Modèle de Rapport d'Audit de la Sécurité des Systèmes d'Information

(En application au décret-loi 2023-17 du 11 mars 2023)

Date	Version	Nature de modification
19/12/2014	1.0	Version initiale
03/06/2015	1.1	Ajout de recommandations
03/05/2017	1.2	Mise à jour des domaines de l'audit
14/10/2019	1.3	MAJ suite à la publication de l'arrêté du ministre des technologies de la communication et de l'économie numérique et du ministre du développement, de l'investissement et de la coopération internationale du 01 Octobre 2019, fixant le cahier des charges relatif à l'exercice de l'activité d'audit dans le domaine de la sécurité de l'information
09/12/2019	1.4	MAJ de la section « Synthèse des résultats de l'audit »
11/09/2023	2.0	MAJ suite à l'entrée en vigueur du décret-loi 2023-17 du 11 mars 2023, relatif à la cybersécurité, et à la publication de la version 2022 de la norme ISO/IEC 27002
18/09/2023	2.1	MAJ suite à la publication de l'arrêté du ministre des technologies de la communication du 12 Septembre 2023, fixant les critères techniques d'audit et les modalités de suivi de la mise en œuvre des recommandations contenues dans le rapport d'audit

<Nom de l'expert auditeur>

<Insérer le logo de l'expert auditeur ici>

Rapport d'Audit de la Sécurité du Système d'Information

De *<Nom_organisme_audité>*

<Insérer le logo de l'expert auditeur ici>

Expert Auditeur chargé de la mission :……

Signature : …….

<Insérer le cachet de l'expert auditeur ici>

Version du document	Date	Diffusion
<version>	***<date>***	Document Confidentiel

1 Avant propos

1.1 Confidentialité du document

Le présent document est confidentiel et sa confidentialité consiste à :

- La non divulgation desdites informations confidentielles auprès de tierce partie,
- La non reproduction des informations dites confidentielles, sauf accord de l'organisme audité,
- 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 l'organisme audité déclarées Confidentielles.

1.2 Historique des modifications

Version	Date	Auteur	Modifications

1.3 Diffusion du document

Diffusion (coté *Nom_Expert_Auditeur*)				
Nom	Prénom	Titre	Tél	Mail
Diffusion (coté *Nom_Organisme_Audité*)				
Nom	Prénom	Titre	Tél	Mail

2 Cadre de la mission

- Rappeler le cadre de la mission d'audit (en application au décret-loi 2023-17 du 11 mars 2023 et à l'arrêté du ministre des technologies de la communication du 12 Septembre 2023, fixant les critères techniques d'audit et les modalités de suivi de la mise en œuvre des recommandations contenues dans le rapport d'audit),
- Indiquer si la présente mission est un audit exhaustif ou audit de suivi (mission sur 3 années),
- Présenter l'objectif de cette mission d'audit (Etat de conformité par rapport à un standard, recommandations, plan d'action),
- Indiquer, le cas échéant, si la présente mission rentre dans le cadre de la préparation à la certification ISO 27001 ou dans une autre démarche de conformité,
- Indiquer, le cas échéant, le(s) standard(s) métier de référence par rapport auquel est réalisée la présente mission d'audit,
- Indiquer les limites et les contraintes de l'audit (échantillonnage, changements depuis l'audit, etc).

3 Termes et définitions

- Donner les définitions des termes utilisés dans le présent rapport.

4 Références

- Indiquer tous les documents de référence utilisés pour la réalisation de la présente mission d'audit.

5 Présentation de l'organisme audité

- Présenter brièvement l'organisme audité (création, nombre d'employés, étendu géographique, missions, services fournis, parties prenantes, clients, etc) conformément au modèle présenté en **Annexe 1**,
- Présenter la cartographie des processus de l'organisme audité (avec la cartographie des flux de données),
- Pour chaque processus, indiquer les exigences en disponibilité, intégrité et confidentialité des données traitées à ce niveau conformément au modèle présenté en **Annexe 2**, ceci afin d'identifier et maîtriser les processus métier de l'organisme audité pour que l'appréciation des risques soit focalisée sur les processus métier les plus critiques selon l'activité de l'organisme audité.

6 Champ d'audit

6.1 Périmètre géographique

- Présenter la liste des structures à auditer :

	Structure	Lieu d'implantation
1		
2		
3		

…		

- Justifier le choix du périmètre géographique de la mission d'audit, et présenter les critères d'échantillonnage, le cas échéant.

6.2 Description des systèmes d'information

- Décrire les systèmes d'information des différentes structures: Pour chaque structure, présenter tous les composants du système d'information avec justification des exclusions le cas échéant selon le modèle « Description du SI de *Nom_Organisme_Audité* » (voir **Annexe 3**),
- Toute exclusion d'un composant du système d'information (serveur, application, base de données, équipement réseau, solution de sécurité ou d'administration, …) doit être bien justifiée.

6.3 Schéma synoptique de l'architecture du réseau

Schématiser le réseau de *Nom_Organisme_Audité* en faisant apparaitre les connexions (LAN, WAN, etc), la segmentation, l'emplacement des composantes du SI, etc…

7 Méthodologie d'audit

- Décrire en détail la méthodologie d'audit adoptée,

- Identifier les domaines de la sécurité des systèmes d'information couverts par la méthodologie d'audit (tout en établissant la correspondance entre les domaines couverts et les référentiels d'audit utilisés).

Remarques et Recommandations :

- ✓ L'audit devra prendre comme référentiel de base le référentiel d'audit de la Sécurité des Systèmes d'Information établi par l'ANCS,
- ✓ La maturité des mesures et contrôles de sécurité mis en place doit être établie en rapport avec les quatre (04) domaines dudit référentiel :
  - **5 Mesures organisationnelles**
  - **6 Mesures liées aux personnes**
  - **7 Mesures d'ordre physique**
  - **8 Mesures technologiques**

- Présenter les outils d'audit utilisés

Outils	Version utilisée	License	Fonctionnalités	Composantes du SI objet de l'audit

- Présenter les checklists utilisés

Titre du document	Version	Source	Description	Composantes du SI objet de l'audit

- Présenter l'équipe du projet coté *Nom_Expert_Auditeur* :

Nom Prénom	Qualité	Qualification	Certifié par l'ANCS	Champs d'intervention
….	Chef de projet	Ingénieur, certifié ISO…, …		Ex : AOP, Audit serveurs, Audit BD, Audit équipements réseaux, …
	Chef d'équipe			
	Membre			
	…			

- Présenter l'équipe du projet coté *Nom_Organisme_Audité* :

Nom Prénom	Qualité	Fonction
…	Chef de projet	Directeur …
	…	

- Présenter le planning d'exécution réel de la mission d'audit selon le modèle « Planning réel d'exécution de la mission d'audit de la sécurité du SI de *Nom_Organisme_Audité* » (voir **Annexe 4**)

8 Synthèse des résultats de l'audit

- Rappeler les critères et les standards/référentiels par rapport auxquels l'audit a été réalisé,

- Rappeler la responsabilité de l'auditeur et les limites de l'audit (échantillonnage, changements depuis l'audit, etc…),

- Rappeler les types et nature de test réalisés pour établir ces résultats,

- Donner une évaluation détaillée de la réalisation du plan d'action issu de la dernière mission d'audit selon le modèle « Evaluation du dernier plan d'action » (Voir **Annexe 5**),

- Présenter l'évolution des indicateurs de sécurité de l'année actuelle par rapport à l'exercice de l'audit précédent.

- Présenter une synthèse des principales bonne pratiques identifiées et défaillances enregistrées lors de l'audit,

- Présenter un état de maturité de la sécurité du système d'information de l'organisme audité selon le modèle « Etat de maturité de la sécurité du système d'information de Nom_Organisme_Audité» (voir **Annexe 6**),

- Présenter les indicateurs de sécurité selon le modèle « Indicateurs de sécurité » (Voir **Annexe 7**),

- Présenter, le cas échéant, les vulnérabilités très critiques détectées et jugées être d'un intérêt particulier pouvant affecter la sécurité du cyber espace national (Voir **Annexe 8**).

Ces vulnérabilités doivent être signalées, immédiatement, lors de la réalisation de la mission d'audit, à l'agence ainsi que l'organisme concerné pour prendre les contremesures nécessaires.

9 Présentation détaillée des résultats de l'audit

- Pour chaque domaine du référentiel d'audit de la sécurité des systèmes d'information, il s'agit de:
    - Présenter la liste des contrôles/mesures vérifiés considérés comme critères d'audit.
    - présenter les bonnes pratiques identifiées.
    - présenter la liste de vulnérabilités.

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 Politiques de sécurité de l'information	**Bonnes pratiques identifiées**	
		Bonne pratique 1	
		Bonne pratique 2	
		….	
		Vulnérabilités enregistrées	
		Vulnérabilité 1 - Référence de la vulnérabilité 1	
		….	
	5.2 Fonctions et responsabi-lités liées à la sécurité de l'information	**Bonnes pratiques identifiées**	
		Bonne pratique 1	
		Bonne pratique 2	
		….	
		Vulnérabilités enregistrées	
		Vulnérabilité 1 - Référence de la vulnérabilité 1	
		….	
	Critère 3		
	….		
6 Mesures de sécurité applicables aux personnes	**Critère 1**		
	…		
7 Mesures de sécurité physique	**Critère 1**		
	…		
8 Mesures de sécurité technologiques	**Critère 1**		
	…		

Pour chaque vulnérabilité non acceptable enregistrée :

Référence de la vulnérabilité:
Description :
Criticité :
Preuve(s) d'audit : les preuves d'audit doivent être regroupées par domaine, triées par critère d'audit et placées dans une Annexe « Preuves d'audit – *Libellé du Domaine* »
Composante(s) du SI impactée(s) :
Recommandation :

Remarques et Recommandations :

- ✓ Les domaines de la sécurité des systèmes d'information couverts par l'audit peuvent être classés en 4 niveaux :
  - Aspects organisationnels de la sécurité des systèmes d'information
  - Aspects liées aux personnes
  - Sécurité physiques des systèmes d'information
  - Sécurité opérationnelle des systèmes d'information

  L'audit de la sécurité opérationnelle doit couvrir les volets suivants :
  - Audit de l'architecture réseau
  - Audit de l'infrastructure réseau et sécurité
  - Audit de la sécurité des serveurs (couche système et rôle du serveur)
  - Audit de la sécurité des applications
  - Audit de la sécurité des postes de travail
- ✓ Lors de la présentation détaillée des vulnérabilités, possibilité de faire référence à des documents annexes qui détaillent les vulnérabilités identifiées par domaine (vulnérabilités d'ordre organisationnel, vulnérabilités liées aux personnes, vulnérabilités d'ordre physique, vulnérabilités d'ordre technique : volet système, volet réseau, volet applicatif, …), sous condition que :

  - Les différentes vulnérabilités détaillées aux niveaux des documents annexes soient identifiées au niveau du tableau de la section 9 avec utilisation des mêmes références de vulnérabilités au niveau du tableau et des documents annexes,
  - Les vulnérabilités soient présentées d'une façon unifiée selon le format ci-dessus.
- ✓ Les critères d'audit doivent être vérifiés sur toutes les composantes du champ de l'audit, toute exclusion du champ de l'audit doit être argumentée.

  En cas de recours à l'échantillonnage, en commun accord avec le maitre d'ouvrage, pour l'audit des certains composants, l'auditeur doit:
  - présenter clairement les critères de choix probants de l'échantillonnage;
  - décrire explicitement l'échantillon (l'échantillon doit être représentatif);
  - couvrir par l'audit tout l'échantillon choisi.
- ✓ Les résultats de l'audit peuvent être classés par composante du système d'information ;

  c.à.d pour chaque composante du SI, l'auditeur peut regrouper toutes les bonnes pratiques identifiées et les vulnérabilités identifiées en les classant par domaine et par critère d'audit.
- ✓ Les preuves d'audit peuvent être de nature :

  - Physique : c'est ce que l'on voit, constate = observation,
  - Testimoniale : témoignages. C'est une preuve très fragile qui doit toujours être recoupée et validée par d'autres preuves,
  - Documentaire : procédures écrites, comptes rendus, notes,

- Analytique : rapprochements, déductions à partir des résultats des tests techniques.

Les preuves d'audit relatives aux aspects de la sécurité opérationnelle doivent comprendre des preuves de nature analytique (résultats de scan, résultats des tests d'intrusion, etc).

Il est fortement recommandé d'accorder de l'importance à la consolidation des résultats de différents outils et moyens d'audit (tests manuels, check-lists de bonnes pratiques, outils automatiques de scan de vulnérabilités, outils de tests d'intrusion).

10 Appréciation des risques

- Décrire la démarche d'appréciation des risques adoptée.
- Justifier le choix des processus métier pour la conduite de l'appréciation des risques.
- Présenter les résultats d'appréciation des risques

Cette étude doit permettre de dresser la liste des scénarii des risques les plus prépondérants triés par ordre de criticité en identifiant :

- 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 :

11 Plan d'action

- Organiser par projets les actions/recommandations associées aux différentes vulnérabilités décelées.
- Indiquer que le plan d'action est établit en commun accord avec l'audité.
- Indiquer que le plan d'action prend en considération les objectifs, les projets en cours et les perspectives de l'audité.
- Indiquer que le plan d'action prend en considération les résultats de l'appréciation des risques déjà établi.
- Indiquer que les estimations proposées par l'auditeur sont données sur la base d'un dimensionnement adéquat des besoins de l'audité, de ses capacités humaines et financières et de l'offre sur la marché tunisien.
- Organiser par projets les actions/recommandations associées aux différentes vulnérabilités décelées.
- Dresser le plan d'action selon le modèle « Plan d'action proposé » (Voir **Annexe 9**)

Annexe 1

Nom de l'organisme	
Acronyme	
Statut	Public, Privé
Secteur d'activité	Administration, Finances/Assurances, Energie/Industrie, Services, Social/Santé, etc. …
Catégorie	Ministère, Administration, Entreprise, Banque, Assurance, …
Site web	
Adresse Email	

Annexe 2

Désignation du processus	Exigences des données traitées en (1)		
	Confidentialité	Intégrité	Disponibilité
Processus 1			
Processus 2			
…			
Processus n			

(1) Classement en 4 niveaux : faible (1), moyen (2), fort (3) et très fort (4).

Annexe 3 : Description du SI de *Nom_Organisme_Audité*

Pour chaque site du périmètre géographique de la mission d'audit:

Applications							
Nom **(1)**	Modules	Description	Environnement de développement	Développée par /Année	Noms ou @IP des serveurs d'hébergement **(2)**	Nombre d'utilisateurs	**Incluse au périmètre d'audit (7)**
...							

Serveurs (par plateforme)					
Nom **(1)**	@IP	Type **(3)**	Système d'exploitation	Rôle/métier **(4)**	**Inclus au périmètre d'audit (7)**
…					

Infrastructure Réseau et sécurité					
Nature **(5)**	Marque	Nombre	Administré par :	Observations **(6)**	**Inclus au périmètre d'audit (7)**
…					

Postes de travail		
Système d'exploitation	Nombre	**Inclus au périmètre d'audit (7)**
…		

(1): Veuillez respecter **la même nomenclature** utilisée au niveau du rapport d'audit.
(2) : **Mentionner le type d'hébergement (Local, Cloud privé, N-Cloud, G-Cloud)**
(3) : Type du serveur : MV (Machine Virtuelle) ou MP (Machine Physique).
(4) : Rôle/métier : Base de données (MS SQL Server, Oracle, …), messagerie, application métier, Contrôleur de domaine, Proxy, Antivirus, etc.
Veuillez indiquer le(s) nom de (la) solutions métier au niveau de chaque serveur.
(5): Nature: Switch, Routeur, Firewall, IDS/IPS, etc
(6) : **Observations : des informations complémentaires sur les actifs de périmètre (exemples: Firewall, routeur, passerelle, point d'accès) : Homologué ou Non homologué**
(7) : 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.**

Annexe 4 : Planning d'exécution réel de la mission d'audit de la sécurité du SI de *Nom_Organisme_Audité*

Composant		Equipe intervenante		Durée en Hommes/jours pour chaque intervenant	
Phase	Objet de la sous phase		Date(s) de réalisation	Sur Site	Totale
Phase 1	1: ……..	Nom:……			
	2: ……	Nom:……			
	….	Nom:……			
	n: ……	Nom:……			
Phase 2	1: ……..	Nom:……			
	2: ……	Nom:……			
	….	Nom:……			
	n: ……	Nom:……			
Phase n	1: ……..	Nom:……			
	2: ……	Nom:……			
	…	Nom:……			
	n: ……	Nom:……			
Durée Totale de la mission (en Homme/jour)					

Annexe 5 : Evaluation de l'application du dernier plan d'action

Projet	Action	Criticité	Chargé de l'action	Charge (H/J)	Taux de réalisation	Evaluation (1)
Projet 1 : …	Action 1.1 : ……					
	Action 1.2 : ……					
	Action 1.3 : ……					
	...					
Projet 2 : …	Action 2.1 : ……					
	Action 2.2 : ……					
	Action 2.3 : ……					
	...					
….						

(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.

Annexe 6 : Etat de maturité de la sécurité du SI de *Nom_Organisme_Audité*

Domaine	Critère d'évaluation	Valeur attribuée	Commentaires
5. Mesures de sécurité organisationnelles	**5.1 Politiques de sécurité de l'information**		
	5.2 Fonctions et responsabilités liées à la sécurité de l'information		
	Critère 3		
	….		
6. Mesures liées aux personnes	**6.1 Sélection des candidats**		
	6.2 Termes et conditions du contrat de travail		
	Critère 3		
	….		
7. Mesures de sécurité physique	**7.1 Périmètres de sécurité physique**		
	7.2 Les entrées physiques		
	Critère 3		
	….		
8. Mesures de sécurité technologiques	**8.1 Terminaux finaux des utilisateurs**		
	8.2 Droits d'accès privilégiés		
	Critère 3		
	…		

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 reproductibles
3 - Processus définis : Standardisation des pratiques
4 - Processus contrôlés : des mesures quantitatives
5 - Processus continuellement optimisés

Annexe 7 : 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	Absence/Totale/Partielle		

	utilisateurs sensibles			
	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		

Annexe 8 : Liste des vulnérabilités très critiques 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

Annexe 9 : Plan d'action proposé

Projet	Action	Priorité	Responsable de l'action	Charge (H/J)	Planification
Projet 1 : ……	Action 1.1 : ……..				
	Action 1.2 : ……..				
	Action 1.3 : ……..				
	…				
Projet 2 : ……	Action 2.1 : ……..				
	Action 2.2 : ……..				
	Action 2.3 : ……..				
Projet n : ……	Action 2.1 : ……..				
	Action 2.2 : ……..				
	Action 2.3 : ……..				