الوكالة الوطنيّة للسّلامة المعلوماتيّة
Agence Nationale de la Sécurité Informatique

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

(En application à la loi n°5 de 2004)

Évolutions du document

Version	Date	Nature des modifications	Auteur
1.0	19/12/14	Version initiale	ANSI
1.1	03/06/15	MAJ suite à la MAJ du référentiel (Annexe A)	ANSI
1.2	03/05/17	Mise à jour des domaines de l'audit	ANSI

Critère de diffusion

Public	Interne	Diffusion restreinte	Hautement Confidentiel

Avant-propos

L'audit de la sécurité des systèmes d'information en Tunisie est stipulé par la loi n° 5 de 2004 et organisé par les décrets applicatifs 2004-1249 et 2004-1250. Les décrets cités identifient les organismes soumis à l'obligation de l'audit, les experts auditeurs habilités à mener des missions d'audit, la démarche de certification de ces experts auditeurs, ainsi que les étapes clés de la mission d'audit et les livrables à fournir à l'organisme audité à la fin de la mission. Cependant, les contrôles de sécurité à vérifier n'ont pas été identifiés au niveau de ces décrets.

Ainsi, l'ANSI estime qu'il est nécessaire de fournir un modèle de rapport d'audit qui permettra aux experts auditeurs de présenter les résultats d'audit en adéquation avec les exigences du décret 2004-1250, aux organismes audités de disposer de garanties sur la qualité des résultats des audits effectués et aux services de suivi de l'audit au sein de l'ANSI de mener efficacement l'étude et l'évaluation des rapports d'audit.

<Nom du Bureau d'audit>

<Insérer le logo du Bureau d'audit ici>

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

De *<Nom_organisme_audité>*

<Insérer le logo de l'organisme audité 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 des dites 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_Bureau_Audit*)				
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 à la loi n°5 de 2004 et au décret 2004-1250)
- 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 ISO27001
- Indiquer le(s) standard(s) de référence par rapport auquel est réalisée la présente mission d'audit
- Indiquer les limites 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)
- 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

6 Champ d'audit

6.1 Périmètre géographique

- Présenter la liste des structures à auditer :

	Structure	Lieu d'implantation
1		
2		
3		
4		
5		
…		

- 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 1).
- 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 la norme ISO/IEC 27002 :2013
- ✓ La maturité des mesures et contrôles de sécurité mis en place doit être établie en rapport avec les quatorze (14) domaines de ladite norme

- 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_Bureau_Audit* :

Nom Prénom	Qualité/Champs d'intervention	Qualification

….	Chef de projet	Ingénieur, Expert Auditeur certifié ….
	Chef d'équipe	…
	Membre, chargé de …	
	…	

- 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 2)

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 3)

- 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 4)

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)	Appréciation (Valeur attribuée)	Description des vérifications effectuées (tests, conditions de test, etc)
A.5	**Critère 1**	**Bonnes pratiques identifiées**		
		Bonne pratique 1		
		Bonne pratique 2		
		….		
		Vulnérabilités enregistrées		
		Vulnérabilité 1 - Référence de la vulnérabilité 1		
		….		
	Critère 2			
	Critère 3			
	….			
A.6	**Critère 1**			
	…			
…				
A.18	**Critère 1**			
	…			

Pour chaque vulnérabilité non acceptable enregistrée :

Référence de la vulnérabilité:
Description :
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 3 niveaux :
  - Aspects organisationnels de la sécurité des systèmes d'information
  - 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

- ✓ Les critères d'audit doivent être vérifiés sur toutes les composantes du périmètre de l'audit, toute exclusion du périmètre 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:
    - o présenter clairement les critères de choix probants de l'échantillonnage;
    - o décrire explicitement l'échantillon (l'échantillon doit être représentatif);
    - o 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).

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 :

- o L'impact/conséquences d'exploitation des vulnérabilités associées
- o La complexité d'exploitation des vulnérabilités associées
- o La probabilité d'occurrence des menaces associées
- o 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 5)

Annexe 1 : Description du SI de *Nom_Organisme_Audité*

Applications					
Nom	Description	Environnement de développement	Développée par /Année	Nombre d'utilisateurs	Incluse au périmètre d'audit (4)
...					

Serveurs					
Nom	Adresse IP	Système d'exploitation	Fonctionnalités (1)	Description	Inclus au périmètre d'audit (4)
…					

Infrastructure Réseau et sécurité					
Nature	Adresse IP	Marque	Nombre	Observations (3)	Inclus au périmètre d'audit (4)
…					

Postes de travail		
Système d'exploitation	Nombre	Inclus au périmètre d'audit (4)
…		

(1) : Fonctionnalités : 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
(2) : Nature : Switch, Routeur, Firewall, IDS/IPS, etc
(3) Observations : des informations complémentaires sur l'équipement par exemple niveau du switch
(4) : Oui/Non. Présenter les raisons de l'exclusion le cas échéant.

Annexe 2 : 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 3 : 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 4 : Etat de maturité de la sécurité du SI de *Nom_Organisme_Audité*

Domaine	Critère d'évaluation	Valeur attribuée	Commentaires
A.5 Politiques de sécurité de l'information			
A.6 Organisation de la sécurité de l'information			
A.7 Sécurité des ressources humaines			
A.8 Gestion des actifs			
A.9 Contrôle d'accès			
A.10 Cryptographie			
A.11 Sécurité physique et environnementale			
A.12 Sécurité liée à l'exploitation			
A.13 Sécurité des communications			
A.14 Acquisition, développement et maintenance des systèmes d'information			
A.15 Relations avec les fournisseurs			
A.16 Gestion des incidents liés à la sécurité de l'information			
A.17 Aspects de la sécurité de l'information dans la gestion de la continuité de l'activité			
A.18 Conformité			

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

Annexe 5 : 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 : ……..				