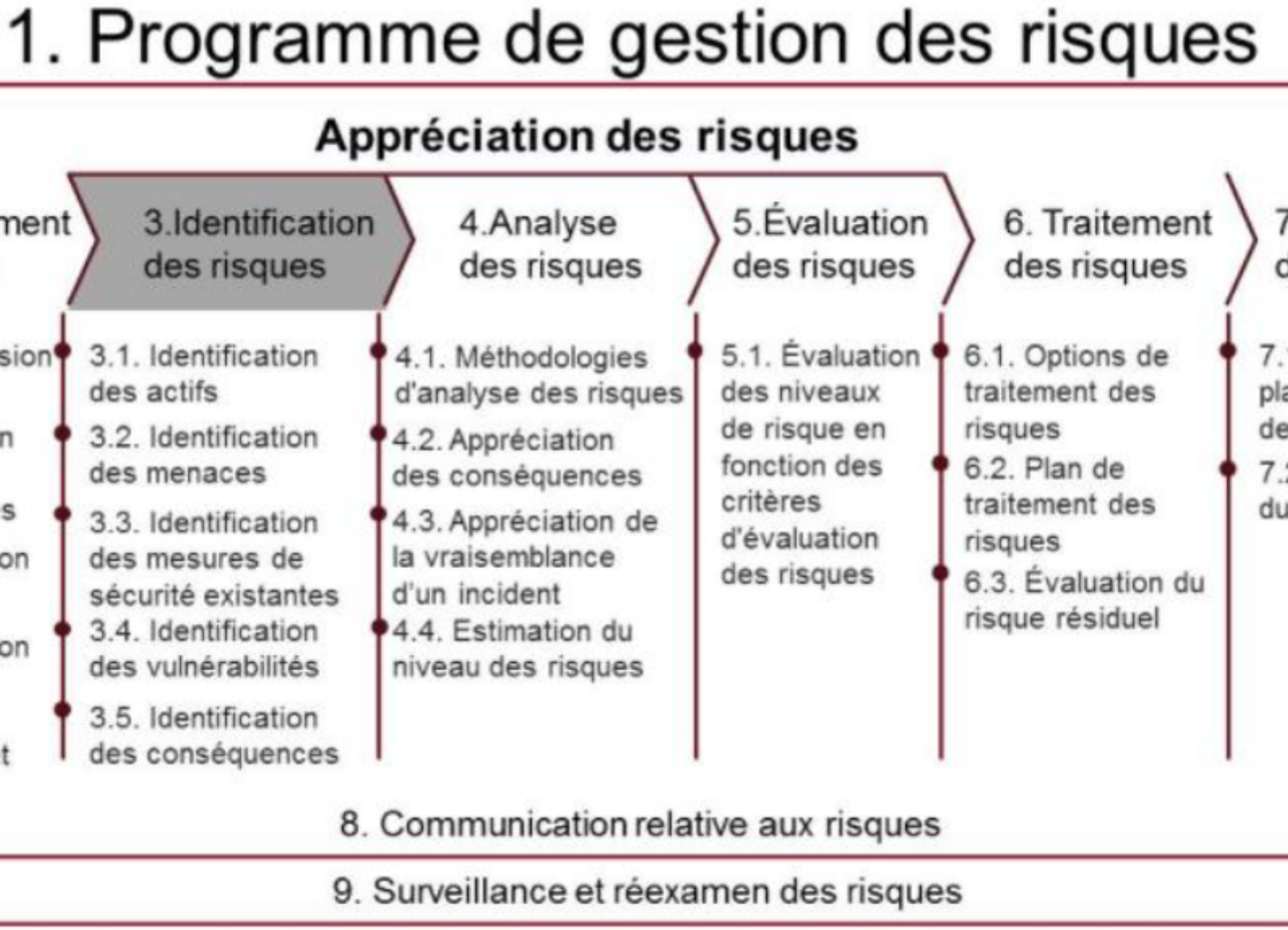
${8_BestPractice#26}			
Vulnérabilités enregistrées			
${8_Vuln#26}			
8 Mesures de sécurité technologiques	27.Principes d'ingénierie et d'architecture système sécurisée	**Bonnes pratiques identifiées**	
		${8_BestPractice#27}	
		Vulnérabilités enregistrées	
		${8_Vuln#27}	
8 Mesures de sécurité technologiques	28.Codage sécurisé	**Bonnes pratiques identifiées**	
		${8_BestPractice#28}	
		Vulnérabilités enregistrées	
		${8_Vuln#28}	
8 Mesures de sécurité technologiques	29.Tests de sécurité dans le développement et l'acceptation	**Bonnes pratiques identifiées**	
		${8_BestPractice#29}	
		Vulnérabilités enregistrées	
		${8_Vuln#29}	
8 Mesures de sécurité technologiques	30.Développement externalisé	**Bonnes pratiques identifiées**	
		${8_BestPractice#30}	
		Vulnérabilités enregistrées	
		${8_Vuln#30}	
8 Mesures de sécurité technologiques	31.Séparation des environnements de développement, de test et de production	**Bonnes pratiques identifiées**	
		${8_BestPractice#31}	
		Vulnérabilités enregistrées	
		${8_Vuln#31}	
8 Mesures de sécurité technologiques	32.Gestion des changements	**Bonnes pratiques identifiées**	
		${8_BestPractice#32}	
		Vulnérabilités enregistrées	
		${8_Vuln#32}	
8 Mesures de sécurité technologiques	33.Informations relatives aux tests	**Bonnes pratiques identifiées**	
		${8_BestPractice#33}	
		Vulnérabilités enregistrées	
		${8_Vuln#33}	
8 Mesures de sécurité technologiques	34.Protection des systèmes d'information en cours d'audit et de test	**Bonnes pratiques identifiées**	
		${8_BestPractice#34}	
		Vulnérabilités enregistrées	
		${8_Vuln#34}	

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}

Détails audit technique
Description dans les Rapports d'audit Technique.
Appréciation des risques
La démarche d'appréciation des risques adoptée
Nous nous proposons d'effectuer une analyse des risques menaçant la sécurité du système d'information du **SOMEF** 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.
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

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:

Organisation de la sécurité

Sécurité des Sites

Sécurité des systèmes et de leur architecture

Exploitation et administration des systèmes

Sécurité applicative et continuité de l'activité

Protection des postes de travail utilisateurs
Sécurité des projets et développements applicatifs
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

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 :

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

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**	