
ROYAUME DU MAROC
ADMINISTRATION DE LA DÉFENSE NATIONALE
DIRECTION GÉNÉRALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION



GUIDE D'AUDIT

DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

INFORMATIONS

AVERTISSEMENT

Destiné à vous assister dans l'adoption d'une démarche cohérente et homogène pour la mise en conformité de la sécurité de vos systèmes d'information avec les règles de sécurité édictées par la Directive Nationale de la Sécurité des Systèmes d'information (DNSSI), ce guide élaboré par la DGSSI traite la démarche à mener afin de réaliser un audit de la sécurité des systèmes d'information. Il est destiné à évoluer avec les usages, mais aussi avec vos contributions et retours d'expérience. Les recommandations citées dans ce guide sont livrées en l'état et adaptées aux menaces au jour de leur publication. Au regard de la diversité des systèmes d'information, la DGSSI ne peut garantir que ces informations puissent être reprises sans adaptation sur les systèmes d'information cibles. Dans tous les cas, la pertinence de l'implémentation des éléments proposés par la DGSSI doit être soumise, au préalable, à la validation du Responsable de la Sécurité des Systèmes d'Information (RSSI) et de l'administrateur du système concerné.

ÉVOLUTION DU DOCUMENT :

Version	Date	Nature des modifications
1.0	01/10/2015	Version initiale

PUBLIC CONCERNÉ PAR CE DOCUMENT :

Direction SI
RSSI
Administrateur systèmes et réseaux
Maîtrise d'ouvrage

POUR TOUTE REMARQUE :

Contact	Email
DGSSI	contact@dgssi.gov.ma

Table des matières

TERMINOLOGIE	3
1 INTRODUCTION	4
2 AUDIT DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION	5
2.1 Concepts généraux relatifs aux audits de Sécurité SI	5
2.1.1 Objectifs des audits de sécurité SI	5
2.1.2 Classification des audits	6
2.1.3 Référentiels relatifs à la sécurité des Systèmes d'Information	6
2.2 Les domaines d'audit de la sécurité SI	8
2.2.1 Audit Organisationnel et Physique	8
2.2.2 Audit Technique de sécurité	10
2.3 Démarche et bonnes pratiques de l'audit	12
2.3.1 Phase de déclenchement et de préparation de l'audit	12
2.3.2 Phase d'exécution de l'audit et analyse des constats	14
2.3.3 Clôture de l'audit	15
3 EXIGENCES RELATIVES À LA PRESTATION D'AUDIT	17
3.1 Exigences relatives au prestataire d'audit	17
3.1.1 Exigences générales	17
3.1.2 Exigences relatives à la responsabilité du prestataire d'audit	18
3.1.3 Exigences relatives aux lois et réglementations en vigueur	18
3.1.4 Exigences relatives à la déontologie du prestataire d'audit	18
3.1.5 Exigences relatives à la protection des données de l'organisme audité	19
3.1.6 Exigences relatives à la gestion des ressources humaines du prestataire d'audit	19
3.1.7 Exigences relatives à la sous-traitance	20
3.2 Exigences relatives aux auditeurs	20
3.2.1 Qualités personnelles	21
3.2.2 Compétences	21
3.2.3 Parcours académique et professionnel	22
3.2.4 Déontologie	23
3.2.5 Critères de sélection des prestataires d'audit	23
RÉFÉRENCES	25

Terminologie

- **Commanditaire de l'audit** : Organisme ou personne demandant un audit.
- **Audit** : L'organisme qui est audité.
- **Auditeur** : Personne possédant la compétence nécessaire pour réaliser un audit.
- **Prestataire d'audit** : Organisme réalisant des prestations d'audits.
- **Convention d'audit** : Accord écrit entre un commanditaire et un prestataire d'audit pour la réalisation d'un audit.
- **Plan d'assurance qualité** : L'engagement du prestataire quant à la politique d'assurance qualité applicable aux prestations.
- **Note de cadrage** : Document de synthèse issu de la réunion du commanditaire d'audit, l'organisme audité et le prestataire d'audit.
- **Périmètre d'audit** : Environnement physique, logique et organisationnel dans lequel se trouve le système d'information sur lequel l'audit est effectué.
- **Critères d'audit** : Ensemble de politiques, procédures ou exigences déterminées.
- **Preuves d'audit** : Enregistrements, énoncés de faits ou autres informations, qui se rapportent aux critères d'audit.
- **Constats d'audit** : Résultats de l'évaluation des preuves d'audit recueillies, par rapport aux critères d'audit.
- **Plan de charge** : Le plan de charge couvre les objectifs de l'audit, le périmètre, les critères d'audit, la démarche à suivre pour l'exécution de la mission, les activités à effectuer, ainsi que le planning prévisionnel de l'audit.
- **Conclusions d'audit** : Résultat d'un audit fourni par l'équipe d'audit après avoir pris en considération les objectifs de l'audit et tous les constats d'audit.

Les attaques informatiques se font de plus en plus nombreuses contre les systèmes d'information des organes sensibles de notre pays, divulguant ainsi des informations confidentielles et mettant en danger la sécurité nationale. Par ailleurs, l'altération du système d'information (SI) n'est pas toujours le fait de malveillances. Elle peut être également due aux pannes, accidents ou erreurs humaines qui affectent la disponibilité, la confidentialité, l'intégrité ou la traçabilité de l'information et entrave le bon fonctionnement des systèmes d'information. Une évaluation systématique de la sécurité du système d'information s'impose donc afin de permettre le développement et la mise en œuvre de pratiques de sécurité efficaces.

L'audit de sécurité des systèmes d'information est une évaluation permettant de s'assurer de l'efficacité des mesures de sécurité mises en place, d'acter l'adoption des solutions de protection adéquates et de réduire les risques pouvant nuire à la sécurité du SI. Il devient donc impératif que les administrations et les organismes publics mettent à jour leur système d'information en procédant à la réalisation d'audits de sécurité SI.

Dans ce contexte, la Directive Nationale de la Sécurité des Systèmes d'Information (DNSSI), élaborée par la Direction Générale de la Sécurité des Systèmes d'Information (DGSSI) et approuvée par le Comité Stratégique de la Sécurité des Systèmes d'Information (CSSSI), décrit les mesures de sécurité qui doivent être appliquées par les administrations et les organismes publics. Ces derniers seront amenés à réaliser un audit de sécurité de leur système d'information afin d'évaluer son niveau de maturité par rapport aux règles de la DNSSI et d'identifier les projets à mettre en œuvre pour se conformer à cette dernière.

L'objectif de ce document est double ; D'une part, permettre aux organismes de l'Etat de bien définir leurs besoins en termes d'audit afin de rédiger d'éventuels appels d'offres. D'autres part, lister les exigences relatives aux prestataires d'audit permettant de garantir à l'organisme audité la compétence des auditeurs et la pertinence de leurs recommandations, ainsi que la qualité des audits effectués.

2.1 Concepts généraux relatifs aux audits de Sécurité SI

L'audit selon la norme ISO 19011 :2011 est « un processus systématique, indépendant et documenté en vue d'obtenir des preuves d'audit et de les évaluer de manière objective pour déterminer dans quelle mesure les critères d'audit sont satisfaits ». En ce qui concerne le domaine de la sécurité des systèmes d'information (SSI), l'audit permet de mettre en évidence les faiblesses et les vulnérabilités organisationnelles et/ou techniques du système d'information et de déterminer des axes d'amélioration visant à augmenter le niveau de sécurité.

Pour mener un programme d'audit, il convient de bien définir les besoins, le périmètre, ainsi que l'implication des différents acteurs concernés.

2.1.1 Objectifs des audits de sécurité SI

Un audit de sécurité SI peut être réalisé pour répondre à des besoins différents, notamment :

- Evaluer le niveau de maturité du SI en terme de sécurité suite à la demande du commanditaire d'audit ;
- Vérifier l'efficacité de la politique de sécurité du SI mise en place ;
- Tester l'installation d'un nouvel élément dans le SI ;
- Analyser et réagir suite à une attaque ;
- Tester la résistance du SI par la simulation des attaques dans des conditions réelles ;
- Se certifier (par exemple ISO 27001) ;
- etc.

Une mission d'audit de sécurité SI ne permet que de trouver les vulnérabilités liées au SI et de proposer des actions correctives à travers un ensemble de vérifications et de contrôles. A l'issue de la mission, le prestataire d'audit livre un rapport détaillé pour mettre en évidence les écarts et les non-conformités trouvés. Un plan d'action contenant les mesures à mettre en œuvre par priorité est établi, partagé et validé avec l'organisme audité.

Il faut distinguer entre l'audit et l'analyse de risques. Cette dernière permet d'apprécier les risques identifiés liés à la sécurité afin de les traiter (accepter,

transférer, éviter, réduire, etc.). Le risque est un concept dynamique qui dépend de la menace, de la vulnérabilité, de l'impact (sur la disponibilité, confidentialité, intégrité) et de la probabilité d'occurrence.

2.1.2 Classification des audits

Les audits peuvent être classifiés en trois catégories :

- **Les audits internes** (appelés aussi audits de 1ère partie) sont réalisés pour les organismes souhaitant que leur système d'information soit examiné par rapport à des exigences de sécurité de système d'information. Ces audits sont établis par des auditeurs internes ou externes à l'organisme.
- **Les audits externes** (appelés aussi audits de 2ème partie) sont commandités par des entités ayant un intérêt à l'égard de l'organisme audité, dans le but d'évaluer le niveau de sécurité du système d'information de ce dernier. Ces audits sont établis par des organismes d'audit externes.
- **Les audits de certification** (appelés aussi audits de tierce partie) sont réalisés pour les organismes qui souhaitent faire reconnaître que la sécurité de leur système d'information est conforme aux exigences comme celles de l'ISO/CEI 27001. Ces audits sont établis par des organismes externes généralement accrédités.

2.1.3 Référentiels relatifs à la sécurité des Systèmes d'Information

Les référentiels de la sécurité des systèmes d'information constituent l'ensemble des normes, des méthodes et de bonnes pratiques permettant de fournir un moyen d'assurance d'une démarche sécuritaire cohérente. Parmi ces référentiels, on peut citer :

- **La Directive Nationale de la Sécurité des Systèmes d'Information (DNSSI) :** élaborée par la DGSSI, elle décrit les mesures de sécurité organisationnelles et techniques qui doivent être appliquées par les administrations et les organismes publics ainsi que les infrastructures d'importance vitale. La DGSSI s'est inspirée de la norme marocaine NM ISO/CEI 27002 :2009 et s'est basée sur les résultats de l'enquête menée au mois de juillet 2013 auprès d'un échantillon représentatif d'administrations et d'organismes publics et d'opérateurs d'importance vitale. Cette directive, diffusée par une circulaire du Chef de Gouvernement le 10 Mars 2014, constitue aujourd'hui la première référence nationale qui fixe les objectifs et les règles de la SSI.
- **La suite ISO/CEI 27000 :** La suite ISO/CEI 27000 (connue sous le nom de Famille des standards SMSI ou ISO27k) comprend les normes de sécurité de l'information publiées par l'organisation internationale de normalisation (ISO) et la Commission Electrotechnique Internationale (CEI).
- **L'ISO/IEC 27001 :** Intitulée « Systèmes de gestion de sécurité de l'information – Exigences », elle a été publiée en octobre 2005 et révisée en 2013. Cette

norme spécifie les exigences relatives à l'établissement, à la mise en œuvre, à la mise à jour et à l'amélioration continue d'un système de management de la sécurité de l'information (SMSI) au sein d'une organisation.

- **L'ISO/IEC 27002** : Intitulée « Code de bonnes pratiques pour la gestion de la sécurité de l'information », elle a été publiée en 2005 et révisée en 2013. L'ISO/CEI 27002 est un ensemble de mesures dites de bonnes pratiques, destinées à être utilisées par tous les responsables de la mise en place ou du maintien d'un SMSI.
- **L'ISO/IEC 27005** : Publiée en 2008 et révisée en 2011, L'ISO/CEI 27005 est une norme de gestion des risques de la Sécurité des Systèmes d'Information.
- **L'ISO 27006** : Cette norme a été remise à jour en 2011. Elle a pour objectif de fournir les exigences pour les organismes procédant à l'audit et à la certification des SMSI.
- **CobiT (Control Objectives for Information and Related Technology)** : Le référentiel CobiT a été développé par l'ISACA. Il fournit des indicateurs, des processus et des bonnes pratiques pour aider les gestionnaires, les auditeurs et les utilisateurs à aligner le système d'information sur les besoins et la stratégie de l'organisme et à élaborer la gouvernance et le contrôle.
- **ITIL (Information Technology Infrastructure Library)** : La bibliothèque ITIL est un ensemble d'ouvrages recensant les bonnes pratiques du management du système d'information. C'est un référentiel très large qui aborde des sujets différents tel que l'organisation, l'amélioration et l'augmentation de la qualité de service.
- **EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité)** : Créée par l'Agence française de la Sécurité des Systèmes d'Information (ANSSI), cette méthode permet d'apprécier et de traiter les risques relatifs à la sécurité des systèmes d'information conformément à la norme ISO : IEC 27005. Elle permet également de construire une politique de sécurité en fonction d'une analyse des risques qui repose sur le contexte de l'organisme et des vulnérabilités liées à son SI.
- **MEHARI (Méthode Harmonisée d'Analyse de Risques)** : Développée et proposée par Clusif (Club de la Sécurité de l'Information Français), est une méthode d'évaluation et de management des risques liés aux systèmes d'information. Elle est conforme aux exigences de la norme ISO/IEC 27005.
- **OCTAVE (Operationally Critical Threat, Asset and Vulnerability Evaluation)** : Produite par l'Institut d'ingénierie logiciel de l'université Carnegie Mellon de Pittsburgh aux USA en 1999. C'est une méthode qui permet d'identifier et d'évaluer les risques de sécurité associés aux systèmes d'information.

2.2 Les domaines d'audit de la sécurité SI

L'audit de sécurité SI représente une activité complexe qui couvre l'ensemble des composants du système d'information. Il consiste à évaluer le niveau de sécurité et à proposer les moyens de correction adaptés. Cette évaluation concerne les domaines suivants :

2.2.1 Audit Organisationnel et Physique

L'audit organisationnel et physique permet de faire un état des lieux complet de la sécurité du SI et d'en identifier les dysfonctionnements et les risques potentiels. Il permet ainsi de couvrir l'ensemble du SI de l'organisme et de détecter les carences liées aux différents processus de gestion et d'organisation de la sécurité. Durant cet audit les éléments suivants peuvent être abordés :

- **Politiques de sécurité de l'information :**
Cette section met l'accent sur la nécessité de la mise en place, et révision régulière d'une politique de sécurité de l'information.
- **Organisation de la sécurité de l'information :**
Cette section définit un cadre de gestion et d'approbation de la politique de sécurité, et traite les aspects contractuels liés à la sécurisation des accès au système d'information par les tiers.
- **Sécurité des ressources humaines :**
Cette section donne des recommandations pour réduire le risque d'erreur ou de fraude favorisant la formation et la sensibilisation des utilisateurs sur les menaces affectant la sécurité de l'information, ainsi que les comportements à adopter pour protéger l'information.
- **Gestion des actifs :**
Cette section décrit la nécessité d'inventorier et de classifier les actifs informationnels de l'organisme, dans le but d'identifier les besoins et le niveau de protection adapté à ces actifs.
- **Contrôle d'accès :**
Cette section définit les mesures pour gérer et contrôler les accès à l'information afin d'assurer la protection des systèmes en réseau. Elle couvre également la sécurité de l'information lors de l'utilisation d'appareils mobiles.
- **Cryptographie :**
Cette section traite les mesures visant à protéger la confidentialité et l'intégrité de l'information par des moyens cryptographiques.
- **Sécurité physique et environnementale :**
Cette section définit les mesures pour protéger les lieux et les locaux de l'organisme contre les accès non autorisés, et pour minimiser les dommages causés par les menaces environnementales. Elle traite également la sécurité des matériels afin de réduire les menaces liés aux risques de vol, et de fuites d'information.

- **Sécurité liée à l'exploitation :**
Cette section définit les mesures permettant d'assurer une exploitation correcte et sécurisée des moyens de traitement de l'information (protection contre les logiciels malveillants, maîtrise des logiciels en exploitation, et gestion des vulnérabilités techniques).
- **Sécurité des communications :**
Cette section définit les mesures d'une part, pour assurer la protection des informations sur les réseaux et la protection de l'infrastructure sur laquelle ils s'appuient, et d'autre part, pour maintenir la sécurité des informations et des logiciels échangés au sein de l'organisme et avec une entité extérieure.
- **Acquisition, développement et maintenance des systèmes d'information :**
Cette section traite les spécifications requises pour assurer la sécurité des systèmes d'information tout au long de leur cycle de vie.
- **Relations avec les fournisseurs :**
Cette section définit les mesures permettant de gérer les prestations de service assurées par des tiers.
- **Gestion des incidents liés à la sécurité de l'information :**
Cette section met l'accent sur la nécessité de la mise en place des procédures pour la détection et le traitement des incidents de sécurité.
- **Aspects de la sécurité de l'information dans la gestion de la continuité de l'activité :**
Cette section décrit les mesures pour mettre en œuvre un plan de continuité de l'activité qui vise à minimiser les impacts causés par les catastrophes naturelles et les pannes matérielles sur l'organisme, afin d'assurer une reprise dans les meilleurs délais.
- **Conformité :**
Cette section traite le respect des réglementations et des obligations légales, ainsi que la conformité des procédures et des mesures de sécurité mises en place avec la politique et les normes de sécurité.

L'audit organisationnel et physique permet de procéder à la vérification de la conformité et de la pertinence des mesures déployées par rapport à la politique de sécurité de l'organisme, à un référentiel, à une norme ou à des procédures. D'une manière générale, il convient de définir les référentiels de sécurité à respecter lors de l'audit en tenant compte des exigences et des attentes des responsables de l'organisme audité. Cependant, les administrations, les organismes publics et les infrastructures d'importance vitale doivent s'assurer à minima de la conformité de leur SI avec la DNSSI.

Pour mener à bien cette phase, une analyse de risques doit être menée. Il convient de choisir la méthode la plus adaptée au contexte selon les besoins de l'organisme ou suivre une démarche personnalisée et simplifiée.

L'audit organisationnel et physique est considéré comme étant un audit de premier niveau, il ne s'agit pas d'une analyse technique profonde, mais plutôt d'un exercice de questions/réponses. En effet, cette phase repose sur l'utilisation de questionnaires adaptés au contexte de l'organisme audité, des interviews, ainsi que sur l'analyse des ressources et des documents fournis.

2.2.2 Audit Technique de sécurité

L'audit technique de sécurité est une évaluation permettant d'analyser en profondeur le système d'information (systèmes, applications, composants et équipements actifs de l'infrastructure réseau, réseaux d'accès interne, réseaux d'interconnexion, etc.) pour identifier les vulnérabilités techniques éventuelles.



Il est recommandé de faire précéder l'audit technique par un audit organisationnel afin d'identifier les points critiques du système d'information nécessitant une étude exhaustive.

Ci-après les activités qui peuvent être réalisées lors d'un audit de sécurité technique :

A. Audit des vulnérabilités infrastructure et système

L'objectif de l'audit des vulnérabilités infrastructure et système est de réaliser les tests permettant de ressortir les faiblesses et les failles techniques sur les systèmes, les applications et les équipements réseaux. Il permet ainsi de proposer un plan de remédiation avec des actions correctives. L'audit des vulnérabilités se déroule en deux phases :

- Phase de découverte des vulnérabilités : cette phase consiste à effectuer des tests automatisés à l'aide d'outils spécifiques qui s'appuient en général sur une base de failles connues (scanners des vulnérabilités systèmes, scanners des vulnérabilités applicatives et web, etc.) pour détecter les éventuelles vulnérabilités du système d'information.
- Phase d'analyse des vulnérabilités : cette phase consiste à analyser les vulnérabilités identifiées lors de la première phase afin de proposer les actions de remédiation en cohérence avec les pratiques et les exigences de sécurité adoptées au sein de l'organisme audité.

B. Audit d'architecture réseau

Cette activité d'audit a pour vocation d'analyser l'architecture réseau existante afin de déterminer les éléments pouvant nuire à la sécurité. Elle consiste à étudier la topologie du réseau, ainsi que les hôtes et les équipements d'interconnexion. L'audit d'architecture repose sur l'analyse de la documentation du réseau et la réalisation des sondages en utilisant des outils de traçage et de découverte. L'objectif étant de s'assurer du respect des bonnes pratiques et des recommandations en matière de sécurité quant à l'emplacement des actifs réseaux et sécurité

(pare-feu, pare-feu applicatif, sondes, proxy, relais anti-virus, relais messagerie, etc.), le cloisonnement, l'échange des flux, les réseaux sans fil, etc.



- L'audit d'architecture peut être étendu aux interconnexions avec des réseaux tiers, et notamment Internet.

- L'audit d'architecture ne peut pas être dissocié de l'audit de configuration car il permet de traiter les points névralgiques de l'architecture du système d'information.

C. Audit de configuration

L'audit de configuration repose sur une évaluation technique de la configuration des composants du système d'information afin de s'assurer que les mesures de sécurité déployées respectent les bonnes pratiques en matière de sécurité. Les audits de configuration peuvent s'effectuer sur tout type d'élément informatique (équipements réseaux, systèmes d'exploitation, logiciels, applications, bases de données, etc.) en utilisant des outils appropriés d'analyse de configuration.

D. Tests d'intrusion

Le concept des tests d'intrusion repose sur l'exploitation des failles identifiées afin de mesurer l'impact réel sur la sécurité du système d'information de l'organisme audité. Ces tests simulent des scénarios d'attaques préparés à l'avance dans des conditions réelles. L'objectif est de tester la résistance du système d'information aux attaques informatiques provenant de l'intérieur ou de l'extérieur du réseau de l'organisme (ex : réseau internet).

- *Les tests d'intrusion externes* : permettent d'évaluer la capacité d'un attaquant externe à pénétrer le réseau interne de l'organisme audité ;
- *Les tests d'intrusion internes* : permettent d'évaluer l'impact d'un acte malveillant mené de l'intérieur du réseau de l'organisme audité.


Généralement, ces tests s'effectuent selon les étapes suivantes :

- Reconnaissance du périmètre à auditer ;
- Recherche des vulnérabilités ;
- Mise en œuvre des attaques (exploits) ;
- Mesure de l'impact ;
- Proposition de recommandations et correctifs.

Les tests d'intrusion peuvent être conduits selon plusieurs approches :


- *Approche en boîte noire* : Le testeur ne dispose d'aucune connaissance préalable de l'environnement avant l'attaque ;
- *Approche en boîte grise* : le testeur dispose de connaissances partielles de l'environnement à auditer ;
- *Approche en boîte blanche* : le testeur dispose de toutes les informations qui lui permettent d'examiner l'architecture complète et non pas juste la surface

d'attaque directement visible.

 Afin d'éviter des conséquences liées aux éventuels dysfonctionnements sur un environnement de production, il est préférable de réaliser les tests d'intrusion qui peuvent causer l'arrêt du système ou l'altération des données critiques sur un environnement de test ou pré-production.

E. Audit applicatif

L'audit applicatif permet d'évaluer le niveau de sécurité des applications déployées au niveau du système d'information de l'organisme audité. Cet audit peut se faire selon plusieurs approches dont l'audit du code applicatif qui consiste à examiner les vulnérabilités liées au code source d'une application. Cette activité exige l'implication d'un auditeur expert du langage de programmation utilisé dans le développement de l'application.

 D'une manière générale, le périmètre de l'audit de sécurité d'un système d'information peut ne pas intégrer toutes les activités citées ci-dessus.

2.3 Démarche et bonnes pratiques de l'audit

Cette section présente un ensemble de recommandations relatives au déroulement de la mission d'audit en se basant sur la norme ISO 19011 :2011. Cette dernière fournit des lignes directrices sur l'audit de systèmes de management (comprenant les principes de l'audit, le management d'un programme d'audit et la réalisation d'audits de systèmes de management).

Une mission d'audit se déroule généralement selon les phases suivantes :

2.3.1 Phase de déclenchement et de préparation de l'audit

Une mission d'audit Sécurité SI débute, sur demande du commanditaire au profit de l'organisme audité, par l'établissement d'une lettre de mission rédigée et signée par le demandeur. Dans certains cas l'organisme audité peut être lui-même le commanditaire d'audit.

Le prestataire d'audit doit nommer un responsable d'audit qui sera en mesure de communiquer avec l'organisme audité. Le responsable d'audit doit avoir un premier contact avec l'organisme audité qui peut être formel ou informel afin de définir les objectifs de l'audit, le périmètre et les critères d'audit, discuter les circuits de communication et les ressources.

Une équipe d'audit doit être formée en fonction du périmètre de l'audit et en prenant en considération les compétences nécessaires pour atteindre les objectifs

de l'audit (voir chapitre 3, section 1.6).

L'organisme audité doit fournir au prestataire d'audit la documentation nécessaire pour appréhender le périmètre de l'audit.

Une convention d'audit doit être établie entre le commanditaire d'audit et le prestataire d'audit au début de la mission et doit être validée et signée par les deux parties prenantes. Cette convention doit :

- Contenir les informations relatives à chaque partie prenante dans la mission d'audit : Noms, Responsabilités et Rôles ;
- Présenter les objectifs de l'audit ;
- Arrêter le périmètre de l'audit et ses modalités (livrables, objectifs, jalons, portée, durée etc.) ;
- Arrêter les critères d'audit (politique de sécurité, normes, référentiels, etc.) ;
- Fixer les dates et les lieux de la mission d'audit ;
- Préciser l'engagement de l'organisme audité à présenter les documents susceptibles d'aider l'équipe de l'audit à accomplir sa mission ;
- Déterminer des moyens de communication (moyens de contacts, interlocuteurs, etc.) ;
- Déterminer les moyens et la logistique nécessaires à l'exécution et à la réussite de l'audit (dispositions logistiques, ressources matérielles, ressources humaines, etc.) ;
- Inclure des clauses de confidentialité nécessaires pour la conduite du projet d'audit.

À ce niveau le prestataire d'audit entame la phase de préparation de l'audit. Il doit établir le plan de charge d'audit qui couvre les objectifs de l'audit, le périmètre, les critères d'audit, la démarche à suivre pour l'exécution de la mission, les activités à effectuer, le planning prévisionnel d'exécution des travaux, etc.

Les membres de l'équipe d'audit doivent préparer la stratégie de tests selon le point de contrôle à auditer, à savoir :

- Revue documentaire ;
- Questionnaires/checklists : Basés sur les critères prédéfinis en plus des checklists des contrôles techniques ;
- Entretiens : Planifier des entretiens qui seront menés avec les interlocuteurs de l'organisme audité ;
- Immersions sur site : visite sur site afin d'auditer le comportement professionnel face aux situations de quotidien ;
- Scénarios de tests techniques.

2.3.2 Phase d'exécution de l'audit et analyse des constats

- Réunion d'ouverture :

L'exécution de l'audit commence par une réunion d'ouverture tenue entre le commanditaire d'audit, l'organisme audité et le prestataire. Son but est de valider le plan de charge d'audit préétabli, exposer le planning prévisionnel de l'audit, présenter les activités d'audit qui seront menées, confirmer les circuits de communication, et fournir des clarifications sur les éventuelles ambiguïtés existantes. Suite à cette réunion, un compte rendu doit être rédigé.

Les livrables de cette phase :

- Plan d'assurance qualité ;
- Note de cadrage ;
- Planning prévisionnel.

- Exécution de l'audit :

Cette phase consiste à exécuter les différents tests planifiés lors de la phase de préparation, notamment :

- L'équipe d'audit effectue des entretiens avec les interlocuteurs de l'organisme audité. Des immersions (des observations d'activités) sont recommandées si les informations recueillies lors des entretiens sont insuffisantes. Si nécessaire l'auditeur peut demander des preuves appuyant les informations fournies par l'audit.
- L'auditeur procède à une analyse d'écart entre les preuves fournies et les critères d'audit afin de générer ses constats. Ces constats sont soit une conformité soit une non-conformité aux critères d'audit.
- Le responsable d'audit doit immédiatement tenir au courant l'audit de tout élément constituant un risque majeur et lui proposer des solutions urgentes pour y remédier.
- Suite à chaque entretien ou immersion, un compte rendu doit être soumis au commanditaire d'audit et son contenu doit être validé avec l'organisme audité.
- Les constats d'audit doivent être documentés et tracés par le prestataire d'audit.
- Le commanditaire d'audit doit effectuer régulièrement le point avec le prestataire d'audit et l'organisme audité afin de s'informer de l'état d'avancement de l'audit et des différents obstacles rencontrés.



Les modifications appliquées sur le système d'information audité doivent être tracées. En fin de mission d'audit, le système d'information ne doit pas être moins sécurisé que l'état initial.

- Enregistrements de la phase d'exécution :

Les documents résultant de la phase d'exécution doivent être soigneusement archivés. Ces documents se déclinent comme suit :

- Les comptes rendus validés et signés par les interlocuteurs de l'organisme audité ;
- Les fiches d'écart dûment remplies. Une fiche d'écart comporte essentiellement :
 - ◊ Les constats des auditeurs ;
 - ◊ Les recommandations ;
 - ◊ Les engagements et/ou actions proposés par l'organisme audité ;
 - ◊ Les commentaires des auditeurs relatifs au point précédent.
- Une grille d'évaluation des niveaux de maturité par rapport aux objectifs de sécurité initialement définis doit être remplie ;
- Les relevés techniques, à savoir :
 - ◊ Les fichiers contenant les résultats des scans de sécurité ;
 - ◊ Le rapport d'analyse des vulnérabilités ;
 - ◊ Les échantillons du trafic capturé.
- Les résultats des tests techniques d'audit sont composés principalement de :
 - ◊ La liste des vulnérabilités (réseaux, systèmes, applicatives, etc.) ;
 - ◊ La liste des anomalies de configuration des équipements (configuration des firewalls et des équipements réseaux).

Les enregistrements de la phase d'exécution de l'audit doivent être évalués, analysés et consolidés par l'équipe d'audit. Cette consolidation est réalisée à travers les actions suivantes :

- Présentation des constats fiables et pertinents, formulés clairement, de manière synthétique ;
- Validation des conclusions d'audit ;
- Préparation des recommandations ;
- Définition des modalités de suivi d'audit.

2.3.3 Clôture de l'audit

Le prestataire d'audit doit rédiger le rapport d'audit et doit être responsable de son contenu. Une réunion de clôture de l'audit est prévue pour présenter le rapport d'audit à la Direction de l'organisme audité et pour répondre aux éventuelles questions qui peuvent se poser. Il convient que l'audit et le commanditaire d'audit y prennent part. Les constats et les conclusions d'audit présentés doivent être bien compris et acceptés par l'audit.

Le rapport d'audit doit être émis dans les délais prédéterminés. En cas de retard, il est recommandé de communiquer au commanditaire d'audit les raisons du retard et de fixer une date d'émission. Le rapport d'audit doit être diffusé auprès des parties désignées par le commanditaire d'audit. Le rapport d'audit doit

rester confidentiel. La mission d'audit est achevée suite à la réalisation de l'ensemble des actions définies dans le plan de charge d'audit et suite à la diffusion du rapport final d'audit.



Les conclusions d'audit peuvent contenir des actions correctives à exécuter après la fin de l'audit. Dans ce sens, la convention d'audit peut exiger aux auditeurs le suivi de la mise en œuvre des actions élaborées sur la base des recommandations de l'audit. L'état d'avancement de la mise en place des actions correctives est rapporté au commanditaire de l'audit.

Livrables de la phase de clôture :

- Le rapport d'audit de la sécurité qui englobe :
 - ◇ Les résultats des différentes activités réalisées ;
 - ◇ Le plan de recommandations global et les prérequis pour leur mise en œuvre.

Il faut noter que les livrables d'une mission d'audit doivent être discutés et fixés au début de la mission. Ils englobent généralement les documents suivants :

- Une politique de sécurité ;
- Une charte d'utilisation des ressources SI ;
- Une matrice et cartographie des risques SI ;
- Un cahier des charges des solutions retenues ;
- Un manuel des procédures SI (procédure d'inventaire des biens, procédure de gestion des accès physiques, procédure de sauvegarde, etc.) ;
- Etc.

Exigences relatives à la prestation d'audit

Au vu de la criticité des prestations d'audit de la sécurité des systèmes d'information, et afin de s'assurer de la compétence des prestataires qui les réalisent, cette partie liste un ensemble d'exigences à respecter par les prestataires d'audit de sécurité SI, ainsi que par les auditeurs. Elles portent sur les domaines législatifs, organisationnels et techniques.

3.1 Exigences relatives au prestataire d'audit

Le prestataire d'audit doit accompagner l'audité dans sa démarche de sécurisation de son système d'information via une évaluation méthodique de l'efficacité des processus de sécurité déjà en place en vue de leur amélioration. Pour ce faire, le prestataire d'audit aura accès à des informations sensibles liées à la sécurité du système d'information de l'organisme audité. Il est donc important de s'assurer de l'objectivité, la responsabilité, le respect des lois en vigueur, l'intégrité du prestataire et sa capacité à protéger les données de l'organisme audité ainsi que de la bonne gestion de ses ressources.

3.1.1 Exigences générales

Les exigences suivantes portent sur la structure juridique du prestataire d'audit, son expérience et sa démarche d'audit :

- Le prestataire d'audit doit être une personne morale dotée d'une personnalité juridique, il sera tenu responsable de ses activités d'audit ;
- Le prestataire d'audit doit avoir des références connues sur le marché relatives à des prestations d'audit similaires ;
- Le prestataire d'audit doit avoir un contrat de travail avec ses auditeurs ;
- Le prestataire d'audit doit proposer au commanditaire une offre technique et financière faisant ressortir sa capacité à réaliser les activités de l'audit aux moyens de compétences adéquates, et selon une méthodologie et un plan de réalisation déterminés. Cette offre doit comprendre :
 - ◇ Une présentation de la démarche et de la méthodologie proposées pour bien mener la mission et garantir la fiabilité des résultats en mettant en exergue la compréhension du contexte et des objectifs de l'audit, ainsi que les outils proposés pour la réalisation de la prestation ;
 - ◇ Le plan de charge proposé pour la réalisation de l'audit qui doit être en adéquation avec les compétences, les profils et les missions ;
 - ◇ Le planning envisagé.

- Le prestataire doit réaliser les activités d'audit dans le cadre d'une convention d'audit préalablement approuvée par le commanditaire.

3.1.2 Exigences relatives à la responsabilité du prestataire d'audit

La convention d'audit doit traiter des modalités de partage des responsabilités entre le prestataire d'audit et l'organisme audité. Cependant, il est recommandé que le prestataire d'audit garde la responsabilité des actions qu'il effectue, en particulier si l'organisme audité ne dispose pas des compétences nécessaires, dans tous les cas :

- Le prestataire doit évaluer le niveau de risque de ses activités et mettre en place les dispositions appropriées pour les prendre en charge ;
- Le prestataire assume la responsabilité de l'audit notamment concernant les éventuels dommages qui pourraient subvenir au cours de l'audit. Ceci doit être clairement décrit dans la convention d'audit ;
- Les méthodes et outils techniques utilisés dans le cadre de l'audit doivent impérativement être validés entre le commanditaire et le prestataire. Il est de la responsabilité du prestataire d'informer l'audit sur les risques liés à ces outils ;
- Le prestataire d'audit s'assure de la sécurité et la confidentialité de ses interactions avec le commanditaire de l'audit.

3.1.3 Exigences relatives aux lois et réglementations en vigueur

Le prestataire doit respecter la législation en vigueur au Maroc, notamment en ce qui concerne le traitement des données à caractère personnel (la loi 09-08), la propriété intellectuelle et les fraudes informatiques.

3.1.4 Exigences relatives à la déontologie du prestataire d'audit

Pour mener à bien une mission d'audit, le prestataire d'audit doit respecter un ensemble d'exigences et de règles relatives à l'éthique professionnelle, il s'agit notamment des exigences suivantes :

- Le prestataire d'audit doit présenter la preuve et les références suffisantes afin d'étayer les informations qu'il fournit pour appuyer sa candidature, notamment en termes de publicité ;
- Le prestataire d'audit s'engage à mener son activité de façon impartiale et doit prouver qu'aucun conflit d'intérêt ne pourrait fausser le résultat de l'audit ;
- Le prestataire d'audit se doit d'être loyal, de bonne foi et respectueux envers l'organisme audité ainsi que son personnel ;
- Le prestataire d'audit doit disposer d'une charte d'éthique décrivant les principes auxquels ses auditeurs doivent se conformer. Cette charte doit

être signée par l'ensemble des auditeurs intervenant dans la mission d'audit.

3.1.5 Exigences relatives à la protection des données de l'organisme audité

Le prestataire d'audit aura accès à des informations sensibles liées au fonctionnement et à la sécurité du système d'information de l'organisme audité, il est alors tenu de respecter les exigences de confidentialités ci-après :

- Le prestataire doit présenter son engagement de confidentialité à l'organisme audité ;
- Le prestataire d'audit ne doit communiquer aucune information concernant l'organisme audité au public ni à une tierce partie sans le consentement formel de l'organisme audité ;
- Il est de la responsabilité du prestataire de garantir que le circuit de production des documents liés à l'audit est sécurisé (poste de travail, circuit de validation interne, impression des documents, sauvegarde des documents, destruction des documents, etc.) ;
- Le prestataire d'audit doit impérativement avoir une politique de diffusion de documents selon leur niveau de confidentialité. Tous les documents résultant de l'audit doivent avoir une diffusion restreinte aux personnes concernées par l'audit ;
- Le prestataire d'audit doit mettre en place un système sécurisé pour le partage des livrables avec l'organisme audité.

3.1.6 Exigences relatives à la gestion des ressources humaines du prestataire d'audit

Le prestataire d'audit doit constituer l'équipe d'audit en tenant compte des compétences nécessaires pour réussir sa mission. Il doit :

- Mettre à contribution suffisamment d'auditeurs expérimentés pour assurer totalement les activités d'audit pour lesquels il s'est engagé ;
- S'assurer du maintien à jour des compétences de ses auditeurs via un cursus de formation continue et de veille technologique ;
- Vérifier l'authenticité et la pertinence des formations, des qualifications et des références de ses auditeurs ;
- Etablir un processus disciplinaire dissuasif en cas d'enfreinte aux règles de sécurité ou à la charte d'éthique ;
- S'assurer que la palette des compétences de l'équipe désignée pour l'audit répond aux besoins de l'organisme audité. La palette de compétences à couvrir pour un audit de sécurité de système d'information, en fonction du périmètre de l'audit, porte globalement sur les aspects suivants :

- ◇ Réseaux et protocoles de communication (infrastructure réseaux, configuration et sécurisation des principaux équipements réseau du marché, réseaux sans fil, Etc.);
- ◇ Systèmes d'exploitation (UNIX/LINUX, WINDOWS, solutions de virtualisation);
- ◇ Bases de données et couches applicatives (guides et principes de développement sécurisé, langages de programmation, systèmes de gestion de bases de données, mécanismes cryptographiques Etc.);
- ◇ Equipements et logiciels de sécurité (pare-feu, antivirus, logiciels de sauvegarde, Etc.);
- ◇ Outils utilisés dans le cadre des tests d'intrusions;
- ◇ Reverse engineering;
- ◇ Normes relatives à la sécurité SI (famille ISO 27000);
- ◇ Les pratiques et normes régissant le métier de l'audit (ISO 19011);
- ◇ Gestion des risque liés à la SSI.

3.1.7 Exigences relatives à la sous-traitance

- Le prestataire peut sous-traiter une partie de l'audit à certaines conditions :
 - ◇ Le prestataire doit se conformer aux dispositions de l'article 158 du décret n 2.12-349 du 08 Joumada I 1434 (20 mars 2013) relatif à la sous-traitance dans le cadre des marchés publics;
 - ◇ Une convention ou un cadre contractuel doit être établi entre le prestataire et le sous-traitant;
 - ◇ La sous-traitance doit être connue et acceptée par l'audité;
 - ◇ Le sous-traitant doit être signataire de la charte d'éthique et de l'engagement de confidentialité du prestataire.
- Le sous-traitant est soumis aux mêmes exigences susmentionnées, au même titre que le prestataire.

3.2 Exigences relatives aux auditeurs

Afin de réussir sa mission d'audit, le prestataire doit mettre à contribution des auditeurs compétents dans les domaines de la sécurité des systèmes d'information. Ces auditeurs sont la clé du succès de cette mission, ils doivent répondre à certaines exigences et avoir les qualités et les compétences nécessaires pour réaliser l'audit. Les auditeurs doivent maîtriser la méthodologie de l'audit, les normes et les techniques relatives à la sécurité des systèmes d'information.

3.2.1 Qualités personnelles

- L'auditeur doit avoir les qualités personnelles décrites au chapitre 7.2 de la norme 19011, à savoir :
 - ◇ Intégrité (justice, honnêteté, sincérité, discrétion) ;
 - ◇ Ouverture d'esprit (capable d'envisager des idées ou points de vue alternatifs) ;
 - ◇ Diplomatie (ayant le tact nécessaire pour aborder et discuter des sujets sensibles pour l'organisme audité) ;
 - ◇ Sens de l'observation (en observation active et permanente de l'environnement audité) ;
 - ◇ Perspicacité (capable de comprendre facilement les différentes situations et tirer les bonnes conclusions) ;
 - ◇ Polyvalence (capable de s'adapter aux différents environnements et situations) ;
 - ◇ Ténacité (pour atteindre les objectifs de l'audit) ;
 - ◇ Sens de l'initiative et de prise de décisions ;
 - ◇ Autonomie.
- L'auditeur doit être doté de qualités pédagogiques afin de communiquer ses recommandations de manière compréhensible aux différentes parties auditées ;
- L'auditeur doit être doté de qualité rédactionnelle et de synthèse ;
- L'auditeur doit pouvoir adapter son discours et exposer ses recommandations selon le public visé (équipes techniques, top management, équipes métier, etc.).

3.2.2 Compétences

Afin de mener à bien leurs missions d'audit, les auditeurs doivent couvrir un ensemble de compétences relatives aux audits de manière générale (détaillées dans la norme ISO 19011), ainsi que des compétences spécifiques aux audits de sécurité SI, à savoir :

- Les principes, procédures et méthodes de l'audit : pour veiller à ce que l'audit soit mené de façon cohérente et systématique. L'auditeur doit donc être capable de :
 - ◇ Appliquer les principes, les procédures et les méthodes d'audit appropriés à sa mission ;
 - ◇ Planifier et organiser les tâches et les différentes étapes de l'audit de façon efficace et efficiente ;
 - ◇ Respecter les délais ;
 - ◇ Avoir le sens des priorités ;

- ◇ Collecter les informations nécessaires pour établir les constats via des interviews méthodiques, l'observation de l'environnement audité, ainsi que les documents fournis par l'organisme audité ;
- ◇ Maîtriser les techniques d'échantillonnage, celles-ci permettent la mise en œuvre des procédures de l'audit sur une sélection pertinente d'éléments à auditer (personnes, serveurs, postes de travail, etc.). Cependant, cette méthode comporte des risques que l'auditeur doit maîtriser (le risque que la conclusion à laquelle aboutit l'auditeur sur la base d'un échantillon puisse être différente de la conclusion à laquelle il serait parvenu si l'ensemble des éléments avaient été soumis à l'audit) ;
- ◇ Vérifier les informations recueillies, la pertinence et la validité des preuves ;
- ◇ Effectuer une étude de risques qui pèsent sur la viabilité de l'audit ;
- ◇ Assurer la confidentialité et la sécurité des informations et des documents recueillis ;
- ◇ Communiquer efficacement à l'écrit comme à l'oral.
- L'auditeur doit maîtriser les réglementations applicables aux activités d'audit en tenant compte de l'activité de l'audité et du type d'audit à effectuer ;
- L'auditeur doit maîtriser les réglementations et les normes applicables aux audits de sécurité SI ainsi que les règles de sécurité qui constituent la DNSSI ;
- L'auditeur doit disposer idéalement des certifications ad-hoc (en particulier certification ISO/CEI 27001, CISA, CISM, CEH, Etc.) et il doit justifier d'une expérience d'audit dans le domaine ;
- L'auditeur doit avoir des compétences dans au moins une des activités de l'audit, il doit cependant être sensibilisé par rapport aux autres activités ;
- L'auditeur doit s'assurer du maintien à jour de ses compétences via un cursus de formation continue et de veille technologique ;
- Le responsable de l'équipe d'audit doit avoir des compétences en gestion d'équipe.

3.2.3 Parcours académique et professionnel

- L'auditeur doit avoir une formation en technologies des systèmes d'information et de communication ;
- L'auditeur doit avoir une expérience dans le domaine de la sécurité des systèmes d'information ;
- L'auditeur doit nécessairement justifier d'une expérience d'au moins 3 années dans le domaine d'audit des systèmes et de la sécurité des systèmes d'information.

3.2.4 Déontologie

Les auditeurs sont également soumis aux exigences d'éthique professionnelle. Ces exigences doivent être détaillées dans la charte d'éthique du prestataire d'audit auquel les auditeurs se rapportent. Elles concernent les principes suivants :

- L'auditeur doit signer l'engagement de confidentialité présenté par le prestataire d'audit ;
- L'auditeur doit signer la charte d'éthique du prestataire ;
- Dans le cadre de la mission d'audit, l'auditeur doit se conformer aux méthodes, outils et techniques qui ont été validés par le prestataire et acceptés par l'organisme audité ;
- Sauf accord ou demande expresse de l'organisme audité, l'auditeur se refuse toute tentative d'intrusion dans le système d'information audité, ou exploitation des failles mises en évidence au travers des activités d'audit ;
- L'auditeur ne doit pas communiquer des informations obtenues dans le cadre de l'audit, y compris aux autres auditeurs du prestataire non concernés par ledit audit ;
- L'auditeur doit signaler au commanditaire tout contenu illicite découvert pendant l'audit.

3.2.5 Critères de sélection des prestataires d'audit

Le choix du prestataire d'audit doit faire l'objet d'une étude minutieuse. Il convient donc d'établir des critères d'évaluation afin de quantifier les exigences citées auparavant à permettre au commanditaire de l'audit la classification des prestataires selon une échelle objective. Le but étant de trier les offres techniques selon une note qui sera attribuée à chaque candidat en application d'un barème de notation ventilé selon les trois critères cités ci-après.

Le premier critère de sélection consiste à étudier les références du prestataire dans le domaine des audits SSI. Dans ce sens, il convient de considérer son expérience dans l'audit des SSI ainsi que le nombre de missions menées par ce prestataire au cours des trois dernières années dans la réalisation de prestations similaires.

Le deuxième critère est articulé sur la qualité de la méthodologie proposée par le prestataire, ainsi que le programme de réalisation des prestations d'audit SSI. Il est recommandé de noter l'offre selon sa conformité aux termes de références du cahier des prescriptions spéciales (CPS) et sa valeur ajoutée par rapport aux exigences du commanditaire d'audit. Ainsi, le commanditaire doit s'assurer de l'adéquation de la démarche et de la méthodologie choisies avec les objectifs tracés de la mission d'audit.

Le troisième critère traite les connaissances et les compétences de l'équipe d'audit. Il s'agit des profils choisis par le prestataire pour mener cette mission, notamment le chef de projet d'audit, les consultants spécialistes en management de la SSI, les consultants techniques spécialistes en SSI ainsi que des experts juridiques justifiant de l'expérience nécessaire en Sécurité des SI. La sélection doit être effectuée en se basant sur le diplôme, le nombre d'années d'expérience dans des prestations similaires ainsi que le nombre et la nature des certifications obtenues.

Par conséquent, il convient de favoriser tout profil ayant une formation au minimum de Bac+5 (Bac + 8 pour les juridiques) et justifiant d'une expérience au minimum de huit ans dans des prestations similaires, et possédant un certain nombre de certifications reconnues mondialement dans son domaine d'intervention.

D'une manière générale, la note globale (NG) de la sélection est obtenue par pondération de la note technique (NT) et la note financière (NF) issue d'une analyse financière des offres. (Ex : $NG = 0.7NT + 0.3NF$).
L'offre retenue sera celle qui aura obtenu la note globale NG la plus élevée.



Conformément aux dispositifs de l'article 38 du décret num 2-12-349 relatif aux marchés publics, l'évaluation des offres techniques concerne les seuls candidats admis à l'issue de l'examen de leurs dossiers administratifs et techniques.

Références

- 1 *"La norme ISO 19011 :2011"*, 2011.
- 2 *"La norme 27002 :2013"*, 2013.
- 3 Agence Française de la Sécurité des Systèmes d'Information (ANSSI, *"Prestitaires d'audit de la sécurité des systèmes d'information (PASSI)"*).
- 4 *"Décret n 2-12-349 relatif aux marchés publics"*.