

Audit SSI



Protocole

- **Audit organisationnel de la SSI**
- **Audit Technique de la sécurité informatique**

Organisme auditée :

Date prévisionnelle de l'audit :

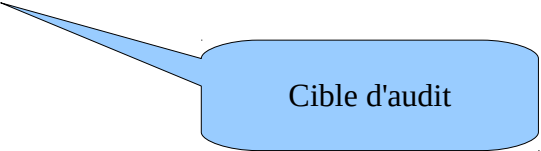
<i>Responsable de l'audit</i>	<i>Responsable administratif d'organisme (ou RSSI par dérogation)</i>

1. Introduction

Le présent document définit les modalités du contrôle de la SSI devant être réalisé au sein de votre organisme.

Le Système d'Information (SI) objet de l'audit est constitué des équipements suivants :

- les postes informatiques reliés ou non aux réseaux locaux,
- les serveurs locaux de ressources (fichiers, impression, travail collaboratif, WEB, etc.),
- les équipements informatiques spécifiques (photocopieurs, imprimantes, badgeuses, automates, etc.).
- Les serveurs offrant les services communs (DMZ)
- etc.



Cible d'audit

2. Objectif de l'audit

L'objectif est de réaliser un état des lieux permettant de connaître les non-conformités par rapport aux règlements, les insuffisances par rapport à l'état de l'art ainsi que les vulnérabilités techniques.

Il consistera essentiellement à apprécier les conditions d'emploi du système cité précédemment de manière à identifier les mesures correctives qu'il serait nécessaire d'y apporter pour traiter des informations sensibles, classifiées de défense ou non.

3. Prestations effectuées et moyen utilisés

L'audit sera réalisé dans les trois domaines complémentaires de la SSI suivants :

- Le domaine organisationnel SSI visant à apprécier les conditions d'emploi et à lister les vulnérabilités globales du système d'information. Les techniques d'interviews seront mises en œuvre.
Le référentiel de contrôle de ce domaine est construit à partir de la réglementation en vigueur et de l'état de l'art applicable au système.
- Le domaine de la sécurité informatique technique permettant de vérifier le paramétrage des fonctions de sécurité et de relever les éventuelles vulnérabilités techniques des équipements. Les investigations seront réalisées au moyen d'outils informatiques spécifiques (cartographie de réseaux, analyse de trames, de services et de configurations, détection de vulnérabilités).

Pour cela, l'équipe d'audit aura besoin :

- De connaître :
 - les informations et les moyens informatiques considérés comme sensibles ;
 - le dossier SSI de l'organisme ;
 - l'inventaire des systèmes informatiques détenus.
- D'obtenir :
 - un accès physique aux réseaux locaux afin de mettre en place les équipements de contrôle ;
 - la documentation descriptive du système d'information et de sa sécurité.

Les résultats des interventions seront formalisés dans divers rapports. Un projet de plan d'amélioration de la sécurité du SI sera inclus dans ces rapports.

4. Modalités d'audit

L'audit organisationnel SSI sera réalisé par

L'audit technique de la Sécurité Informatique sera effectué par

Ces personnes ont signé une attestation de non divulgation d'information elles sont astreintes au secret professionnel en ce qui concerne les informations relatives au résultat du contrôle.

Les travaux à effectuer seront réalisés :

- sur le site audité (interview, investigations techniques, etc.),
- dans les locaux des auditeurs (analyse des documents et des données collectées, rédaction des rapports, etc.).

5. Planning prévisionnel

La durée prévisionnelle du contrôle est de ... heures. La période d'intervention choisie conjointement par les auditeurs et le RSSI du site contrôlé est spécifiée sur la page de garde de ce protocole.

... personnes interviendront sur le site :

- rencontrera des personnes au profil adapté aux thèmes retenus (OSSI, responsable informatique, administrateurs, utilisateurs, ...). Les heures des rencontres seront à préciser en fonction des disponibilités de chacun. Ce contrôle est basé sur les techniques de l'interview dont la durée est de l'ordre d'une heure. Les directives de sécurité définies dans le dossier SSIC de l'organisme serviront de base aux entretiens.
- effectuera les investigations techniques sur les réseaux locaux et les systèmes. La présence d'au moins un administrateur du site est obligatoire afin de prendre en compte les différentes remarques concernant les actions correctives immédiates qui seront demandées.

6. Diffusion des résultats du contrôle

- Un compte-rendu d'audit (technique et environnemental) de la sécurité informatique sera rédigé et envoyé aux destinataires suivants :
- Le délai de réalisation est d'un mois après la fin de la période d'audit
- Ce document portera la mention de manipulation :

7. Engagements réciproques

Le personnel du site audité s'engage :

- à introduire les auditeurs sur le site et à les mettre en relation avec les responsables du système d'information,
- à fournir aux auditeurs toute documentation relative au système d'information et susceptible de les aider dans l'accomplissement de leurs tâches,
- à coopérer par la mise à disposition des installations sous sa responsabilité, dans le cadre de l'installation des équipements de contrôles permettant de réaliser les investigations techniques,
- à participer aux entretiens qui seront demandés par les auditeurs,
- à indiquer les actions mises en place suite aux suggestions d'amélioration préconisées.

Les auditeurs s'engagent :

- à utiliser les outils d'audit dans le seul but de contribuer à la diminution des vulnérabilités majeures (plan d'amélioration),
- à ne pas occasionner de dégradation de service dans la mesure où le SIC est conforme aux règles en vigueur,
- à ne divulguer les résultats de l'audit qu'aux personnes habilitées ayant le besoin d'en connaître.