BULLETIN OFFICIEL DES ARMEES

Edition Chronologique n°48 du 8 novembre 2013

PARTIE PERMANENTE
Administration Centrale

Texte n°3

DIRECTIVE N° 28/DEF/DGSIC
portant sur l'exécution des audits de sécurité des systèmes d'information au sein du ministère de la défense.

Du *17 octobre 2013*

DIRECTION GÉNÉRALE DES SYSTÈMES D'INFORMATION ET DE COMMUNICATION.

DIRECTIVE N° 28/DEF/DGSIC portant sur l'exécution des audits de sécurité des systèmes d'information au sein du ministère de la défense.

Du 17 octobre 2013

NOR D E F E 1 3 5 1 7 6 9 X

Pièce(s) Jointe(s) :

Deux annexes.

Classement dans l'édition méthodique : BOEM 161.4

Référence de publication : BOC N°48 du 8 novembre 2013, texte 3.

SOMMAIRE

1. PRÉSENTATION GÉNÉRALE ET GUIDE D'USAGE.

1.1. Présentation.

1.2. Niveaux de préconisation.

1.3. Modalités d'application.

1.4. Gestion des dérogations aux règles de la directive.

2. CADRE DOCUMENTAIRE.

2.1. Documents applicables.

2.2. Normes et standards applicables.

2.3. Autres documents et site de référence.

3. DOMAINE COUVERT ET EMPLOI.

3.1. Services attendus.

3.2. Périmètre et limites.

3.2.1. Périmètre des audits.

3.2.2. Périmètre des inspections.

4. LES RÈGLES.

4.1. Formation et qualification des auditeurs.

4.1.1. Pré-requis à l'affectation dans un organisme d'audit.

4.1.2. Fiche de poste.

4.1.3. Recrutement.

4.1.4. Formation initiale - adaptation à l'emploi.

4.1.5. Formation continue.

4.1.6. Prestataires externes.

4.2. Modalités de réalisation d'un audit.

4.2.1. Audit organisationnel.

4.2.2. Audit technique.

4.3. Outils d'audit.

4.4. Réunion de clôture.

4.5. Format du rapport d'audit.

4.6. Charte d'audit.

ANNEXE(S)

ANNEXE I. QUELQUES ASPECTS DU MÉTIER D'AUDITEUR.

ANNEXE II. LISTE DE CATÉGORIES D'OUTILS (1).

1. PRÉSENTATION GÉNÉRALE ET GUIDE D'USAGE.

Nota. Les mots entre crochets ([]) figurent dans les documents applicables.

1.1. **Présentation.**

S'inscrivant en complément de la directive n° 15/DEF/DGSIC du 10 novembre 2010 sur les audits au sein du ministère [DIR AUDITS], cette directive aborde tous les aspects qui se rapportent aux modalités pratiques de réalisation d'un audit allant de la formation des auditeurs, aux aspects du métier d'auditeur, en passant par les méthodes et outils utilisés, jusqu'au contenu attendu du rapport d'audit ainsi qu'au format de la charte. En effet, ces sujets sont susceptibles d'évolution pour coller à l'état de l'art du domaine de l'audit contrairement au processus d'audit, lui même reconnu par les instances internationales de normalisation. Les différentes équipes d'audit du ministère de la défense bénéficient ainsi d'un référentiel unique pour réaliser les audits.

Cette directive s'inscrit dans les missions de la direction générale des systèmes d'information et de communication (DGSIC), aux termes du décret n° 2006-497 du 2 mai 2006 modifié, portant création de la direction générale des systèmes d'information et de communication et fixant l'organisation des systèmes d'information et de communication du ministère de la défense.

1.2. **Niveaux de préconisation.**

Les règles définies dans ce document ont différents niveaux de préconisation et sont conformes au référentiel général d'interopérabilité (RGI) et à la *request for comment* (RFC) 2119 :

- obligatoire : ce niveau de préconisation signifie que la règle édictée indique une exigence absolue de la directive ;

- recommandé : ce niveau de préconisation signifie qu'il peut exister des raisons valables, dans des circonstances particulières, pour ignorer la règle édictée, mais les conséquences doivent être comprises et pesées soigneusement avant de choisir une voie différente ;

- déconseillé : ce niveau de préconisation signifie que la règle édictée indique une prohibition qu'il est toutefois possible, dans des circonstances particulières, de ne pas suivre, mais les conséquences doivent être comprises et le cas soigneusement pesé ;

- interdit : ce niveau de préconisation signifie que la règle édictée indique une prohibition absolue de la directive.

1.3. **Modalités d'application.**

L'ensemble des règles définies dans cette directive s'applique aux équipes procédant à des audits de sécurité des systèmes d'information du ministère de la défense.

1.4. **Gestion des dérogations aux règles de la directive.**

Les dérogations font l'objet d'une approbation par l'autorité qualifiée concernée ou son représentant. Elles concernent les circonstances et justifications du non-respect d'une règle.

2. CADRE DOCUMENTAIRE.

2.1. **Documents applicables.**

RGI	:	référentiel général d'interopérabilité, version 1.0 du 12 mai 2009.
RGS	:	référentiel général de sécurité, version 1.0 du 6 mai 2010.
IGI 1300	:	instruction générale interministérielle n° 1300/SGDSN/PSE/SSD du 30 novembre 2011 (1) sur la protection du secret de la défense nationale.
PSSI	:	instruction n° 133/DEF/SEC/DIR/SIC du 18 mars 2002 modifiée, relative à la politique de sécurité des systèmes d'information du ministère de la défense.
IM 900	:	instruction ministérielle n° 900/DEF/CAB/-- du 26 janvier 2012 (1) relative à la protection du secret de la défense nationale au sein du ministère de la défense.
D I R AUDITS	:	directive n° 15/DEF/DGSIC du 10 novembre 2010 portant sur la réalisation des audits de sécurité des systèmes d'information au sein du ministère de la défense.
R E F AUDITS	:	référentiel n° 01/DEF/DGSIC du 20 juin 2013 (1) portant sur les documents utilisés lors des audits de sécurité des systèmes d'information au sein du ministère de la défense.
DIR HSI	:	directive n° 27/DEF/DGSIC du 24 janvier 2013 portant sur l'homologation des systèmes d'information du ministère de la défense.

2.2. **Normes et standards applicables.**

RFC 2119 : *request for comment* - mots-clés pour les niveaux d'obligation.

2.3. **Autres documents et site de référence.**

ISO 19011	:	*international organisation for standardization* - lignes directrices pour l'audit des systèmes de management.
ISO 27002	:	technologies de l'information - techniques de sécurité - code de bonne pratique pour le management de la sécurité de l'information.
ISO 27005	:	technologies de l'information - techniques de sécurité - gestion des risques en sécurité de l'information.
ISO 27006	:	technologies de l'information - techniques de sécurité - exigences pour les organismes procédant à l'audit et à la certification des SMSI (système de management de la sécurité de l'information).
ISO 27007	:	technologies de l'information - techniques de sécurité - lignes directrices pour l'audit des SMSI.
ISO 27008	:	technologies de l'information - techniques de sécurité - lignes directrices pour les auditeurs des contrôles de sécurité de l'information.
Site DGSIC	:	site DGSIC à l'adresse Intradef : www.dgsic.defense.gouv.fr.
Sites SSI	:	- site SSI de l'agence nationale de la sécurité des systèmes d'information (ANSSI) à l'adresse internet : http://www.ssi.gouv.fr ; - site SSI du ministère à l'adresse intradef : http://synoptic.intradef.gouv.fr/ssi.

3. DOMAINE COUVERT ET EMPLOI.

3.1. **Services attendus.**

La mise en application des différents éléments présentés dans cette directive doit permettre, dans le cadre d'une démarche d'amélioration, une uniformisation des processus de base communs à l'ensemble des équipes procédant à des audits.

En particulier cette démarche contribue à renforcer la confiance du commanditaire et de l'exploitant dans la qualité des résultats de l'audit et de leur complétude.

En corollaire, elle facilite également la reproductibilité des résultats pour un système d'information (2) donné et ce, indépendamment des personnels auditeurs. Cependant, ceci ne s'applique bien entendu qu'aux travaux communs, aux équipes d'audit du ministère et pas aux missions, responsabilités ou compétences spécifiques de certaines d'entre elles. De plus, pour un système d'information donné, si les objectifs des audits successifs diffèrent ou que des contraintes opérationnelles rendent une partie du système inaccessible ou bien que le périmètre a évolué, les résultats pourront présenter des différences sensibles.

Enfin, cette directive pourra servir de cadre de référence pour contractualiser avec une société d'audit extérieure au ministère.

3.2. **Périmètre et limites.**

3.2.1. ***Périmètre des audits.***

L'audit de sécurité est une démarche d'investigation conduite sur un système d'information en cours de déploiement, en exploitation ou prêt à l'être dans le cas d'une première homologation. Cette démarche inclut un diagnostic et conduit à des recommandations ou des conseils. Les audits peuvent porter sur les systèmes d'information (SI), les organisations qui les mettent en œuvre et les utilisateurs. Les audits, effectués sur tout ou partie d'un SI, ont pour objet :

- de qualifier les risques effectifs ou d'en quantifier le niveau ;

- de vérifier, voire d'évaluer, la qualité, l'efficacité et la cohérence, des dispositifs, mesures et procédures de sécurité ;

- de mettre en évidence les vulnérabilités résiduelles ;

- de proposer les éventuelles actions correctives.

Ils sont effectués selon une méthode cohérente avec la politique de sécurité du ministère, de préférence conforme à la famille de normes ISO/CEI 27000.

On distingue trois catégories :

- l'audit d'homologation qui sanctionne le processus d'homologation d'un SI ou confirme (ré-homologation) son maintien en condition de sécurité et permet à l'autorité d'homologation de se prononcer ;

- l'audit de diagnostic de sécurité d'un SI effectué sur un SI tel que défini supra pour établir le niveau de sécurité d'un SI ;

- l'audit de conformité permettant de s'assurer que le déploiement du SI est réalisé en rapport à un état de référence.

Une équipe d'audit est généralement constituée d'un ou plusieurs équipiers qui peuvent, suivant le périmètre du SI, être des auditeurs organisationnels ou des auditeurs techniques, placés sous la responsabilité d'un chef d'équipe. De plus l'équipe peut se voir confier du personnel en formation de parrainage ou d'adaptation à l'emploi.

Chaque audit comprend, *a minima*, une réunion préparatoire, une réunion de lancement et une réunion de clôture. Ces réunions permettent de déterminer le périmètre exact à auditer, la présentation de la méthodologie mise en œuvre, les interlocuteurs fonctionnels et techniques qui seront sollicités, le planning, les besoins techniques à mettre à disposition pour les auditeurs ainsi que les livrables attendus, de procéder à un débriefing à chaud des résultats de l'audit avec l'ensemble des acteurs, voire de préconiser (si besoin) des mesures de corrections immédiates à mettre en œuvre.

Les évaluations TEMPEST (terme d'origine anglo-saxonne désignant l'ensemble du domaine des signaux compromettants) sont réalisées par les équipes d'audits pour l'étude de signaux parasites compromettants. Elles ont pour objectifs de contrôler les normes techniques et de vérifier que le zonage réalisé, conjugué aux règles d'installation des matériels techniques employés, permet l'atténuation des signaux parasites compromettants par conduction et rayonnement.

3.2.2. ***Périmètre des inspections.***

Bien que les équipes d'inspection du ministère de la défense se voient appliquer les mêmes règles organisationnelles en ce qui concerne la formation et la qualification des auditeurs (point 4.2.1).

4. LES RÈGLES.

La directive est déclinée sous deux angles : organisationnel (RO) et technique (RT). Les règles sont numérotées séquentiellement par catégorie.

4.1. **Formation et qualification des auditeurs.**

La compétence des auditeurs est le facteur déterminant qui entre en jeu dans la confiance que le commanditaire et l'exploitant vont avoir dans les résultats de l'audit.

Pour ses personnels d'audit, le ministère ne recherche pas le diplôme de certification (3), leur niveau de compétences minimal provient d'une formation initiale (en école de formation au sein du ministère ou alors par recrutement direct) complétée par une formation d'adaptation à l'emploi. Puis le processus d'entretien et d'amélioration des compétences est réalisé au sein des organismes en interne et par la réalisation de stages conformément au plan de formation établi et suivi par le responsable de l'organisme.

4.1.1. ***Pré-requis à l'affectation dans un organisme d'audit.***

Compte tenu des spécificités du métier d'auditeur, il est nécessaire de procéder au recrutement de personnels disposant d'un niveau de qualification adapté et habilité confidentiel défense. Ce niveau s'acquiert par une expérience professionnelle ou un diplôme *a minima* de niveau 3 (4) ou équivalent. Le manquement à ces exigences affaiblirait les capacités d'analyse des équipes d'audit et donc augmenterait le risque de ne pas identifier des vulnérabilités critiques sur les systèmes d'information du ministère. Cependant, on ne peut ignorer, pour des impératifs de gestion, l'éventualité d'une première affectation en sortie d'école de formation initiale.

RO 1 : il est recommandé que le futur auditeur ait une première expérience professionnelle soit dans l'administration des systèmes et des réseaux informatiques, soit en sécurité des systèmes d'information (SSI), voire en développement, ou alors qu'il soit détenteur d'un diplôme de niveau 3 dans l'un des domaines précités.

À noter : par première expérience professionnelle il convient de comprendre un minimum de 2 ans dans le poste.

RO 2 : il est déconseillé qu'un personnel en sortie d'école de formation initiale soit affecté directement dans une équipe d'audit.

RO 3 : il est obligatoire que le futur auditeur, dans le cas d'une affectation en sortie d'école de formation initiale, ne soit pas positionné en situation de responsabilité d'auditeur avant la fin de son parrainage (5) (cf. RO 10).

4.1.2. ***Fiche de poste.***

La fiche de poste est un élément majeur qui doit permettre aux directions des ressources humaines de répondre au besoin des équipes d'audit et de fournir des candidats dont le profil est en adéquation avec les exigences du métier d'auditeur, qu'il soit chef d'équipe, auditeur organisationnel, auditeur technique, etc.

RO 4 : il est obligatoire que le chef de l'équipe d'audit ou que l'auditeur organisationnel ait au minimum un niveau fonctionnel 3a (ou équivalent pour le personnel civil).

RO 5 : il est obligatoire de faire figurer dans une fiche de poste d'auditeur les qualités humaines parmi celles données dans l'annexe I.

4.1.3. ***Recrutement.***

Le métier d'auditeur a des exigences particulières tant sur les compétences techniques que pour les qualités humaines à avoir.

RO 6 : il est recommandé que le recrutement des auditeurs en interne ministère par les organismes d'audit soit réalisé par un système de prospection.

RO 7 : il est recommandé que la candidature du futur auditeur soit validée par un entretien avec l'organisme d'audit.

4.1.4. ***Formation initiale - adaptation à l'emploi.***

RO 8	:	il est obligatoire que toute personne, dès son affectation en équipe d'audit, suive une formation d'adaptation (6) à l'emploi *ad hoc*.
RO 9	:	il est obligatoire que cette formation soit réalisée à la fois sous forme théorique et sous forme pratique.
RO 10	:	il est obligatoire que les plans de formation de parrainage, d'adaptation à l'emploi et de suivi de progression professionnelle soient validés par le chef de l'organisme d'appartenance.
RO 11	:	il est obligatoire que les acquis de l'auditeur soient validés par le chef de l'équipe d'audit suivant un tableau de suivi de progression (ou équivalent suivant les directives de formation de l'organisme).
À noter	:	cette validation organisée en interne ou au sein des organismes de formation peut aussi être réalisée au moyen de travaux pratiques.

4.1.5. ***Formation continue.***

La sécurité des systèmes d'information est étroitement liée à l'émergence et aux déploiements de nouvelles technologies. Les connaissances des auditeurs techniques doivent être régulièrement actualisées. Il s'agit donc de maintenir, par de la formation et de l'auto formation, un niveau de compétences techniques au plus près de l'état de l'art de la sécurité des systèmes en service.

RO 12	:	il est obligatoire de mettre en place un plan de formation continue, en accord avec la commission spécialisée de la formation (CSF cybersécurité), qui se décline en plan de formation pour l'auditeur et en objectif de compétences pour l'unité.
RO 13	:	il est obligatoire que les acquis dans le domaine de l'audit SSI soient validés suivant le plan de formation par le chef de l'organisme.
À noter	:	il s'agit là de pouvoir assurer le maintien des compétences.

4.1.6. ***Prestataires externes.***

RO 14	:	il est obligatoire de ne recourir qu'à des prestataires d'audit en sécurité des systèmes d'information (PASSI) qualifiés au sens du RGS.
À noter	:	les organismes passant des marchés introduiront cette exigence.

4.2. **Modalités de réalisation d'un audit.**

Il est généralement admis qu'un audit peut se subdiviser en deux domaines :

- l'audit organisationnel ;

- l'audit technique.

RO 15 : il est obligatoire qu'un audit, sauf directives du commanditaire précisées au sein de la charte et rappelées en introduction du compte-rendu, porte sur l'ensemble de l'écosystème (7) du SI.

À noter : les aspects organisationnels (dont la rédaction de la documentation), environnementaux (dont la protection physique) et techniques [dont tout ou partie du réseau d'accueil (8)] devront être vérifiés. Dans ce cadre le principe des cercles concentriques pourra être utilement appliqué (9).

RO 16 : il est obligatoire que le référentiel utilisé pour l'audit soit expressément précisé au sein du compte-rendu d'audit (généralement les documents réglementaires applicables utilement résumés au sein de la politique SSI de l'organisme, mais également, pour l'aspect technique, les guides de configuration et équivalents).

À noter : en particulier la conformité des mesures mises en place par rapport à la procédure d'exploitation de sécurité (PES), si elle existe, devra être vérifiée.

4.2.1. ***Audit organisationnel.***

L'audit organisationnel s'intéresse aux aspects de gestion et d'organisation de la sécurité sur le plan organisationnel, humain et physique mis en œuvre pour protéger le SI, que ce soit au niveau *global security environment* (GSE), *local security environment* (LSE) ou *electronic security environment* (ESE) et ce conformément à la politique de sécurité de l'organisme. L'objectif visé par cette étape est donc d'avoir une vue globale de la sécurité environnementale du SI et d'identifier les risques potentiels.

RO 17 : il est recommandé que dans le cadre de l'audit des entretiens soient réalisés avec a minima le responsable de la sécurité des systèmes d'information [RSSI (ou son représentant)], l'officier de sécurité (ou son représentant), un administrateur SSI et un utilisateur du système.

À noter : dans le cas d'un projet, il convient d'inclure le responsable fonctionnel du projet à auditer.

*4.2.2. **Audit technique.***

L'audit technique (10) est réalisé par une approche méthodique, adaptée au système et fonction de l'objectif, du champ et des critères, allant de la découverte et de la connaissance du réseau ou équivalent pour les systèmes d'armes et systèmes industriels (bus, etc.) en passant par le sondage des services réseaux et vulnérabilités associées (y compris les matériels actifs) jusqu'au paramétrage des serveurs et équipements clients (y compris les matériels spécifiques pour les SA et SI industriels), pour finir par la vérification des configurations des logiciels ou applications métiers et la protection des données.

RO 18 : il est obligatoire de conduire l'audit technique suivant une approche méthodique, traduite par la structure du compte-rendu d'audit (11) couvrant l'ensemble des composants matériels et logiciels du système d'information et abordant notamment les domaines génériques suivants :

- identification/authentification ;
- contrôle d'accès ;
- intégrité ;
- imputabilité/audit ;
- sécurité des échanges dont le chiffrement.

RO 19 : il est recommandé d'utiliser, en fonction du SI, l'ensemble des catégories d'outils énoncés au sein de l'annexe II.

À noter : la liste sera insérée au compte-rendu (sans préciser le nom de l'outil).

RO 20 : il est recommandé de disposer de la présence d'un administrateur d'un système en production lors de son audit pour valider la réalisation de certains tests pouvant perturber ledit système et nuire accidentellement à son bon fonctionnement.

4.3. **Outils d'audit.**

La qualité des audits techniques est dépendante de la maîtrise des outils utilisés. Une méconnaissance de certaines fonctionnalités peut mettre en péril un système critique. Il est donc primordial de favoriser une connaissance approfondie des outils, tout en ne négligeant pas la veille de nouvelles solutions plus efficaces ou couvrant de nouvelles technologies ainsi que la mise en commun des retours d'expériences des différents auditeurs techniques du ministère.

RT 1 : il est obligatoire que les équipes d'audit disposent de « boites à outils » validées par l'autorité qualifiée (AQ) (12).

RT 2 : il est obligatoire que les équipes d'audit tiennent à jour une liste des outils (logiciels et matériels) qu'elles détiennent en précisant leur finalité.

RT 3 : il est recommandé d'utiliser des outils qui couvrent la liste non exhaustive des catégories figurant en annexe II. (13).

RT 4 : il est obligatoire que les outils utilisés et le paramétrage de ces derniers lors de l'audit ne mettent pas en péril le bon fonctionnement des systèmes en production.

À noter : il s'agit de mettre en œuvre les processus afin de ne pas perturber le système audité conformément à la charte d'audit.

RT 5 : il est obligatoire de tracer les actions des auditeurs sur les systèmes audités en production.

À noter : par le système ou *a minima* sur un registre.

RO 21 : il est obligatoire que les auditeurs disposent d'équipements spécifiques et dimensionnés aux activités d'audit (notamment ordinateurs portables, clés USB, etc.), répondant à un cahier des charges particulier.

À noter : ces équipements, approuvés par l'autorité qualifiée de l'équipe d'audit, doivent rester sous le contrôle et la responsabilité de l'organisme d'audit. Le cahier des charges peut être élaboré par le groupe de coordination

technique.

RO 22 : il est obligatoire que les équipes d'audit disposent, en interne, de plates-formes de tests, d'entraînement et de préparation aux investigations.

RT 6 : il est recommandé que les équipes d'audit utilisent des outils techniques *open source*.

RT 7 : il est recommandé d'utiliser les outils validés lors des groupes de coordination technique.

RO 23 : il est obligatoire que les équipes d'audit assurent ou fassent assurer une veille sur les outils techniques utilisés ou utiles aux équipes d'audit.

RO 24 : il est obligatoire que les équipes d'audit se rencontrent deux fois par an pour échanger sur l'utilisation des outils lors des groupes de coordination technique (GCT) (14).

RO 25 : il est obligatoire que les machines d'audit soient effacées de manière sécurisée après chaque audit.

À noter : il s'agit de mettre en place une stratégie permettant de facilement rendre illisibles les données présentes sur le disque dur de la machine d'audit par formatage, chiffrement intégral de disque, etc. La solution choisie ne doit mettre en œuvre que des outils agréés pour le niveau de classification des données présentes sur la machine et impliquer une réinstallation complète du poste avant tout nouvel audit.

En l'état actuel, et en l'absence de solution de surcharge agréée pour le classifié de défense, les équipes d'audit doivent disposer de disques durs dédiés à chaque niveau de classification et marqués en conséquence, surchargés en fin d'audit.

RO 26 : il est obligatoire de protéger les informations recueillies lors des audits au niveau de protection *ad hoc*.

4.4. **Réunion de clôture.**

RO 27 : il est obligatoire que les éléments présentés lors de la réunion de clôture figurent dans le rapport final.

À noter : les caractéristiques de la réunion de clôture sont définies dans la [DIR AUDITS].

4.5. **Format du rapport d'audit.**

Il est important que l'avis global sur le niveau de sécurité du système d'information soit donné selon une métrique commune à l'ensemble des équipes d'audit et qu'il soit accompagné d'un commentaire.

Des éléments graphiques pour présenter les résultats d'audit sont un outil de communication important, néanmoins il faut faire attention à ce qu'ils ne puissent pas être interprétables et ne doivent pas se substituer à un commentaire circonstancié.

Un exemple de rapport structuré par fonctions de sécurité et sous-thèmes fonctionnels est proposé dans le référentiel associé à cette directive [REF AUDITS]. Certaines obligations, applicables au rapport d'audit d'homologation, découleront de ce modèle qui sera mis à jour par le GCT.

RO 28 : il est obligatoire que le rapport d'audit adopte 2 niveaux de lecture avec les éléments suivants :

- une synthèse à destination du commanditaire qui doit donner le niveau de sécurité globale du système et le niveau de sécurité de chaque fonction de sécurité du système ;

- le détail des vulnérabilités identifiées présentées dans une organisation par fonction de sécurité, assorti de recommandations cohérentes avec les besoins de sécurité du service audité.

RO 29 : il est recommandé que le rapport d'audit présente une description de scénarios d'attaque réalisables sur le système.

RO 30 : il est obligatoire de rappeler la définition des échelles utilisées pour qualifier les résultats de l'audit.

RO 31 : il est obligatoire que les recommandations issues de l'audit soient présentées sous la forme d'un tableau de forme libre avec lequel l'autorité d'homologation et le RSSI peuvent réaliser et suivre leur plan d'actions.

À noter : il est important que les livrables de l'audit facilitent l'élaboration puis le suivi du plan d'action correspondant aux recommandations.

4.6. **Charte d'audit.**

La charte d'audit doit mentionner le périmètre exact de la prestation, le respect du secret, l'habilitation des personnels auditeurs, les contraintes du métier, la méthode de destruction des traces des tests sur les serveurs audités, etc. Un exemple de charte d'audit est proposé dans le référentiel associé à cette directive [REF AUDITS]. La charte doit inclure :

- la nécessité d'une compréhension commune des vulnérabilités entre l'auditeur et l'audité ;

- la nécessité que l'audité informe, selon leurs périmètres respectifs, les acteurs concernés du déroulement de l'audit et des attendus de leur part.

RO 32 : il est obligatoire, en cas de visite préliminaire, que les éléments de la charte d'audit soient rappelés aux acteurs concernés.

RO 33 : il est obligatoire qu'un accord formel sur la charte soit donné par :

- le commanditaire de l'audit ;

- l'auditeur ;

- l'audité.

Pour le ministre de la défense et par délégation :

Le général de corps d'armée,
directeur général des systèmes d'information et de communication,

Gérard LAPPREND.

---

(1) n.i. BO.

(2) Ensemble des moyens informatiques ayant pour finalité d'élaborer, de traiter, de stocker, d'acheminer, de présenter ou de détruire des informations. Le terme SI (système d'information) s'applique également aux SI des systèmes d'armes et aux systèmes de contrôle commande industriel (ex : SCADA, etc.).

(3) Notamment les normes suivantes : CISSP, certification internationale validant les connaissances des experts et leur démarche permanente (obligatoire) de formation ; lead auditor ISO 27001 sanctionnant la connaissance des normes ISO 2700x dont l'audit ; certified information systems auditor (CISA) mondialement reconnue parmi les professionnels de l'audit.

Cependant, la politique de formation du ministère n'est pas antinomique de la démarche de certification. Ainsi un organisme, ou un auditeur à titre personnel, à toute latitude pour entreprendre un processus de certification.

(4) Niveau brevet de technicien supérieur (BTS), institut universitaire de technologie (IUT).

(5) Cette phase appelée parrainage consiste à faire encadrer le nouvel affecté par un personnel auditeur qualifié (au sens déjà formé aux opérations d'audit) afin de lui transmettre le savoir faire correspondant à chaque opération ou tâche qu'il devra effectuer.

(6) Ou suivant le cas de parrainage.

(7) L'écosystème comprend le système et l'environnement au sein duquel il est installé (d'où l'utilisation du terme).

(8) Cependant comme pour l'homologation, le principe d'héritage pourra être appliqué pour le réseau d'accueil (exemple des intranets déjà audités par ailleurs).

(9) En partant du cercle le plus éloigné pour se rapprocher du SI : l'organisation, puis la protection physique (GSE, LSE), puis le réseau et les services de sécurité apportés par le réseau (principe d'héritage), puis les serveurs et postes de travail, puis les logiciels ou applications spécifiques (ESE) et au final les données.

(10) L'audit de code qui consiste à vérifier la « qualité » du code (exécute mais n'exécute que les opérations demandées) est une technique d'investigation particulière, au même titre que l'analyse cryptologique ou la rétro ingénierie, et n'est donc pas abordée par la directive.

(11) Les modèles des documents font l’objet d’une publication séparée, cf. [REF AUDITS].

(12) Cette responsabilité peut être déléguée au chef de l’organisme.

(13) Les outils signaux parasites compromettants (SPC), de par leur spécificité, ne sont pas inclus dans la liste.

(14) De façon à garantir l'homogénéité des pratiques et du niveau des auditeurs, le fonctionnaire de sécurité des systèmes d'information (FSSI) anime un groupe de coordination technique des audits SSI (« GCT audits ») qui se réunit deux fois par an.

ANNEXE I.

QUELQUES ASPECTS DU MÉTIER D'AUDITEUR.

1. QUALITÉS HUMAINES.

Capacités de synthèse.

Capacités relationnelles.

Curiosité intellectuelle.

Discrétion.

Disponibilité.

Expression écrite.

Expression orale (pédagogie et négociation).

Honnêteté.

Objectivité.

Rigueur.

Sens de l'organisation.

2. SÉCURITÉ.

Habilitation confidentiel défense minimum [une habilitation secret défense (SD)/secret organisation du traité de l'Atlantique Nord (OTAN) (SO) ou très secret COSMIC (TSC) peut être requise pour certains systèmes].

Nationalité française (pour le personnel de la défense).

3. CONNAISSANCES.

Réglementation applicable au ministère de la défense sur les SIC et la SSI.

Connaissance de base sur les SIC.

Savoir rédiger un rapport.

Connaître les principes d'intrusion.

Compétences en anglais technique [profil linguistique standardisé (PLS) : 2222 - diplôme de compétence en langue (DCL) 2 et 3].

4. MISSIONS.

Mobilité pour des missions sur le territoire national et à l'étranger.

Réalisation d'audit, incluant la participation ou la responsabilité des activités suivantes :

- organisation de l'audit ;

- préparation de l'audit ;

- réalisation de l'audit sur site ;

- restitution des résultats d'audit à chaud ;

- analyse des informations recueillies ;

- rédaction du rapport d'audit.

Animer et participer à la veille technologique.

5. MISSIONS ANNEXES.

Réaliser ou participer à des démonstrations de recherche de vulnérabilité.

Réaliser ou participer à des sensibilisations.

ANNEXE II.

LISTE DE CATÉGORIES D'OUTILS (1).

1. RÉSEAU.

Sondage et reconnaissance réseau (cartographie, protocoles, etc).

Tests automatiques de vulnérabilités réseau.

Analyse et interception de flux réseau dont fabrication et injection de trames.

Audit des équipements réseau (routeurs, switchs).

Tests de robustesse des outils de sécurité réseau [pare-feu, *intrusion detection system* (IDS), outils d'authentification].

Scan de découverte de connexions dangereuses.

2. BASE DE DONNÉES.

Audit de système de gestion de base de données.

3. AUTHENTIFICATION.

Tests de robustesse des objets d'authentification.

---

(1) Cette liste sera actualisée lors des groupe de coordination technique (GCT) d'auditeurs.

Les guides de configuration validés sont disponibles en ligne sur intradef, en l'absence de guide de configuration disponible une vulnérabilité doit être levée et l'équipe d'audit doit faire remonter le besoin au comité régissant la production de guide.