Afin de permettre le développement et la mise en œuvre de pratiques de sécurité efficaces, une évaluation systématique de la sécurité du système d’information s’impose.

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 ORPSIC des différents organes mettent à jour leur système d’information en procédant à la réaliation d’audits de sécurité SI.

Le présent guide décrit les mesures de sécurité qui doivent être appliquées par les ORPSIC. 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 en vigueur et d’identifier les projets à mettre en œuvre pour s’y conformer.

**Objectif de l’audit :**

* Evaluer le niveau de maturité du SI en terme de sécurité;
* 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) ;

Référentiels relatifs à la sécurité des Systèmes d’Information

* l’Instruction particulière 5617 et ses documents connexes;
* La Directive Nationale de la Sécurité des Systèmes d’Information (DNSSI);
* La suite ISO/CEI 27000 ;
* L’ISO/IEC 27001 ;
* L’ISO/IEC 27002;
* L’ISO/IEC 27005 ;
* L’ISO 27006;
* Publications du NIST;
* CobiT (Control Objectives for Information and Related Technology);
* ITIL (Information Technology Infrastructure Library),

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 sé- curité et à proposer les moyens de correction adaptés. Cette évaluation concerne les domaines suivants :

* Audit Organisationnel et physique
* Audit Technique de Sécurité
* Tests d’intrusion
* Audit Applicatif

**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 poten- tiels. 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.

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 poten- tiels. 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 comporte- ments à adopter pour protéger l’information.

• **Gestion des actifs :**Cette section décrit la nécessité d’inventorier et de classifier les actifs infor- mationnels 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’infor- mation afin d’assurer la protection des systèmes en réseau. Elle couvre éga- lement 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’inté- grité 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 cor- recte et sécurisée des moyens de traitement de l’information (protection contre les logiciels malveillants, maitrise des logiciels en exploitation, et ges- tion 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,développementetmaintenancedessystèmesd’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 ser- vice 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 na- turelles 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.

Il s’agit d’un audit de premier niveau, il ne s’agit pas d’une analyse technique profonde, mais plutôt d’une checklist a renseigner (ANNEXE I) à partir des réponse avancer par le rpsic de lorgane audité. En effet, cette phase repose sur l’utilisa- tion de questionnaires adaptés au contexte de l’organisme audité, des interviews, ainsi que sur l’analyse des ressources et des documents fournis.

**Audit Technique de sécurité**

L’audit technique de sécurité est une évaluation permettant d’analyser en pro- fondeur le système d’information (systèmes, applications, composants et équipe- ments actifs de l’infrastructure réseau, réseaux d’accès interne, réseaux d’inter- connexion, etc.) pour identifier les vulnérabilités techniques éventuelles.

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

* **Audit des vulnérabilités infrastructure et système**
* **Audit d’architecture réseau**
* **Audit de configuration**

**Audit des vulnerabilites**

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 sys- tèmes, 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 vul- nérabilités 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.

**Audir d’architecture:**

Cette activité d’audit a pour vocation d’analyser l’architecture réseau exis- tante 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’intercon- nexion. 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 recommanda- tions en matière de sécurité quant à l’emplacement des actifs réseaux et sécurité

**Audit de configuration**

L’audit de configuration repose sur une évaluation technique de la configura- tion 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.

**Test 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’or- ganisme 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’in- formation aux attaques informatiques provenant de l’intérieur ou de l’extérieur du réseau de l’organisme (ex : réseau internet).

* *Lestestsd’intrusionexternes*:permettentd’évaluerlacapacitéd’unattaquant externe à pénétrer le réseau interne de l’organisme audité ;
* *Les tests d’intrusion internes* : permettent d’évaluer l’impact d’un acte mal- veillant mené de l’intérieur du réseau de l’organisme audité.

Généralement, ces tests s’effectuent selon les étapes suivantes : • Reconnaissance du périmètre à auditer ;

• Recherchedesvulnérabilités;  
• Mise en œuvre des attaques (exploits) ;  
• Mesuredel’impact;  
• Proposition de recommandations et correctifs.

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

* *Approche en boite noir* : Le testeur ne dispose d’aucune connaissance préa-

lable de l’environnement avant l’attaque ;

* *Approcheenboitegrise*:letesteurdisposedeconnaissancespartiellesdel’en- vironnement à auditer ;

*Approche en boite 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 en- vironnement 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 environne- ment de test ou pré-production.

**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.

**deroulement de l’audit**

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

**Phase de déclenchement de l’audit**

Au debut de chaque annee l’ORPSIC établi un planing de passage aux unites relevant de son organe. Pour chaque Audit, Une équipe doit être formée en fonction du périmètre de l’audit et en prenant en considération les compétences nécessaires pour atteindre les objectifs.

Aisin 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
* 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 profes- sionnel face aux situations de quotidien ;
* Scénarios de tests techniques.

**Phase d’exécution de l’audit et analyse des constats**

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’orga- nisme audité. Des immersions (des observations d’activités) sont recom- mandées si les informations recueillies lors des entretiens sont insuffisantes. Si nécessaire l’auditeur peut demander des preuves appuyant les informa- tions fournies par l’audité.
* L’auditeurprocèdeàuneanalysed’écartentrelespreuvesfourniesetlescri- tères d’audit afin de générer ses constats. Ces constats sont soit une confor- mité soit une non-conformité aux critères d’audit.
* Leresponsabled’auditdoitimmédiatementteniraucourantl’auditédetout 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.
* Lecommanditaired’auditdoiteffectuerrégulièrementlepointaveclepres- tataire d’audit et l’organisme audité afin de s’informer de l’état d’avance- ment de l’audit et des différents obstacles rencontrés.

Les documents résultant de la phase d’exécution doivent être soigneusement ar- chivés. 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 essentielle- ment:

⋄ Les constats des auditeurs ;  
⋄ Lesrecommandations;  
⋄ 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.
* Lesrésultatsdesteststechniquesd’auditsontcomposésprincipalementde:
  + ⋄  La liste des vulnérabilités (réseaux, systèmes, applicatives, etc.) ;
  + ⋄  La liste des anomalies de configuration des équipements (configuration

des firewalls et des équipements réseaux).

1. Les enregistrements de la phase d’exécution de l’audit doivent être évalués, ana- lysés 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 ma- nière synthétique ;
   * Validation des conclusions d’audit ;
   * Préparationdesrecommandations;
   * Définition des modalités de suivi d’audit.

**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 éven- tuelles questions qui peuvent se poser. Il convient que l’audité et le commandi- taire d’audit y prennent part. Les constats et les conclusions d’audit présentés doivent être bien compris et acceptés par l’audité.

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.)