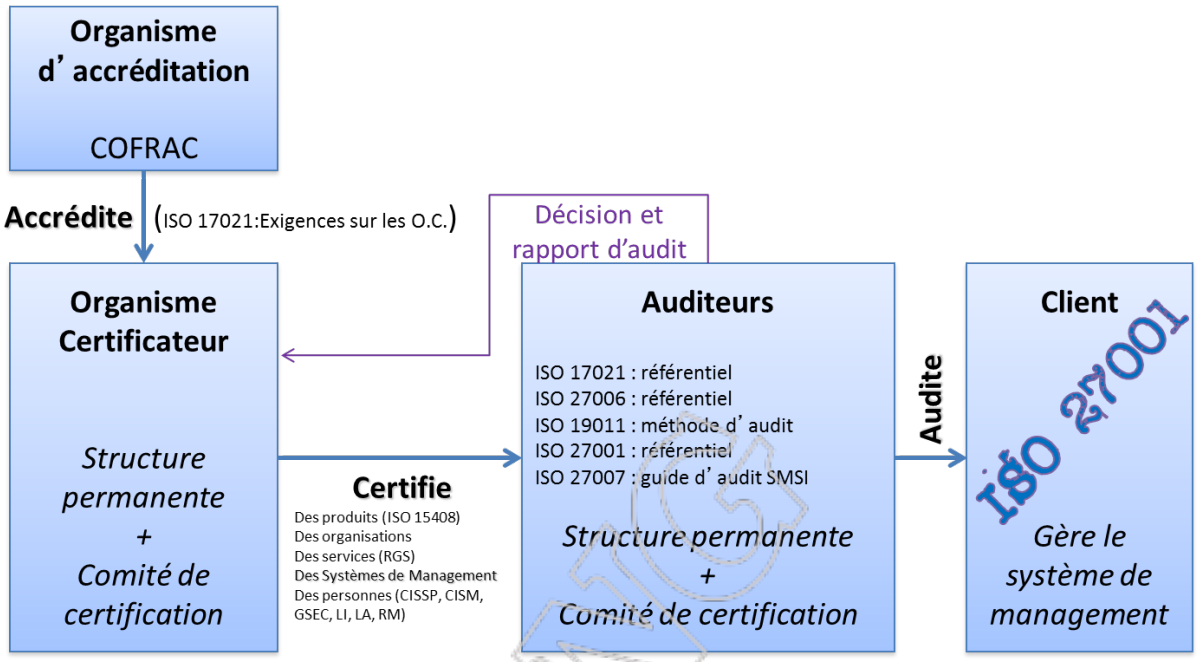
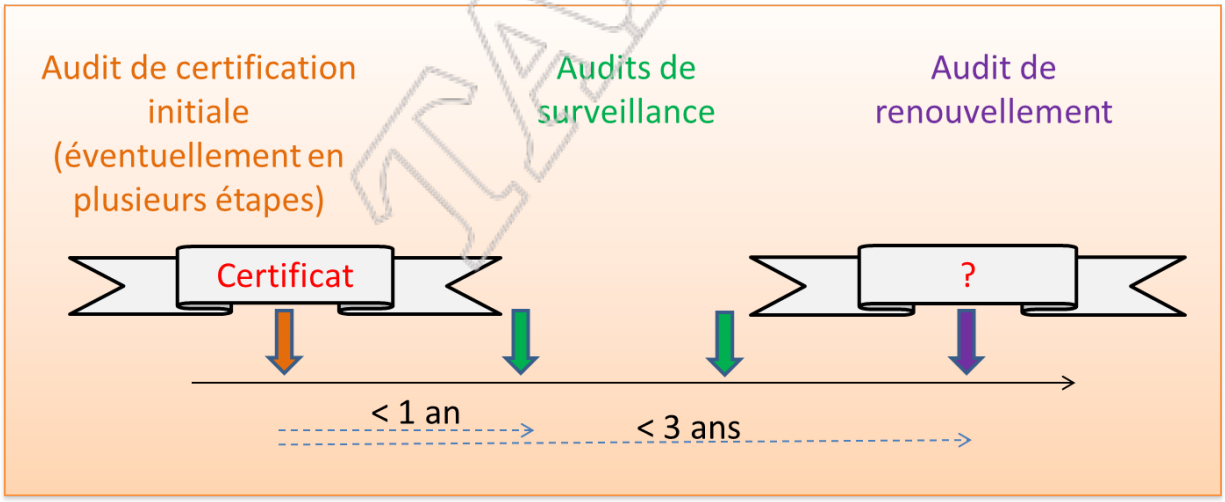
Table des matières

La norme ISO 27001

Processus de certification



Calendrier de certification



La famille de normes ISO-2700x

Description générale

Famille de standards pour les Systèmes de Management de la Sécurité de l'Information

C'est un ensemble de normes décrivant les bonnes pratiques en management de la sécurité de l'information (SMSI).

Ensemble de mesures techniques et organisationnelles permettant d'atteindre un objectif de sécurité et une fois atteint de s'y maintenir (ou de le modifier).

27000	Définitions

27001	Implémentation d'un SMSI
27002	Liste de mesures de sécurité (ex. 17799)
27003	Guide d'implémentation
27004	Normes de mesures du management de la sécurité
27005	Gestion des risques
27006	Guide de processus de certification et d'enregistrement
27007	Audit des SMSI

ISO 27000 – Quelques définition

Sécurité de l'information	Protection de la **confidentialité**, de l'**intégrité**, et de la **disponibilité** de l'information. D'autres propriétés telles que la preuve, la traçabilité, l'authenticité, l'imputabilité, la non-répudiation et la fiabilité peuvent aussi être concernées.
SMSI	Partie du Système de management global, basée sur une approche du risque lié à l'activité, visant à établir, mettre en œuvre, exploiter, surveiller, réexaminer, tenir à jour et améliorer la sécurité de l'information
Disponibilité	Propriété d'être accessible et utilisable à la demande par une entité autorisée
Intégrité	Propriété de protection de l'exactitude et de la complétude des actifs.
Confidentialité	Propriété selon laquelle l'information n'est pas rendue disponible ou divulguée à des personnes, des entités, des processus
Actifs	Tout élément représentant une valeur pour l'organisation (information, logiciels, actifs physiques, services, personnel, savoir-faire, réputation, image, …)
Menace	Cause potentielle d'un incident indésirable, qui peut nuire à un système ou une organisation
Vulnérabilité	Faille dans un actif ou dans une mesure de sécurité qui peut être exploitée par une ou plusieurs menaces.
Vraisemblance	Possibilité que quelque chose se produise
Risque	Effet (⇔ écart par rapport à des attentes) de l'incertitude sur la réalisation des objectifs.

ISO 27001 – Quelques grands principes

Contraintes obligatoires
(Appelées « clauses »)

- Définition du SMSI (enjeux, périmètre, objectifs, acteurs)
- Responsabilité de la Direction (de l'organisation)
- Audits internes du SMSI
- Revue de Direction (du SMSI)
- Amélioration continue du SMSI

Principe de l'amélioration continue

(Approche « processus »)

- BUILD /Création du SMSI
- BUILD /Mise en œuvre du SMSI
- RUN / Surveillance du SMSI
- RUN / Mise à jour du SMSI

Plan de l'ISO-27001:2013

Contexte de l'organisation

- Besoins et attentes des parties intéressées
- Domaine d'application du SMSI

Leadership

- Engagement de la Direction
- Politique de sécurité de l'information (adaptée, objectifs, engagement)
- Rôles et responsabilités des acteurs

Planification

- Fixation des objectifs conformes au contexte
- Appréciation et traitement des risques
- Plan pour atteindre les objectifs fixés

Support

- Moyens : ressources, compétences, sensibilisation, communication, documentation

Fonctionnement

- Planification des contrôles
- Ré évaluation et traitement des risques

Evaluation et performance

- Suivi des indicateurs
- Audits
- Revue de Direction

Amélioration

- Correction des non conformités
- Amélioration continue

Le PDCA ou l'Amélioration continue, fondement de l'ISO-27001

Plan : identifier les risques et définir les mesures

- Source de la mesure : déclaration d'applicabilité et analyse de risques

- Procédures
- Identification des propriétaires des risques et des acteurs de la mise en œuvre

Do : mettre en application les mesures choisies

- Vérification de la mise en œuvre in situ, par interviews des experts techniques
- Mise en situation des gens et vérification de l'application des procédures et règles fixées

Check : contrôler et maintenir le système

- Vérification de l'application des procédures de mesure de l'efficacité des mesures de sécurité choisies
- Revue des indicateurs
- Vérification des CR des revues de Direction

Act : améliorer continuellement l'activité

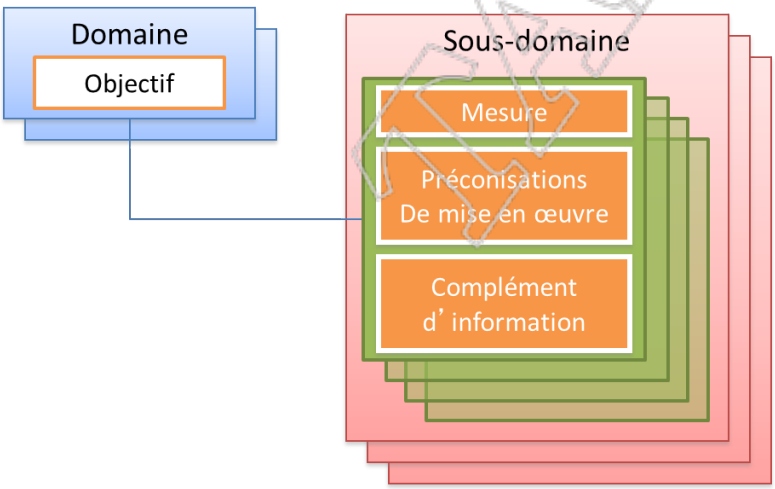
- Vérification de la mise en œuvre des plans d'action définis dans les CR des revues de direction
- Vérification de la mise en œuvre des mesures de sécurité choisies

ISO 27002 – Un catalogue de mesures

ISO 27002 – Description générale

Elle liste les mesures de sécurité applicables pour réduire les risques (référence), selon :

- 14 domaines
- 35 objectifs de sécurité
- 114 mesures organisationnelles et techniques de sécurité



ISO 27002 – Des domaines qui couvrent bien les besoins

1. Politique de sécurité de l'Information

Apporter à la SI une orientation et un soutien de la part de la Direction, conformément aux exigences métier et à la loi

2. Organisation de la sécurité de l'information

Etablir le cadre de gestion pour engager puis vérifier la mise en œuvre et le fonctionnement de la SI au sein de l'organisation

3. Sécurité des ressources humaines
S'assurer que les salariés et les contractants comprennent leurs responsabilités et qu'ils sont compétents pour leur poste

4. Gestion des actifs
Identifier les actifs de l'organisation et définir les responsabilités appropriées en matière de protection

5. Contrôle des accès
Limiter l'accès à l'information et aux moyens de traitement de l'information

6. Cryptographie
Garantir l'utilisation correcte et efficace de la cryptographie pour protéger la confidentialité et l'intégrité de l'information

7. Sécurité physique et environnementale
Empêcher tout accès physique non autorisé, tout dommage ou intrusion portant sur l'information et les moyens de traitement de l'information de l'organisation

8. Sécurité liée à l'exploitation
S'assurer de l'exploitation correcte et sécurisée des moyens de traitement de l'information

9. Sécurité des communications
Garantir la protection de l'information sur les réseaux et des moyens de traitement de l'information sur lesquels elle s'appuie

10. Acquisition, développement et maintenance des systèmes d'information
Veiller à ce que la SI fasse partie intégrante des systèmes d'information tout au long de leur cycle de vie.

11. Relation avec les fournisseurs
Garantir la protection des actifs de l'organisation accessibles aux fournisseurs

12. Gestion des incidents liés à la sécurité de l'information
Garantir une méthode cohérente et efficace de getsion des incidents liés à la sécurité de l'information, incluant la communication des évènements et des failles liés à la sécurité.

13. Aspects de la sécurité de l'information dans la gestion de la continuité de l'activité
La continuité de la sécurité doit faire partie intégrante des systèmes de gestion de la continuité de l'activité.

14. Conformité
Eviter toute violation des obligations légales, statutaires, réglementaires ou contractuelles relatives à la sécurité de l'information, éviter toute violation des exigences de sécurité.

ISO 27002 – Un exemple de mesures

Organisation de la sécurité de l'information
| Organisation interne
| | Fonctions et responsabilités liées à la SI

Le **domaine** est découpé en **sous-domaines**, chacun redécoupé en **thèmes**. Chaque thème contient une ou plusieurs mesures

| | Séparation des tâches
| | Relation avec les autorités
| | Relation avec des groupes de travail spécialisés
| | La sécurité de l'information dans la gestion de projet
|Appareils mobiles et télétravail
| | Politique en matière d'appareils mobiles
| | Télétravail

Mesure

Il convient de traiter la SI dans la gestion des projets, quel que soit le projet concerné

Préconisations

- Les objectifs de sécurité doivent être intégrés aux objectifs du projet
- Une appréciation des risques doit être effectuée au début du projet et les mesures à mettre en œuvre identifiées
- La SI doit être intégré à toutes les phases de la méthodologie de projet appliquée
- Les incidences sur la SI doivent être revues régulièrement
- Des responsabilités en matière de SI doivent être déterminées et attribuées

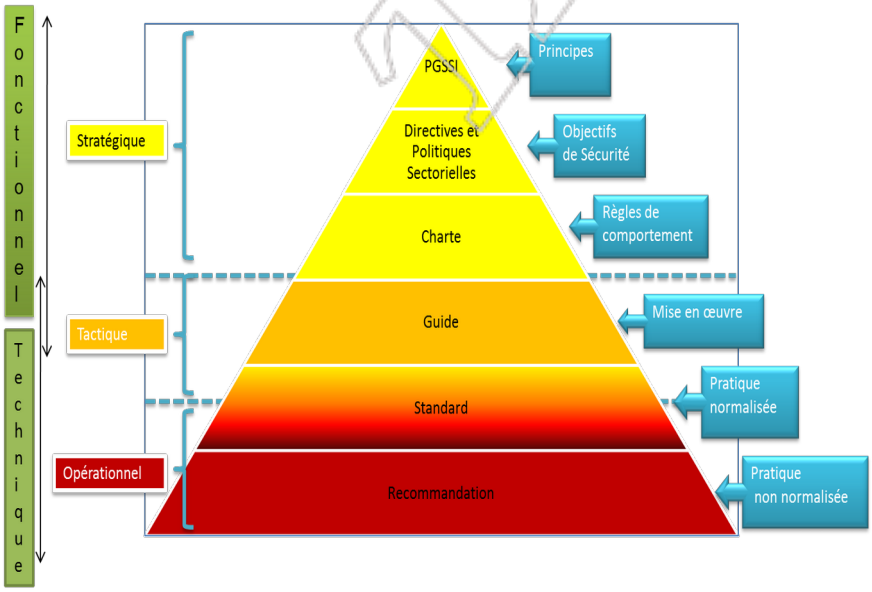
Corpus documentaire de sécurité de l'information

Général

Pour que la sécurité puisse être appliquée correctement dans l'Entreprise, il est nécessaire d'en formaliser les règles.

Le corpus documentaire comprend généralement plusieurs niveaux de documents.

Illustration d'une hiérarchie possible de documents



Des documents d'ordre « stratégique »

Une Politique Générale de Sécurité

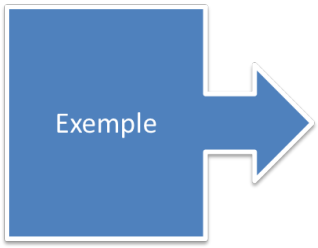
Equivalent de l'ISO 27001, elle fixe la démarche et l'organisation en place

Des Politiques Locales de Sécurité

Equivalentes de l'ISO 27002, elles fixent l'ensemble des mesures applicables sur leur périmètre d'application

Des Directives sectorielles

Elles fixent les grandes règles, organisationnelles et techniques, applicables sur des sujets particuliers.



- Gestion des **Audits**
- Gestion de l'**Authentification**
- Gestion des **Habilitations**
- Gestion des **Incidents** de Sécurité
- Gestion des **Risques**
- Gestion des **Tiers**
- Sécurité dans les **Projets**
- Sécurité des **Réseaux**
- Sécurité des **Smartphones**
- Sécurité des **Objets Communicants**
- Sécurité des **Services de Paiement**
- Lutte contre la **Fraude**
- Gestion de la **Preuve**
- Sécurité des **Serveurs**
- Gestion de la **Capacité**
- Gestion des noms de **Domaine**
- (**Conformité** Légale et Réglementaire)

Des documents d'ordre « tactiques »

Des normes et standards

Ces documents vont standardiser des méthodes (par exemple l'analyse de risques), ou des façons de travailler.

Des guides

Ils vont préciser les modalités de mise en œuvre de certaines règles des politiques (générale et locales)

Des documents d'ordre « opérationnel »

Des chartes d'utilisation

Qui vont préciser les règles applicables pour l'usage ou l'accès à un environnement précis (exemple : charte des administrateurs, charte informatique)

Des recommandations, des procédures

Qui expliquent comment mettre en œuvre quelque chose de manière sécurisée

La PGSI

Description générale

Document fondateur, signé par la direction générale

Elle s'appuie sur les fondamentaux de l'entreprise (son organisation, ses enjeux métiers…). Elle vise à traiter en priorité les risques les plus critiques au regard des enjeux métiers. Elle accompagne l'augmentation progressive du niveau de sécurité des SI en intégrant le principe d'amélioration continue.

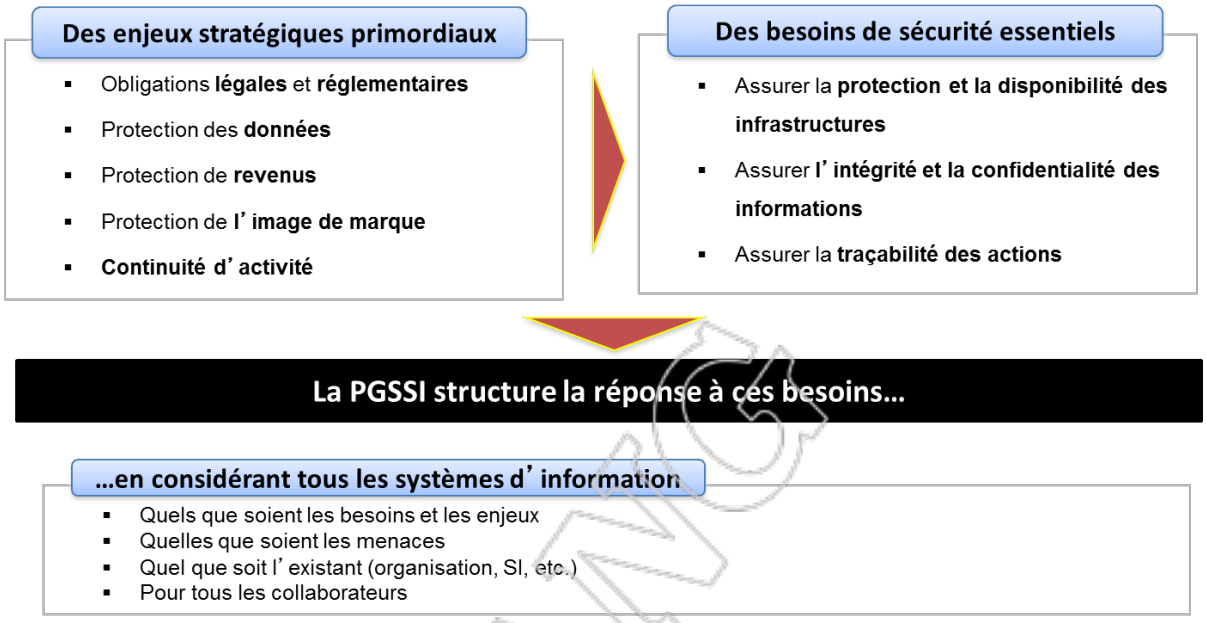
La PGSSI décrit les principes, l'organisation et les moyens qu'une organisation souhaite mettre en œuvre pour assurer la sécurité de ses SI et ainsi répondre aux enjeux de l'entreprise.

Les points généraux qui y sont abordés sont ensuite déclinés en des documents plus opérationnels (charte, guide, standard,…).

Ces documents sont différenciés par les enjeux qu'ils visent à couvrir ou les technologies concernées.

La PGSI doit d'abord se poser la question du contexte et des enjeux. Le contexte et les enjeux permettent de définir les besoins de sécurité. Enfin, le document va devoir expliquer comment répondre à ces besoins, d'un point de vue :

- De la démarche à adopter
- De l'organisation
- Des organes de contrôle



Un exemple de PGSI : la PSSIE

Le plan

Première partie : instruction

- Objet, champ d'application, date d'entrée en vigueur
- Dispositions transitoire, formation des agents
- Pilotage et évolutions de la Politique
- Organisation de l'Etat pour la mise en application
- Mise en application, contrôle et suivi de l'application
- Traitement des incidents et gestion de crise

Deuxième partie : objectifs et règles

- Politique, organisation, gouvernance
- Ressources humaines
- Gestion des biens
- Intégration de la SSI dans le cycle de vie des systèmes d'information
- Sécurité physique
- Sécurité des réseaux
- Architecture des SI
- Exploitation des SI
- Sécurité du poste de travail
- Sécurité du développement des systèmes
- Traitement des incidents

- Continuité d'activité
- Conformité, audit, inspection, contrôle

Première partie : instruction

La présente instruction fixe les conditions de mise en œuvre de la politique de sécurité des systèmes d'information de l'État(PSSIE).

L'ANSSI assure la fonction d'autorité nationale de sécurité et de défense des systèmes d'information, conformément au décret n° 2009-834 du 7 juillet 2009. A ce titre, et dans le cadre des orientations fixées par le Premier ministre, l'ANSSI décide des mesures que l'État met en œuvre pour répondre aux crises affectant ou menaçant la sécurité des systèmes d'information des autorités publiques et des opérateurs d'importance vitale. Elle coordonne l'action gouvernementale en la matière.

Dans le cadre de ses missions, l'ANSSI :

- Elabore les mesures de protection des SI proposées au Premier ministre et veille à leur application ;
- Mène des inspections des systèmes d'information ;
- Etablit et tient à jour en permanence la situation des SI de l'État, en liaison avec les chaînes fonctionnelles SSI et les directions des systèmes d'information (DSI) des ministères ;
- Met en œuvre un centre de détection chargé de la surveillance permanente des réseaux ;
- Assure des échanges d'informations avec les constructeurs de matériels, les éditeurs de logiciels ainsi que les opérateurs de communications électroniques et les opérateurs d'importance vitale, afin de mieux comprendre les mécanismes d'attaques, d'étudier les parades possibles et de favoriser la diffusion rapide des correctifs de sécurité.

Les 10 principes stratégiques

P1. Lorsque la maîtrise de ses systèmes d'information l'exige, l'administration fait appel à des **opérateurs et des prestataires de confiance**.

P2. Tout système d'information de l'État doit faire l'objet d'une **analyse de risques** permettant une prise en compte préventive de sa sécurité, adaptée aux enjeux du système considéré. Cette analyse s'inscrit dans une démarche d'amélioration continue de la sécurité du système, pendant toute sa durée de vie. Cette démarche doit également permettre de maintenir à jour une **cartographie précise des systèmes d'information** en service.

P3. Les **moyens humains et financiers** consacrés à la sécurité des systèmes d'information de l'État doivent être planifiés, quantifiés et identifiés au sein des ressources globales des systèmes d'information.

P4. Des moyens d'**authentification forte** des agents de l'État sur les systèmes d'information doivent être mis en place. L'usage d'une carte à puce doit être privilégié.

P5. Les opérations de gestion et d'administration des systèmes d'information de l'État doivent être tracées et contrôlées.

P6. La protection des systèmes d'information doit être assurée par l'**application rigoureuse de règles précises**. Ces règles font l'objet de la présente PSSIE.

P7. Chaque **agent de l'État**, en tant qu'utilisateur d'un système d'information, doit être **informé de ses droits et devoirs** mais également **formé et sensibilisé à la cyber sécurité**. Les mesures techniques mises en place par l'État dans ce domaine doivent être connues de tous.

P8. Les administrateurs des systèmes d'information doivent appliquer, après formation, les règles élémentaires d'hygiène informatique.

P9. Les **produits et services** acquis par les administrations et destinés à assurer la sécurité des systèmes d'information de l'État doivent faire l'**objet d'une évaluation et d'une attestation préalable de leur niveau de sécurité**, selon une procédure reconnue par l'ANSSI («labellisation»).

P10. Les informations de l'administration considérées comme sensibles, en raison de leurs besoins en confidentialité, intégrité ou disponibilité, sont **hébergées sur le territoire national**.

Deuxième partie : objectifs et règles

Politique, organisation, gouvernance

Mettre en place une organisation adéquate, garantissant la prise en compte préventive et réactive de la sécurité.

- Organisation de la SSI
- Acteurs de la SSI
- Responsabilités internes et vis à vis des tiers
- PSSI ministérielle
- Application des mesures de sécurité au sein de l'entité

Ressources humaines

Faire des personnes les maillons forts des SI de l'État

- Utilisateurs : charte d'utilisation
- Personnel permanent,
- Mouvements,
- Personnel non-permanent

Gestion des biens

Tenir à jour une cartographie détaillée et complète des SI

- Inventaire des ressources SI
- Cartographie

Qualifier l'information de façon à adapter les mesures de protection

- Qualification des informations
- Protection des informations

Intégration de la SSI dans le cycle de vie des systèmes d'information

Apprécier, traiter, et communiquer sur les risques relatifs à la sécurité des systèmes d'information

- Gestion des risques et homologation des SI

Gérer dynamiquement les mesures de protection, tout au long de la vie du SI

- Intégration de la sécurité dans les projets
- Mise en œuvre au quotidien de la SSI

- Créer un tableau de bord de la SSI

Utiliser des produits et services dont la sécurité est évaluée et attestée selon des procédures reconnues par l'ANSSI, afin de renforcer la protection des SI

Veiller aux exigences de sécurité lorsqu'il est fait appel à de la prestation par des tiers

Sécurité physique

Inscrire la sécurisation physique des SI dans la sécurisation physique des locaux et dans les processus associés.

- Règles générales
- Règles s'appliquant aux zones d'accueil du public
- Règles s'appliquant aux locaux techniques

Dimensionner les protections physiques des centres informatiques en fonction des enjeux liés à la concentration des moyens et données abrités

- Règles générales
- Règles s'appliquant aux zones internes et restreintes
- Règles de sécurité s'appliquant aux salles informatiques et aux locaux techniques

Traiter de manière globale la sécurité des systèmes d'information et de communication qui assurent la sûreté d'un site

Sécurité des réseaux

Sécurité des réseaux nationaux

- Systèmes autorisés sur le réseau
- Interconnexions avec des réseaux externes
- Filtrage réseau pour les flux sortants et entrants
- Protection des informations

Sécurité des réseaux locaux

- Cloisonner le SI en sous-réseaux de niveaux de sécurité homogènes
- Interconnexion des sites géographiques locaux d'une entité
- Cloisonnement des ressources en cas de partage de locaux

Sécurité des mécanismes de commutation et de routage

- Implanter des mécanismes de protection contre les attaques sur les couches basses
- Surveiller les annonces de routage
- Configurer le protocole IGP de manière sécurisée
- Sécuriser les sessions EGP
- Modifier systématiquement les éléments d'authentification par défaut des équipements et services
- Durcir les configurations des équipements de réseaux

Accès spécifiques

Sécurité des réseaux sans fil

Sécurisation des mécanismes de commutation et de routage

Cartographie réseau

Architecture des SI

Appliquer les principes de défense en profondeur à l'architecture matérielle et logicielle des centres informatiques

- Principes d'architecture de la zone d'hébergement
- Architecture de stockage et de **sauvegarde**
- Passerelle Internet

Exploitation des SI

Protection des informations sensibles

Sécurité des ressources informatiques

Gestion des autorisations et contrôle d'accès logique aux ressources

- Contrôle des accès logiques
- Processus d'autorisation
- Gestion des authentifiants
- Gestion des authentifiants d'administration

Exploitation sécurisée des ressources informatiques

- Administration des systèmes
- Envoi en maintenance et mise au rebut
- Lutte contre les codes malveillants
- Mise à jour des systèmes et des logiciels
- Journalisation

Protection des informations sensibles

Sécurité des ressources informatiques

Gestion des autorisations et contrôle d'accès logique aux ressources

Exploitation sécurisée des ressources informatiques

Défense des SI

- Gestion des matériels informatiques fournis à l'utilisateur
- Nomadisme
- Sécurisation des imprimantes et copieurs multifonctions manipulant des informations sensibles

Exploitation des centres informatiques

- Sécurité des ressources informatiques
    - Systèmes d'exploitation
    - Logiciels en Tiers Présentation / en Tiers Application / en Tiers Données
    - Passerelle d'échange de fichiers
    - Messagerie technique
    - Filtrage des flux applicatifs
    - Flux d'administration
    - Service DNS

- Effacement / Destruction de supports
- Traçabilité, Imputabilité
- Supervision
- Accès aux périphériques amovibles
- Accès aux réseaux
- Audits et contrôles

Sécurité du poste de travail

Durcir les configurations des postes de travail en protégeant les utilisateurs

- Mise à disposition du poste
- Sécurité des postes de travail
- Réaffectation du poste et récupération d'informations
- Gestion des privilèges sur les postes de travail
- Protection des informations
- Nomadisme

Paramétrer les imprimantes et copieurs multifonctions afin de diminuer leur surface d'attaque

- Durcissement des imprimantes et copieurs mft
- Sécurisation de la fonction de numérisation

Sécurisation de la téléphonie

- Sécuriser la configuration des autocommutateurs
- Codes d'accès téléphoniques
- Limiter l'utilisation du DECT

Contrôle de conformité

- Utiliser des outils de vérification automatique de la conformité

Sécurité du développement des systèmes

Reconnaître la sécurité comme une fonction essentielle, et la prendre en compte dès la conception des projets

- intégrer la sécurité dans les développements locaux.
- intégrer des clauses SSI dans les contrats de sous-traitance de développement informatique

Mener les développements logiciels selon une méthodologie de sécurisation du code produit

- Limiter les fuites d'information
- Réduire l'adhérence des applications à des produits ou technologies spécifiques
- Utiliser des outils de vérification automatique de la conformité
- Instaurer des critères de développement sécurisé
- Intégrer la sécurité dans le cycle de vie logiciel
- Améliorer la prise en compte de la sécurité dans les développements Web
- Calculer les empreintes de mots de passe de manière sécurisée.

Accompagner le développement sécurisé d'applications à risques par des contre-mesures minimisant l'impact d'attaques nouvelles

- Mettre en œuvre des fonctionnalités de filtrage applicatif pour les applications à risque

Traitement des incidents

Partager l'information (alertes, incidents) dans le respect des règles de prudence et mutualiser les opérations de remise en état, de façon à lutter efficacement contre les attaques

- Traitement des alertes de sécurité émises par les instances nationales (ANSSI)
    - Mobilisation en cas d'alerte
- Remontée des incidents de sécurité rencontrés
    - Qualification et traitement des incidents
    - Remontée des incidents

Continuité d'activité

Se doter de plans de continuité d'activité, et les tester

- Définition du plan de continuité d'activité des systèmes d'information d'une entité
- Mise en œuvre du plan local de continuité d'activité des systèmes d'information
    - Suivi de la mise en œuvre du plan de continuité d'activité local des Systèmes d'Information (PCA des SI)
    - Mise en œuvre des dispositifs techniques et des procédures opérationnelles
    - Protection de la disponibilité des sauvegardes
    - Protection de la confidentialité des sauvegardes

Se doter de plans de continuité d'activité, et les tester

- Maintien en conditions opérationnelles du plan local de continuité d'activité des Systèmes d'Information
    - Exercice régulier du plan local de continuité d'activité des systèmes d'information
    - Mise à jour du plan local de continuité d'activité des systèmes d'information

Conformité, audit, inspection, contrôle

Effectuer des contrôles (audits, inspections) et des exercices réguliers de façon à mesurer les progrès accomplis et corriger les manquements

- Contrôles locaux
- Bilan annuel

Le référentiel général de sécurité

Présentation générale

Le Référentiel général de sécurité (RGS) a pour objet le renforcement de la confiance des usagers dans les services électroniques mis à disposition par les autorités administratives, et s'impose ainsi à elles comme un cadre contraignant tout en étant adaptable et adapté aux enjeux et besoins de tout type d'autorité administrative.

Le RGS propose :

- Une méthodologie orientée autour de la responsabilisation des autorités vis-à-vis de leurs SI à travers la démarche d'homologation ;
- Des règles et bonnes pratiques que doivent mettre en œuvre les administrations lorsqu'elles recourent à des prestations spécifiques : certification et horodatage électroniques, audit de sécurité.

Il comprend les règles permettant aux autorités administratives de garantir aux citoyens et aux autres administrations un niveau de sécurité de leurs systèmes d'information adapté aux enjeux et risques liés à la cybersécurité.

Le RGS intègre les principes et règles liées à :

- La description des étapes de la mise en conformité ;
- La cryptologie et à la protection des échanges électroniques ;
- La gestion des accusés d'enregistrement et des accusés de réception ;
- La qualification des produits de sécurité et des prestataires de services de confiance ;
- La validation des certificats par l'État.

Qualification des produits de sécurité

La qualification de produits de sécurité prévoit trois niveaux de qualification : élémentaire (CSPN), standard et renforcée (**Critères communs**).

Un produit de sécurité est **qualifié** s'il a fait l'objet d'une attestation de qualification (instruction et délivrance des attestations par l'ANSSI), et d'un maintien de conditions de sécurité conforme aux procédures décrites.

La **procédure de qualification** repose sur une certification préalable (*certification de sécurité de premier niveau des produits des technologies de l'information* – CSPN Ti).

La certification Critères Communs

Elle s'appuie sur des travaux d'évaluation réalisés par des **laboratoires agréés** par le Premier ministre et accrédités par le Comité français d'accréditation (COFRAC) selon la norme NF EN ISO/CEI 17025.

Ces laboratoires sont communément appelés *Centres d'évaluation de la sécurité des technologies de l'information* (***CESTI***).

Les évaluations sont menées conformément à des normes ou standards spécifiés par l'ANSSI.

Les certificats émis par l'ANSSI par délégation du Premier ministre attestent que les produits certifiés sont conformes à une spécification technique appelée « cible de sécurité ».

Cette « *cible de sécurité* » peut elle-même être certifiée conforme à un cahier des charges appelé « *profil de protection* ».

Ce profil permet d'exprimer des exigences de haut niveau et peut être partagé par une communauté d'intérêts telles que la communauté bancaire, celle de la santé ou du transport….

Le certificat atteste, au jour de sa signature, de la conformité d'une version précise d'un produit ou d'un système aux exigences listées dans sa cible de sécurité.

Pour prolonger dans le temps la confiance dans cette conformité ou faciliter la certification des évolutions d'un produit précédemment certifié, le centre de certification propose des solutions de maintenance de certificats.

Le Guide d'hygiène informatique

Plan général

Le guide propose 42 règles de sécurité simples à comprendre, distribuées selon 10 principes :

I. Sensibiliser et former
II. Connaître le système d'information
III. Authentifier et contrôler les accès
IV. Sécuriser les postes
V. Sécuriser le réseau
VI. Sécuriser l'administration
VII. Gérer le nomadisme
VIII. Maintenir le système d'information à jour
IX. Superviser, auditer, réagir
X. Pour aller plus loin

Sensibiliser et former

- Former les équipes opérationnelles à la sécurité des systèmes d'information
- Sensibiliser les utilisateurs aux bonnes pratiques élémentaires de sécurité informatique
- Maîtriser les risques de l'infogérance

Connaître le système d'information

- Identifier les informations et serveurs les plus sensibles et maintenir un schéma du réseau
- Disposer d'un inventaire exhaustif des comptes privilégiés et le maintenir à jour
- Organiser les procédures d'arrivée, de départ et de changement de fonction des utilisateurs
- Autoriser la connexion au réseau de l'entité aux seuls équipements maîtrisés

Authentifier et contrôler les accès

- Identifier nommément chaque personne accédant au système et distinguer les rôles utilisateur/administrateur
- Attribuer les bons droits sur les ressources sensibles du système d'information
- Définir et vérifier des règles de choix et de dimensionnement des mots de passe
- Protéger mes mots de passe stockés sur les systèmes
- Changer les éléments d'authentification par défaut sur les équipements et services
- Privilégier lorsque c'est possible une authentification forte

Sécuriser les postes

- Mettre en place un niveau de sécurité minimal sur l'ensemble du parc informatique
- Se protéger des menaces relatives à l'utilisation de supports amovibles
- Utiliser un outil de gestion centralisé afin d'homogénéiser les politiques de sécurité
- Activer et configurer le pare-feu local des postes de travail
- Chiffrer les données sensibles transmises par voie Internet

Sécuriser le réseau

- Segmenter le réseau et mettre en place un cloisonnement entre ces zones
- S'assurer de la sécurité des réseaux d'accès Wifi et de la séparation des usages
- Utiliser des protocoles réseaux sécurisés dès qu'ils existent
- Mettre en place une passerelle d'accès sécurisé à Internet
- Cloisonner les services visibles depuis internet du reste du système d'information
- Protéger sa messagerie professionnelle
- Sécuriser les interconnexions réseau dédiées avec les partenaires
- Contrôler et protéger l'accès aux salles serveurs et aux locaux techniques

Sécuriser l'administration

- Interdire l'accès à Internet depuis les postes ou serveurs utilisés pour l'administration des SI
- Utiliser un réseau dédié et cloisonné pour l'administration du système d'information
- Limiter au strict besoin opérationnel les droits d'administration sur les postes de travail

Gérer le nomadisme

- Prendre des mesures de sécurisation physique des terminaux nomades
- Chiffrer les données sensibles, en particulier sur le matériel potentiellement perdable
- Sécuriser la connexion réseau des postes utilisés en situation de nomadisme
- Adopter des politiques de sécurité dédiées aux terminaux mobiles

Maintenir le système d'information à jour

- Définir une politique de mise à jour des composants du système d'information
- Anticiper la fin de la maintenance des logiciels et systèmes et limiter les adhérences logicielles

Superviser, auditer, réagir

- Activer et configurer les journaux des composants les plus importants
- Définir et appliquer une politique de sauvegarde des composants critiques
- Procéder à des contrôles et des audits de sécurité réguliers puis appliquer les actions correctives associées
- Désigner un référent en sécurité des systèmes d'information et le faire connaître auprès du personnel
- Définir une procédure de gestion des incidents de sécurité

Pour aller plus loin

- Mener une analyse de risques fonctionnelle
- Privilégier l'usage de produits et de services qualifiés par l'ANSSI

Le Framework NIST

Ce référentiel américain, couvre un peu tout ce que couvre l'ISO 27001 et l'ISO 27002. On y retrouve des mesures liées à la gouvernance, mais aussi des mesures techniques.

Le NIST propose d'ailleurs des associations entre les différents référentiels (dont l'ISO 27k, mais pas seulement) et sa propre liste de mesures.

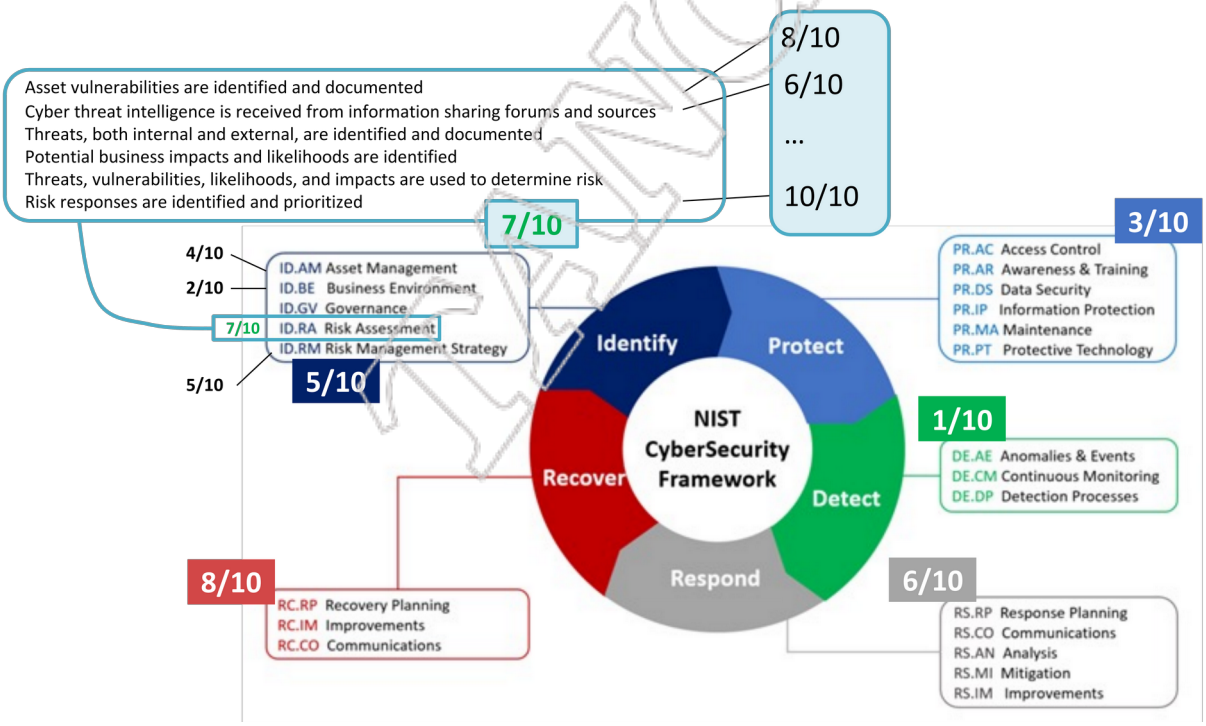
La gestion de la sécurité est découpée en 5 axes présentés sur une roue. Pour chacun de ces axes, sont définies des thématiques, auxquelles sont ensuite associées des mesures.

Les organisations américaines l'utilisent en mettant une note qui correspond au niveau de couverture de chacune des mesures, ce qui permet d'assigner une note à chacune des thématiques, et donc aux 5 axes.

Ces tableaux de notes sont partagés avec la Direction Générale comme un tableau de bord, duquel peuvent se déduire des points d'amélioration (là où les notes ne sont pas bonnes), et donc un plan stratégique.

En revanche, et bien que la liste des mesures inclue certaines mesures de gouvernance de sécurité dont le « risk assessment », on constate qu'en pratique l'application de ce framework est surtout basée sur la conformité au référentiel, et malheureusement bien peu sur une approche par les risques, pourtant un fondement essentiel de la sécurité de l'information (seule une approche par les risques permet de prioriser efficacement les mesures à mettre en place).

Voici un schéma qui résume cela :



Avec un état comme celui-ci, on conclurait facilement que la partie détection doit être priorisée l'année suivante. Et en fonction du budget et de des coûts de mise en œuvre de cette thématique, que seules certaines des mesures liées à la détection seront implémentées. Alors qu'il est possible que le plus gros risque soit lié à une autre thématique (protection, par exemple)…

Le principal défaut de ce *framework* est donc lié à un usage discutable. Car associé à une analyse de risques (qui fait partie des thèmes), il est parfaitement intéressant.