BULLETIN OFFICIEL DES ARMEES

Edition Chronologique n°51 du 3 décembre 2010

PARTIE TEMPORAIRE
Administration Centrale

Texte n°14

DIRECTIVE N° 15/DEF/DGSIC
portant sur la réalisation des audits de sécurité des systèmes d'information au sein du ministère de la défense.

Du *10 novembre 2010*

DIRECTION GÉNÉRALE DES SYSTÈMES D'INFORMATION ET DE COMMUNICATION.

DIRECTIVE N° 15/DEF/DGSIC portant sur la réalisation des audits de sécurité des systèmes d'information au sein du ministère de la défense.

Du 10 novembre 2010

NOR D E F E 1 0 5 2 6 1 8 X

Référence de publication : BOC N°51 du 3 décembre 2010, texte 14.

SOMMAIRE

1. PRÉSENTATION GÉNÉRALE ET GUIDE D'USAGE.

1.1. **Présentation.**

La présente directive a pour objet de définir le processus d'audit de sécurité ou de conformité des systèmes d'informations au sein du ministère de la défense. Les différentes équipes d'audit du ministère de la défense bénéficient ainsi d'un référentiel unique pour réaliser les audits.

Les éléments fonctionnels et techniques, comme l'homogénéisation des formations minimales et communes des auditeurs, les outils mis en œuvre dans le cadre des audits ou le contenu des rapports d'audit, feront l'objet d'une directive spécifique. Cette dernière inclura aussi des modèles de documents, comme la charte d'audit, qui sont échangés entre les diverses parties intervenant dans un audit.

À noter que cette directive englobe également les obligations faites vis à vis du tableau de bord des homologations de la sécurité des systèmes d'informations (TBHSSI) que la fonction d'audit doit alimenter. Elle aborde enfin la question du suivi des audits afin de délimiter le rôle des auditeurs.

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 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 [RGI] et à la [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 dont il est toutefois possible, dans des circonstances particulières, de s'affranchir, mais les conséquences doivent être intégrées et le cas soigneusement apprécié ;

- 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 l'audit des systèmes d'informations du ministère de la défense ainsi qu'aux responsables des systèmes audités. Elle concerne les aspects suivants : définition des acteurs intervenant dans le processus d'audit, déroulement d'un audit.

Les directions et services transposent les exigences de la présente directive dans les cahiers des charges des marchés publics en relation avec les prestations d'audit.

2. CADRE DOCUMENTAIRE.

2.1. **Documents applicables.**

[CPP] Code de procédure pénale.

[IM4418] Instruction n° 4418/DEF/SEC/DIR/SIC du 25 septembre 2000 relative à la mise en œuvre de la sécurité des systèmes d'information au sein du ministère de la défense.

[RGI] Référentiel général d'interopérabilité version 1.0 du 12 mai 2009.

2.2. **Normes et standards applicables.**

[RFC 2119] Mots-clés pour niveaux d'obligation.

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

[Site DGSIC] site DGSIC à l'adresse intradef /www.dgsic.defense.gouv.fr

[Site SSI] site SSI ministériel à l'adresse intradef /www.ssi.defense.gouv.fr

site SSI gouvernemental à l'adresse internet/www.ssi.gouv.fr

3. DOMAINE COUVERT ET EMPLOI.

3.1. **Services attendus.**

L'adoption de la même méthodologie par l'ensemble des équipes procédant à des audits doit permettre de garantir la reproductibilité des résultats pour un système d'information donné et ce, indépendamment des personnels auditeurs.

De même, l'utilisation de la même structure de rapports facilitera l'utilisation et la comparaison de ces rapports.

3.2. **Périmètre et limites.**

Le domaine couvert concerne les audits des systèmes d'information du ministère.

3.3. **Interopérabilité et interfaçage (si besoin).**

La présente directive définit le processus d'audit au sein du ministère. Les résultats d'un audit de la sécurité des systèmes d'informations (SSI), dans le cadre d'une homologation, servent à alimenter l'application TBHSSI. Ce processus se situe donc en amont de ce dernier.

4. LES RÈGLES.

4.1. **Règles techniques.**

Sans objet.

4.2. **Règles organisationnelles.**

4.2.1. ***Objectif de l'audit.***

Les objectifs de l'audit peuvent être multiples. Ils peuvent s'inscrire dans une démarche d'homologation des systèmes, dans le but de détecter à un instant donné les vulnérabilités pour dresser une évaluation pratique des risques pesant sur le système d'information.

RO 01 : il est obligatoire que les objectifs de l'audit soient définis par l'autorité qualifiée (ou son représentant) ou l'autorité d'homologation (ou son représentant).

4.2.2. ***Champ de l'audit.***

RO 02 : il est recommandé que le champ de l'audit précise notamment :

- le niveau de sensibilité du système d'information (classification des données, contraintes sur le système...) ;

- les lieux ;

- le périmètre technique et organisationnel des investigations ;

- la période calendaire souhaitée ;

- un point de contact ;

- tout élément susceptible d'éclairer le commanditaire sur l'intérêt de l'audit.

RO 03 : il est obligatoire que le champ de l'audit soit cohérent avec les objectifs de l'audit.

4.2.3. ***Critères de l'audit.***

Il s'agit de l'ensemble des références utilisées pour mesurer la conformité du système d'information. Il peut s'agir de textes réglementaires, de politiques, de procédures, de normes, de guides de bonnes pratiques.

RO 04 : il est recommandé que le champ et les critères de l'audit soient définis conjointement par le commanditaire et l'équipe d'audit.

RO 05 : il est obligatoire que dans le cas d'une modification touchant aux objectifs, au champ ou aux critères de l'audit, les deux parties (le commanditaire et l'équipe d'audit) soient d'accord.

4.2.4. ***Demande d'audit.***

RO 06 : il est obligatoire que les demandes d'audit des systèmes d'information des armées, services et directions soient formulées auprès de chaque autorité qualifiée ou de leur représentant.

RO 07 : il est obligatoire que les autorités qualifiées établissent les priorités d'audit dans le périmètre de leurs différents systèmes d'information.

Les ressources du ministère sont limitées. Il est nécessaire que les autorités qualifiés définissent les systèmes d'informations dont les audits sont prioritaires afin de permettre l'optimisation du plan de charge des équipes d'audit.

RO 08 : il est recommandé que les autorités qualifiées fixent les priorités en fonction des critères suivants :

- caractère opérationnel du système ;

- caractère vital pour le bon fonctionnement de l'organisme ;

- niveau de classification ;

- échéances réglementaires (autorisation temporaire d'emploi, renouvellement d'homologation...) ;

- date du dernier audit.

RO 09 : dans le cas où le commanditaire est l'état-major des armées (EMA), il est obligatoire que ce dernier examine toutes les demandes d'audit. Par un dialogue en amont avec les autorités qualifiées et les responsables des équipes d'audit, il les ordonne à son niveau en prenant en compte les éléments transmis. Il les répartit dans un plan de charge qu'il transmet aux responsables des équipes d'audit. Ce plan de charge constitue un ordre de réalisation des audits prescrits.

4.2.5. ***Déclenchement de l'audit.***

RO 10 : il est obligatoire qu'au moment du déclenchement de l'audit (sur planification du programme d'audit, ou sur demande ponctuelle), le responsable des équipes d'audit de l'organisme mandaté constitue une équipe d'audit.

RO 11 : il est obligatoire que l'équipe d'audit effectue les actions suivantes : rappel des objectifs, du champ et des critères d'audit en liaison avec l'organisme audité.

RO 12 : il est recommandé d'envoyer à l'audité un questionnaire préliminaire.

RO 13 : il est recommandé d'organiser une visite préliminaire sur site.

RO 14 : il est obligatoire de rédiger une charte d'audit qui détaille notamment les objectifs, le champ, les critères et le planning de l'audit.

RO 15 : il est obligatoire que les auditeurs aient les compétences adaptées à la nature de l'audit.

RO 16 : si des auditeurs, en cours de qualification, sont incorporés à des fins pédagogiques à l'équipe d'audit, il est obligatoire qu'ils soient strictement encadrés par le responsable de l'audit.

Une équipe d'audit doit s'assurer au mieux de son indépendance vis-à-vis des responsables du système audité et être garante de l'impartialité de ses résultats au travers d'une démarche objective.

RO 17 : il est obligatoire, pour la constitution de l'équipe d'audit, que le responsable des équipes d'audit s'assure qu'il n'y a pas parmi les personnels retenus de conflit d'intérêt à participer à l'audit.

RO 18 : il est obligatoire que les membres de l'équipe d'audit soient en possession d'un certificat de sécurité valide en adéquation avec le niveau d'habilitation requis pour l'accès au système d'information à auditer.

4.2.6. ***Visite préliminaire.***

La visite préliminaire constitue une première étape dans la prise de contact entre l'auditeur et l'entité auditée.

Elle est aussi l'occasion d'examiner la faisabilité de l'audit en tenant compte de facteurs tels que :

- l'existence des informations suffisantes et appropriées pour pouvoir préparer l'audit ;
- la possibilité d'une coopération adéquate de la part de l'audité ;
- la disponibilité des ressources nécessaires et l'adéquation du temps imparti ;
- l'état de maturité du système et de son niveau d'appropriation par l'exploitant.

RO 19 : il est recommandé qu'au cours de la visite préliminaire, les points suivants soient précisés :

- rappel de la légitimité de la réalisation de l'audit ;
- vérification de l'aptitude du système d'information à être audité ;
- présentation des informations sur le calendrier proposé et la composition de l'équipe d'audit ;
- identification et demande d'accès aux documents pertinents ;
- détermination des règles de sécurité applicables sur le site ;
- prise en compte des dispositions logistiques pour l'audit ;
- présentation de la démarche d'audit.

Selon l'importance ou la complexité du système d'information, la visite préliminaire sur site peut être facultative si l'ensemble des documents fournis par l'audité, par courrier ou messagerie électronique, est suffisant pour préparer l'audit et si la charte proposée n'amène pas de questions particulières. Dans le cas contraire, une reconnaissance sera envisagée.

RO 20 : il est recommandé que l'équipe diligentée pour la visite préliminaire soit composée, *a minima*, d'un auditeur organisationnel et d'un auditeur technique.

RO 21 : il est recommandé que la visite préliminaire ait une durée minimale d'une journée hors délai de route.

RO 22 : il est recommandé que la visite préliminaire soit planifiée avec suffisamment d'anticipation pour permettre à l'équipe d'audit de disposer de deux semaines complètes pour étudier les documents fournis.

RO 23 : il est obligatoire, lorsque l'audit est jugé non réalisable par l'équipe d'audit, qu'un compte rendu soit adressé pour action au commanditaire.

4.2.7. ***Revue des documents.***

La revue des documents permet :

- de déterminer la conformité documentaire du système d'information aux critères d'audit ;

- d'acquérir une connaissance suffisante du système et de son environnement en vue de réaliser un état des lieux et d'élaborer un plan d'audit approprié.

RO 24 : il est obligatoire que l'audité fournisse, avant le début de l'audit sur site, l'ensemble des documents relatif à la mise en service du système d'information.

RO 25 : il est recommandé, pour une homologation, que le référentiel type à fournir, se compose des documents suivants : fiche d'expression rationnelle des objectifs de sécurité (FEROS), procédures d'exploitation de sécurité (PES), stratégie d'homologation, procédures et documents d'administration et d'utilisation (DAU) ou de leurs équivalents pour les systèmes internationaux [dans un cadre de l'organisation du traité de l'atlantique nord (OTAN) : system-specific security requirement statement (SSRS), security operational procedure (SECOPS),...].

RO 26 : il est obligatoire que le responsable de l'audit informe le commanditaire et l'audité si la documentation se révèle inadéquate ou insuffisante. Un compte rendu est alors adressé pour action au commanditaire.

4.2.8. ***Préparation des activités d'audit.***

Le responsable de l'équipe d'audit a en charge la rédaction d'un document appelé charte d'audit. Ce document servira de base d'accord entre le commanditaire, l'autorité qualifiée et ou d'homologation, l'équipe d'audit et l'audité en ce qui concerne la réalisation de l'audit. Ce document doit faciliter la programmation dans le temps et la coordination des activités d'audit.

RO 27 : il est obligatoire que la charte couvre les éléments suivants :

- les objectifs de l'audit ;

- les critères d'audit et l'ensemble des documents de référence ;

- le périmètre technique et organisationnel ;

- les dates et lieux où seront menées les activités d'audit sur site ;

- les réunions de démarrage et de clôture avec la liste des participants ;

- les rôles et responsabilités des membres de l'équipe d'audit et des éventuels accompagnateurs [secrétariat général de la défense nationale (SGDSN)...] ;

- les ressources appropriées dont la mise à disposition est nécessaire ;

- la conduite à tenir par les auditeurs en cas de suspicion de compromission ou de manquement à la loi ;

- l'identification des représentants de l'audité durant l'audit ;

- la confidentialité des données récupérées et l'anonymisation des constats et des résultats ;

- les possibilités et les conditions de prises de vue photographiques ;

- l'engagement du site audité à effectuer une sauvegarde des données avant l'audit ;

- l'engagement des auditeurs à tout mettre en œuvre pour ne pas perturber le fonctionnement du système audité ;

- les lieux et équipements du site nécessitant une mise en garde de l'équipe d'audit dans le domaine de l'hygiène, la sécurité et les conditions de travail (HSCT) ;

- la liste des destinataires du compte rendu à chaud et du rapport d'audit.

RO 28 : il est recommandé que la charte traite des éléments suivants de la logistique (déplacements, hébergement, dispositions sur site, moyen mis à disposition, modalités financières...).

4.2.9. ***Réalisation de l'audit sur site.***

4.2.9.1. Réunion d'ouverture.

Le but de cette réunion est de confirmer la charte d'audit, de présenter brièvement la manière dont les activités d'audit seront menées, de confirmer les circuits de communication et d'offrir la possibilité à l'audité de poser des questions. La réunion d'ouverture aborde donc les points suivants :

- présentation des participants, de leurs rôles ;

- rappel des finalités de l'audit ;

- confirmation des objectifs, du champ et des critères d'audit ;

- les méthodes et procédures utilisées pour réaliser l'audit ;

- confirmation des horaires (notamment la date et l'heure de la réunion de clôture) et des dispositions pratiques ainsi que de la disponibilité des ressources prévues et des personnels éventuels devant servir de guide ;

- confirmation des circuits de communication formels entre l'équipe d'audit et les audités ;

- confirmation des règles de confidentialité ;

- rappel des consignes de sécurité, de sûreté et d'urgence applicable à l'équipe d'audit ;

- la méthode pour régler d'éventuels litiges entre audité et auditeur.

RO 29 : il est obligatoire que l'audit débute formellement par une réunion d'ouverture en présence des responsables du site, des responsables de l'organisme et/ou du système audité et des responsables des fonctions ou des processus à auditer.

4.2.9.2. Exécution de l'audit.

RO 30 : il est obligatoire que la durée de cette phase soit adaptée à la complexité du champ de l'audit et ne pas être contrainte à tout prix par le calendrier prévisionel.

4.2.9.3. Communication pendant l'audit.

Le climat de confiance audité/auditeur est un élément fondamental quant au bon déroulement d'un audit, cependant :

RO 31 : il est déconseillé, durant la phase de recueil sur le site, que le responsable de l'équipe d'audit tienne informé l'audité de l'avancement des travaux et de toutes les difficultés rencontrées.

RO 32 : il est obligatoire que le responsable de l'équipe d'audit tienne informé le commanditaire si ce dernier le demande et si l'équipe d'audit a réuni suffisamment d'éléments.

RO 33 : il est obligatoire que le responsable de l'équipe d'audit rende compte immédiatement à l'audité et, si nécessaire, au commanditaire de l'audit, de tout élément constaté au cours de l'audit qui laisse supposer un risque immédiat ou significatif.

RO 34 : il est obligatoire que les auditeurs respectent un devoir de discrétion, lors de leurs entretiens, en particulier vis à vis d'audits antérieurs concernant d'autres sites ou d'autres systèmes d'information.

4.2.9.4. Rôles et responsabilités des guides et observateurs.

RO 35 : il est obligatoire que l'audité (ou son représentant désigné) accompagne l'équipe d'audit pour faciliter ses investigations.

RO 36 : il est obligatoire que l'audité désigne un ou plusieurs responsables chargés :

- d'organiser les entretiens ;

- de préparer les visites dans les lieux particuliers du site ;

- de s'assurer que les règles concernant les consignes de sécurité et les procédures de sûreté concernant le site sont connues et respectées par les membres de l'équipe d'audit ;

- de fournir des clarifications et aider à recueillir des informations ;

- de fournir le soutien logistique nécessaire à la réalisation de l'audit dans des conditions optimales.

RO 37 : il est obligatoire que pour les aspects techniques, l'audité désigne de préférence un ou des administrateurs (1) ou, à défaut, un ou des opérateurs pour aider à l'exécution de commandes et prévenir d'éventuelles conséquences techniques

4.2.9.5. Recueil et vérification des informations.

L'auditeur organisationnel rencontre les responsables impliqués dans la sécurité du système et de l'organisme et recueille les informations relatives à son domaine.

Les autres auditeurs (un ou plusieurs selon le mandat) de l'équipe d'audit effectuent les investigations techniques sur le système. Elles consistent principalement en une cartographie et des relevés de configurations des constituants du système.

RO 38 : il est obligatoire que les constations soient factuelles aussi bien sur la partie organisationnelle que sur les aspects techniques de l'audit.

RO 39 : il est obligatoire que les informations concernant les interfaces entre les fonctions, activités et processus soient vérifiées par recoupement et dans la mesure du possible étayées par des références documentaires.

RO 40 : il est obligatoire que l'auditeur organisationnel garantisse l'anonymat de la provenance des informations collectées durant les interviews.

RO 41 : il est recommandé de procéder à un audit automatique exhaustif de parc plutôt qu'à un audit par échantillonnage, lorsque la taille du système le permet, afin de limiter l'incertitude quant aux résultats des audits techniques. Les informations récoltées doivent donc être enregistrées et pouvoir être détaillées en tant qu'argumentaire dans le rapport final.

4.2.9.6. Constats d'audit.

Durant la phase de recueil et de vérification des informations, l'équipe d'audit peut être amenée à constater un incident de sécurité ou la présence de contenu illicite constitutif de crime ou délit sur le système d'information.

Pour rappel, l'article 40. du code de procédure pénale (2) dispose que « toute autorité constituée, tout officier public ou fonctionnaire qui, dans l'exercice de ses fonctions, acquiert la connaissance d'un crime ou d'un délit est tenu d'en donner avis sans délai au procureur de la République et de transmettre à ce magistrat tous les renseignements, procès-verbaux et actes qui y sont relatifs ».

Pour le ministère de la défense et dans le cas particulier des audits, l'autorité constituée est le commanditaire. Auditant au profit du commanditaire, les auditeurs ont uniquement un devoir d'information envers ce dernier. C'est l'autorité constituée qui aura l'obligation de prévenir le procureur de la République conformément à l'art. 40. du code de procédure pénale (2).

RO 42 : il est obligatoire que toutes les vérifications donnent lieu à des constats d'audit. Ces constats peuvent prendre soit la forme de simples mentions de conformité, soit de fiches d'écart, rédigées sous la forme « critère/écart/preuve ». Toutes les preuves liées aux investigations menées sont conservées.

RO 43 : il est obligatoire que les auditeurs rendent compte au commanditaire, à l'autorité hiérarchique, ainsi qu'au représentant local du service de sécurité, de la constatation d'un incident de sécurité, de la présence d'un contenu illicite ou d'une suspicion de compromission.

Pour les forces armées, le représentant local du service de la sécurité sera un officier de la DPSD du site audité, pour les autres directions le représentant de leur propre service de sécurité interne.

RO 44 : il est obligatoire que le responsable de l'équipe d'audit rende compte à sa propre hiérarchie.

RO 45 : il est obligatoire que les auditeurs, le commanditaire ainsi que le représentant de l'autorité hiérarchique du site décident conjointement, en fonction de la nature de l'incident, de la poursuite ou non de l'audit.

RO 46 : il est obligatoire que les moyens techniques soient mis en œuvre afin que les différents éléments de preuve soient préservés pour être éventuellement mis à disposition sur demande de l'autorité judiciaire.

RO 47 : il est recommandé que conformément au respect du besoin d'en connaître, du respect de la vie privée et du secret des correspondances, la constatation de l'incident, de la présence de contenu illicite ou de la suspicion de compromission puisse ne pas être abordée lors de la réunion de clôture.

RO 48 : il est obligatoire que le responsable de l'équipe d'audit informe, à son retour, le représentant local du service de sécurité de son site d'appartenance de la constatation d'un incident de sécurité, de la présence de contenu illicite, sans en dévoiler le contenu, sur le système d'information audité ou d'une suspicion de compromission.

4.2.9.7. Préparation des conclusions d'audit.

RO 49 : il est recommandé qu'à la fin de chaque journée, l'équipe se réunisse et consolide ses observations. En fonction des résultats obtenus, un ajustement du planning d'audit pourra être décidé.

RO 50 : il est obligatoire qu'à la fin de la période de recueil d'informations, l'équipe se réunisse à huis clos pour mettre en forme la présentation de la réunion de clôture et statuer sur les écarts constatés, afin de présenter ses conclusions.

4.2.9.8. Réunion de clôture.

Elle doit permettre à l'audité de comprendre et d'accepter les résultats de l'audit. Des recommandations doivent y être présentées.

Selon les situations, la réunion de clôture peut se résumer à une restitution des constats et des conclusions ou bien se formaliser avec un compte-rendu dans lequel figurera la liste de présence.

En cas de divergence d'opinion relative aux constats et/ou aux conclusions d'audit, un débat entre auditeurs et audités est possible. Cependant, l'équipe d'audit conserve toute latitude quant à ses conclusions dans le cadre de la mission qui lui a été confiée qui vise l'indépendance et l'objectivité des résultats.

RO 51 : il est obligatoire qu'une réunion de clôture, appelée aussi « compte rendu à chaud » soit organisée pour présenter les constats et les premières conclusions de l'audit.

RO 52 : il est obligatoire que le responsable du site audité, ou son représentant, soit présent à cette réunion.

RO 53 : il est obligatoire que lors de la restitution des constations et conclusions de l'audit, la présentation ainsi que la présence des différents représentants des fonctions ou processus audités soient conformes aux besoins d'en connaître respectifs de chacun.

RO 54 : il est recommandé, dans le cadre d'une homologation, que l'équipe d'audit fournisse, lors de cette réunion, un avis préliminaire sur le niveau de sécurité du système.

RO 55 : il est obligatoire que les administrateurs du système d'information audité attestent de la bonne marche du système, dégageant la responsabilité des auditeurs techniques de tous problèmes postérieur à l'audit.

RO 56 : il est recommandé que le commanditaire de l'audit ainsi que d'autres parties invitées, dans la mesure où ces dernières ont le besoin d'en connaître, participent à la réunion de clôture ;

RO 57 : il est recommandé que le responsable de l'équipe d'audit informe l'audité de toutes situations rencontrées pendant l'audit, susceptibles d'altérer la confiance qui peut être accordée aux conclusions d'audit ;

RO 58 : il est obligatoire qu'à l'issue de la réunion, le support de la présentation (sauf mention contraire, document classifié CD-SF) ainsi qu'une proposition de mesures correctives et préventives, à conduire par l'organisme audité, soient transmis à la liste de destinataires définie dans la charte d'audit. Ce document doit permettre à l'audité et à l'autorité qualifiée de planifier au plus vite les actions nécessaires à la mise en conformité du système, sans attendre la réception du rapport d'audit. Ce document servira de base pour tout audit ultérieur sur le même système d'information.

4.2.10. ***Élaboration et remise du rapport d'audit.***

Les éléments organisationnels et techniques recueillis sur le système d'information audité sont ensuite exploités dans les locaux de l'équipe d'audit. Cette phase d'analyse peut nécessiter plusieurs semaines de travail selon l'importance du système audité.

Le rapport d'audit contient une liste de recommandations qui comprend pour chaque mesure :

- un numéro de référence ;

- un libellé décrivant de manière synthétique la recommandation ou la mesure ;

- une priorité, correspondant au niveau de criticité de la vulnérabilité associée à la recommandation ou à la mesure (vis à vis d'une homologation) sur une échelle à trois valeurs :

    - rouge : critique ;

    - orange : majeure ;

    - jaune : mineure ;

- un justificatif.

RO 59 : il est obligatoire que l'ensemble des preuves et enregistrements techniques (journaux, fichiers de configuration, résultat de scan, capture d'écran...) soient conservés pendant la durée de mise en œuvre du plan de recommandations, au cas où les administrateurs du site audité auraient besoin d'informations particulières. Une fois le plan de recommandations décliné et ensuite mis en œuvre, les preuves et enregistrements sont détruits par des procédés réglementaires.

La présence d'éléments critiques peut avoir pour conséquence qu'une homologation, ou même une autorisation provisoire d'exploitation, soit exclue. La mise en évidence de vulnérabilités majeures peut permettre d'envisager une autorisation provisoire d'exploitation, sous réserve que le plan d'actions soit mis en œuvre. La mise en évidence de vulnérabilités mineures ne remet pas à priori la sécurité du système mais il convient de les prendre en compte. Toutefois, c'est l'analyse globale des vulnérabilités qui permet de donner un avis vis-à-vis de l'homologation du système.

RO 60 : il est obligatoire que, dans le rapport, l'équipe d'audit fournisse un avis à l'autorité d'homologation sur le niveau de sécurité du système. Cet avis lui permet d'instruire le dossier d'homologation.

RO 61 : il est obligatoire que le rapport final d'audit soit classifié, sauf mention contraire (comme les systèmes OTAN...), au minimum au niveau « confidentiel défense - spécial France ». Il sera transmis sous forme papier ou numérique à la liste de destinataires définie dans la charte d'audit.

RO 62 : il est obligatoire que pour les armées, la liste de diffusion du rapport final comprenne au minimum :

- le commanditaire ;

- l'audité ;

- l'autorité qualifiée ou son représentant légal ;

- le fonctionnaire de sécurité des systèmes d'information (FSSI) ;

- les archives de l'entité dont est issue l'équipe d'audit.

4.2.11. ***Clôture de l'audit.***

L'audit est considéré comme terminé lorsque toutes les activités décrites dans la charte d'audit ont été réalisées et que le rapport d'audit approuvé a été diffusé.

4.2.12. ***Suivi d'audit.***

Les conclusions de l'audit peuvent mentionner la nécessité d'actions correctives, préventives ou d'amélioration, quand cela est applicable.

L'élaboration du plan d'action est de la responsabilité du responsable de la sécurité des systèmes d'information (RSSI) ou des officiers de sécurité des systèmes d'information (OSSI) qui doit le faire approuver par l'autorité qualifiée (AQ). L'exécution du plan d'action est du ressort du RSSI concerné par l'audit ou de l'OSSI selon la cible d'audit.

RO 63 : il est obligatoire que l'autorité qualifiée définisse les actions à mener ainsi que les responsables pour actions et délais associés.

RO 64 : il est obligatoire que les actions soient réalisées par l'audité dans des délais convenus.

Les actions ne sont pas considérées comme faisant partie de l'audit.

RO 65 : il est obligatoire que l'état d'avancement et d'achèvement des actions préconisées dans le plan d'actions soit rapporté auprès de l'autorité qualifiée dont dépend le système d'information dans les six mois.

4.2.13. ***Suivi d'audit dans l'application du tableau de bord des homologations de la sécurité des systèmes d'information.***

RO 66 : il est obligatoire que l'application ministérielle « TBHSSI » soit renseignée après chaque audit d'homologation par l'équipe d'audit ayant réalisé la prestation.

RO 67 : il est obligatoire que chacune des différentes mesures du tableau de recommandations soit, selon sa pertinence, ventilée dans l'un des environnements de sécurité : GSE, LSE ou ESE.

RO 68 : il est obligatoire que les auditeurs soient formés à l'utilisation de l'application « TBHSSI ».

5. GLOSSAIRE ET ACRONYMES.

Audit de sécurité : l'audit de sécurité est une démarche d'investigation conduite sur un système d'information (2) en cours de déploiement, en exploitation ou prêt à l'être dans le cas d'une première homologation. Il inclut un diagnostic et conduit à des recommandations ou des conseils. Il permet de faire une mesure, à un instant donné, du niveau de sécurité d'un système d'information et de son écart au regard d'un référentiel documentaire de sécurité ou de dispositions de sécurité communément reconnues.

Il peut se décomposer en interventions techniques et/ou organisationnelles.

Lorsque l'audit s'inscrit dans le cadre d'une démarche d'homologation, le rapport d'audit fait partie du dossier d'homologation qui permet à l'autorité d'homologation de se prononcer.

Les audits effectués sur tout ou partie d'un système d'information ont pour objet, par rapport à des documents, une cible, des attendus et un niveau de sécurité :

- 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 tant sur le plan organisationnel que technique ;

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

- de proposer les éventuelles recommandations et actions correctives ;

- de fournir un avis à l'autorité d'homologation, lorsque l'audit s'inscrit dans le cadre d'une démarche d'homologation.

Les vulnérabilités organisationnelles et techniques relevées sont consignées dans un support de débriefing et un rapport d'audit comprenant une liste de propositions.

Les audits sont effectués selon une méthode cohérente avec la politique de sécurité du ministère. Ils contribuent à la qualification du volet défensif de cette politique.

Audit de conformité : l'audit de conformité permet d'évaluer les écarts entre la configuration de référence définie dans l'homologation générique, et les conditions de déploiement.

Audit organisationnel : l'audit organisationnel constitue l'un des deux volets d'un audit SSI. Il vise à évaluer l'environnement et les conditions d'utilisation d'un système d'information. Les conformités organisationnelles portent aussi bien sur la chaîne fonctionnelle SSI que sur les conditions d'emploi du système. Il concerne le GSE, le LSE et la gestion des utilisateurs du système.

Audit technique : il constitue le second volet de l'audit SSI. Il consiste à vérifier que l'architecture et les paramétrages du système d'information entrant dans le champ de l'audit sont conformes aux objectifs et aux exigences de sécurité, définis dans l'ensemble des documentations relatives au système d'information audité, ainsi qu'aux bonnes pratiques. Il couvre le LSE.

Autorité constituée : on appelle autorité constituée les magistrats et hauts fonctionnaires investis d'un pouvoir reconnu (JOS Q. n° 10257). Dans le cadre des audits, c'est le commanditaire.

Champ de l'audit : étendue et limites d'un audit. Le champ décrit généralement les lieux, les unités organisationnelles, les activités et les processus ainsi que la période de temps couverte.

Charte d'audit : description des activités et des dispositions nécessaires pour réaliser un audit (mandats, pouvoirs, attributions, obligations en matière d'établissement de rapports et ressources).

Commanditaire de l'audit : organisme ou personne demandant un audit. Le commanditaire peut être l'audité ou tout autre organisme qui a le droit réglementaire ou contractuel de demander un audit. (Il s'agit de l'organisme qui demande un audit. En général, les demandes émanent des autorités qualifiées (AQ). Cependant, le commanditaire peut être une direction de programme ou de projet d'un système, un responsable de site, un organisme tiers...).

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.

Constats d'audit : résultats de l'évaluation des preuves d'audit recueillies, par rapport aux critères d'audit. Les constats d'audit peuvent indiquer la conformité ou la non-conformité aux critères d'audit ou des opportunités d'amélioration.

Contrôle : il s'agit d'une démarche consistant à réaliser un examen limité et précis afin de vérifier l'application des procédures et de la réglementation. Les contrôles peuvent indifféremment porter sur des systèmes d'information, les sites hôtes ou les organisations concernées.

Critères d'audit : ensemble de politiques, procédures ou exigences déterminées. Les critères d'audit sont la référence vis-à-vis de laquelle les preuves d'audit sont comparées.

Équipe d'audit : un ou plusieurs auditeurs réalisant un audit, assistés, si nécessaire, par des experts techniques. Un auditeur de l'équipe d'audit est nommé responsable de l'équipe d'audit.

L'équipe d'audit peut comprendre des auditeurs en cours de qualification.

Environnement de sécurité : les trois domaines de sécurité en profondeur d'un système d'information et repris par l'application TBHSSI sont les suivants : GSE, LSE et ESE.

ESE (Electronic Security Environment) : inclus dans le LSE, l'environnement de sécurité électronique désigne l'ensemble des moyens techniques de sécurité mis en place au niveau du système.

Expert technique : personne apportant à l'équipe d'audit des connaissances ou une expertise spécifiques.

GSE (Global Security Environment) : l'environnement de sécurité physique global désigne l'environnement physique général dans lequel est situé le système.

Inspection : il s'agit d'une démarche conduite par une entité indépendante de l'autorité responsable du système. Elle consiste essentiellement à réaliser un examen qualitatif et à vérifier l'adéquation des moyens et mesures avec les objectifs de sécurité, la réglementation et les directives en vigueur.

LSE (Local Security Environment) : inclus dans le GSE, l'environnement de sécurité local recouvre l'environnement de sécurité physique, du personnel, documentaire et procédural relevant du domaine de l'autorité d'homologation et qui désigne les locaux dans lesquels sont mise en œuvre les systèmes d'information.

OSSI : officiers de sécurité des systèmes d'information.

Plan d'action : document traduisant la stratégie sous forme d'actions opérationnelles articulées autour d'objectifs, d'étapes à franchir, de délais à ne pas dépasser ainsi que de ressources à répartir entre divers responsables.

Preuve d'audit : enregistrements, énoncés de faits ou autres informations, qui se rapportent aux critères d'audit et sont vérifiables. Les preuves d'audit peuvent être qualitatives ou quantitatives.

Programme d'audit : ensemble d'un ou plusieurs audits planifiés dans un laps de temps et dans un but déterminés. Un programme d'audit comprend toutes les activités nécessaires pour la planification, l'organisation et la réalisation des audits.

RSSI : responsable de sécurité des systèmes d'information.

TBHSSI : application tableau de bord des homologations SSI.

TBHSSI contribue à :

- disposer d'un outil d'aide à la décision pour les responsables de la SSI ;

- l'enregistrement de l'ensemble des systèmes d'information du ministère ;

- améliorer le suivi des travaux afférents aux homologations de sécurité ;

- la dématérialisation et la diffusion contrôlée des documents de sécurité associés à cette homologation (FEROS, VASSI, rapport d'audit, étude SPC, PES, décision d'homologation, etc...), vers les acteurs SSI identifiés pour chaque système ;

- améliorer le suivi des corrections identifiées lors d'audit, de contrôle ou d'inspection ;

- disposer des indicateurs de gestion permettant d'évaluer le niveau de sécurité des organismes et de guider la politique SSI du ministère ;

- favoriser le travail collaboratif entre les acteurs SSI du ministère ;

- améliorer le partage de la connaissance sur les incidents de sécurité du ministère.

Pour le ministre de la défense et par délégation :

L'amiral,
directeur général des systèmes d'informations et de communication,

Christian PÉNILLARD.

---

(1) La présence d'un administrateur est le plus souvent nécessaire afin de permettre à l'auditeur technique de disposer des privilèges suffisants pour réaliser les différentes investigations techniques (système, réseau, bases de données...).

(2) L'audit peut également porter sur un système d'arme.