PARTIE II

Management de la Sécurité du Système d'Information & Gestion des Risques

Introduction

- La Gestion de la Sécurité du Système d'Information consiste à mettre en place les moyens **humains** et **matériels** afin d'assurer en permanence la sécurité d'un système d'information.
- La norme **ISO/CEI 27001** définit ainsi un SMSI (Système de Management de la Sécurité de l'Information) :
  - 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.
- Le système de management inclut
  - l'organisation,
  - les politiques,
  - les activités de planification,
  - les responsabilités,
  - les pratiques,
  - les processus et
  - les ressources.

Gouvernance de la Sécurité du SI

- La Gouvernance de la Sécurité du Système d'Information regroupe l'ensemble des **outils organisationnels** permettant la Gestion de la Sécurité du Système d'Information.
- Parmi ces outils, on trouve notamment :
  - La(es) Politique(s) de Sécurité
  - Les Normes
  - Les Processus et Procédures
  - Les Lignes Directrices

1. Politique(s) de Sécurité

- Une politique de sécurité est établie par la Direction Générale d'une entreprise et définit des objectifs généraux et des buts à atteindre.
- Elle définit également les rôles et responsabilités relatifs à la sécurité au sein de l'entreprise.
- La politique de sécurité explicite les obligations législatives et réglementaires de l'entreprise, mais également ses besoins liés au(x) métier(s), ainsi que les attentes de la direction générale.
- Par exemple, une politique de sécurité rappellera les règles édictées par la **CNIL** et désignera un Correspondant Informatique et Libertés (CIL) au sein de l'entreprise.
- La politique de sécurité d'une administration française devra pour sa part tenir compte du **RGS** (Référentiel Général de Sécurité) destiné à sécuriser les échanges électroniques de la sphère publique et disponible sur le site de l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information).

1. Politique(s) de Sécurité

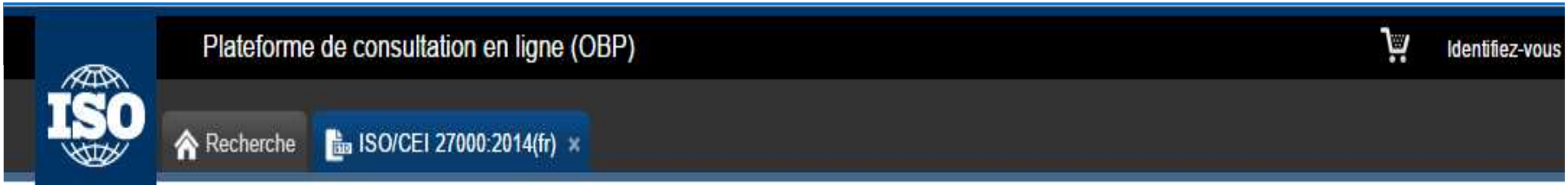
- **CNIL :** la Commission Nationale de l'Informatique et des Libertés impose des règles très strictes dès lors qu'une entreprise collecte des données personnelles.

Exemple :

- Tout responsable de traitement informatique de données personnelles doit adopter des mesures de sécurité physiques (sécurité des locaux), logiques (sécurité des systèmes d'information) et adaptées à la nature des données et aux risques présentés par le traitement.
- Le non-respect de l'obligation de sécurité est sanctionné de 5 ans d'emprisonnement et de 300 000 € d'amende. (art. 226-17 du code pénal)

2. Les Normes

- Une entreprise peut décider ou simplement être obligée par son activité de respecter un certain nombre de normes relatives à la sécurité.
- Ces normes peuvent s'appliquer au Système de Management de la Sécurité Informatique comme la norme **ISO/CEI 27001**, ou bien être relatives à un domaine d'activité comme la norme **PCI-DSS** (Payment Card Industry - Data Security Standards) pour les activités utilisant des moyens de paiement par carte bancaire.
- Une entreprise peut aussi décider de mettre en application un certain nombre de bonnes pratiques professionnelles telles que celles définies par **ITIL** (Information Technology Infrastructure Library) ou encore **CobiT** (Control Objectives for Information and related Technology, en français Objectifs de Contrôle de l'Information et des Technologies Associées).
- Toujours pour les administrations, la norme de référence est le **RGS** (Référentiel Général de Sécurité).
- Les normes peuvent être d'origine externe comme les précédentes, ou bien d'origine interne dans un objectif de standardisation, par exemple le choix d'un type de système d'exploitation ou d'une technologie d'authentification particulière pour toute l'entreprise.
- L'adhésion, par choix ou obligation statutaire, au respect d'une norme lui confère un aspect obligatoire et contrôlable par exemple au moyen de certifications.



ISO/CEI 27000:2014(fr) Technologies de l'information — Techniques de sécurité — Systèmes de management de la sécurité de l'information — Vue d'ensemble et vocabulaire

Disponible en: en fr ru

— ISO/IEC 27001, *Systèmes de management de la sécurité de l'information — Exigences*

— ISO/IEC 27002, *Code de bonne pratique pour les mesures de sécurité de l'information*

— ISO/IEC 27003, *Lignes directrices pour la mise en oeuvre du système de management de la sécurité de l'information*

— ISO/IEC 27004, *Management de la sécurité de l'information — Mesurage*

— ISO/IEC 27005, *Gestion des risques liés à la sécurité de l'information*

— ISO/IEC 27006, *Exigences pour les organismes procédant à l'audit et à la certification des systèmes de management de la sécurité de l'information*

— ISO/IEC 27007, *Lignes directrices pour l'audit des systèmes de management de la sécurité de l'information*

— ISO/IEC/TR 27008, *Lignes directrices pour les auditeurs des contrôles de sécurité de l'information*

— ISO/IEC 27010, *Gestion de la sécurité de l'information des communications intersectorielles et interorganisationnelles*

— ISO/IEC 27011, *Lignes directrices du management de la sécurité de l'information pour les organismes de télécommunications sur la base de l'*ISO/IEC 27002

— ISO/IEC 27013, *Guide sur la mise en oeuvre intégrée de* l'ISO/IEC 27001 *et de l'*ISO/IEC 20000-1

— ISO/IEC 27014, *Gouvernance de la sécurité de l'information*

— ISO/IEC/TR 27015, *Lignes directrices pour le management de la sécurité de l'information pour les services financiers*

— ISO/IEC/TR 27016, *Management de la sécurité de l'information — Économie organisationnelle*

3. Les Processus et les Procédures

- Ce sont des explications détaillées, pas à pas, sur la mise en application des mesures de sécurité choisies.

Exemples :

- Processus de gestion des changements
- Procédure de création ou de suppression de compte utilisateur
- Procédure de mise au rebut ou de sortie de matériel
- Procédure de gestion des incidents
- Procédure d'évaluation de la sécurité

- L'obligation de mettre en œuvre ces procédures est en général rappelée dans la Politique de Sécurité.

2. Les Lignes Directrices

- Ce sont des descriptions clarifiant ce qu'il convient de réaliser et par quels moyens, en vue d'atteindre les objectifs fixés par la Politique de Sécurité de l'organisation.

Exemples :

- Équiper chaque poste de travail d'un logiciel antivirus à jour.
- Procéder à un effacement complet des données par un logiciel recommandé par l'ANSSI avant la mise au rebut d'un support mémoire de masse.

- Les lignes directrices sont des conseils et/ou des recommandations, elles ne présentent donc pas le caractère obligatoire des normes et standards.

Différences entre politique, norme, procédure et ligne directrice :

Pour illustrer ces différences, nous prendrons l'exemple d'une entreprise de menuiserie qui assemble des meubles et a instauré une Politique de Sécurité relative à l'usage des marteaux.

- **Politique : "** Toutes les planches doivent être clouées ensemble au moyen de marteaux approuvés par l'entreprise, de façon à assurer une uniformité dans notre production ainsi que la sécurité des employés".

- **Norme :** "Des marteaux de 30 cm à manche en fibre seront employés pour les opérations d'assemblage, uniquement avec des clous en acier trempé. Des marteaux pneumatiques devront être employés pour tout travail répétitif d'une durée supérieure à 1 heure."

- **Procédure :** "1- Placer le clou perpendiculairement à la planche. 2- Frapper le clou par un mouvement complet du marteau. 3- Répéter cette opération jusqu'à ce que la tête du clou atteigne la planche."

- **Ligne directrice :** "Afin d'éviter de fendre le bois lors du clouage, il est possible de procéder à un pré-perçage avec un foret"

Classification de l'Information

- Toutes les informations d'un système n'ont pas la même valeur. Il est donc nécessaire de les évaluer au regard des critères de Disponibilité, Intégrité et Confidentialité afin de déterminer le niveau de protection dont elles doivent être dotées.
- Les niveaux de protection vont déterminer les procédures d'accès aux informations.
- Le but de la classification des actifs est de définir des "étiquettes" que l'on peut attacher à chacun d'eux, afin de faire savoir à tous ceux qui sont amenés à travailler avec ces actifs en quoi et dans quelle mesure ils ont de l'importance pour la sécurité.
- La classification cherche à déterminer la **sensibilité** de l'information au regard du critère de **confidentialité**.

Classification de l'Information - exemples

- Un exemple est la classification employée par le **Ministère de la Défense** en France concernant la confidentialité des actifs :

Non Classifié < Confidentiel Défense < Secret Défense < Très Secret Défense

- Dans le **domaine civil**, on trouvera fréquemment une classification similaire du type : Public < Interne < Confidentiel < Secret

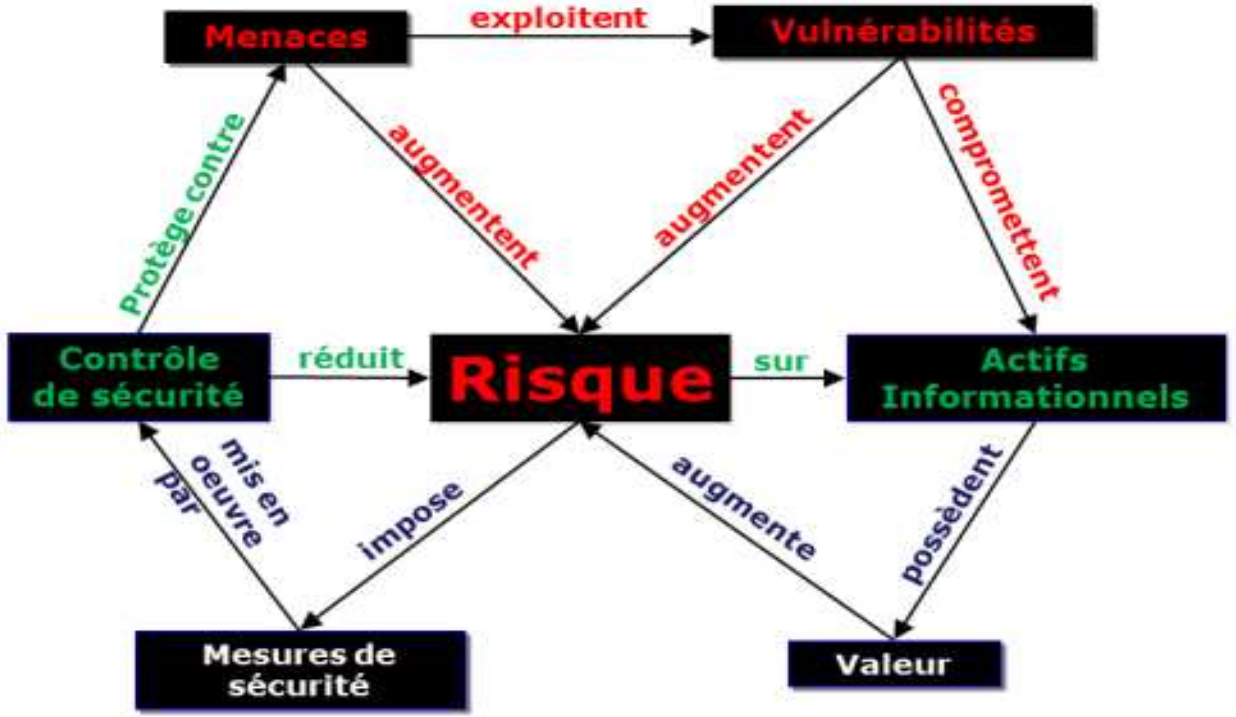
- La classification va également analyser la **criticité** de l'information au regard des critères d'**intégrité** et de **disponibilité**.
- La criticité selon ces critères s'évalue généralement sous forme de niveaux : Faible < Moyen < Haut

- Ces niveaux représentent l'importance pour l'entreprise qu'aurait la perte d'intégrité ou de disponibilité d'un actif.

- La classification ainsi obtenue sera un point d'entrée indispensable pour effectuer l'analyse et la gestion des risques.

Gestion des Risques

- **Qu'est-ce qu'un Risque ? «** Le risque exprime le fait qu'une entité, action ou événement, puisse empêcher de maintenir une situation ou d'atteindre un objectif dans les conditions fixées, ou de satisfaire une action programmée »
- **Relations autour du Risque :**



Gestion des Risques

- De ce schéma, on peut donc dire que le Risque est la potentialité qu'une Menace exploite une Vulnérabilité d'un Actif informationnel.
- La Gestion des Risques va donc consister à **identifier, évaluer et atténuer** les risques auxquels est exposée une entité.
- Il s'agit d'un processus récurrent et permanent au cours duquel l'entité doit :
  - Connaître ses actifs
  - Connaître les menaces qui pèsent sur elle et la probabilité de leur survenance
  - Connaître les vulnérabilités de son système d'information
  - Savoir comment et avec quelle efficacité elle a mis en place des mesures de protection
  - Déterminer les écarts et les traiter
- Les deux composantes principales de la Gestion des Risques seront donc :
  - L'**Analyse et l'Évaluation** des Risques
  - Le **Traitement** des Risques

L'Analyse et l'Évaluation des Risques

- **Identification des Risques :** Cette phase consiste à :
  1. Identifier les actifs (ceci a été fait lors de la classification)
  2. Identifier les menaces auxquelles sont confrontés ces actifs
  3. Identifier les vulnérabilités qui pourraient êtres exploitées par les menaces
  4. Identifier les impacts que les pertes de disponibilité, intégrité ou confidentialité peuvent avoir sur les actifs

- **Analyse et Évaluation :** Dans cette phase, il convient de :
  1. Évaluer qualitativement et/ou quantitativement les impacts identifiés dans la phase précédente
  2. Évaluer la probabilité réaliste de survenance des failles de sécurité de cette nature, au vu des menaces et des vulnérabilités identifiées, des impacts associés à ces actifs et des mesures actuellement mises en œuvre
  3. Estimer et valoriser les niveaux de risques
  4. Déterminer si les risques sont acceptables ou nécessitent un traitement. Il est impératif à cette étape d'en référer à la direction de l'entité qui est seule habilitée à accepter un risque.

L'Analyse et l'Évaluation des Risques

- Il existe de nombreuses méthodes permettant de formaliser l'analyse de risques, les plus pratiquées en France sont :
  - La méthode **EBIOS**, élaborée par l'ANSSI : **E**xpression des **B**esoins et **I**dentification des **O**bjectifs de **S**écurité,
  - La méthode **MEHARI** élaborée par le Clusif : **MÉ**thode **H**armonisée d'**A**nalyse de **Ri**sques.

Traitement des Risques

- Une fois les risques identifiés, analysés et évalués en termes d'impact, la phase suivante consiste en un choix de traitement des risques :
  - Application des mesures appropriées pour réduire le risque,
  - Acceptation des risques en connaissance de cause et avec objectivité, dans la mesure où ils sont acceptables au regards des politiques de sécurité de l'organisation et des critères d'acceptation des risques,
  - Évitement ou refus des risques (exemple, pour éviter tout risque d'attaque par le réseau, débranchement des accès Internet)
  - Transfert des risques liés à l'activité associée à des tiers, par exemple assureurs, fournisseurs, infogérance

Application de Mesures de Sécurité

- Le choix des types de mesures de sécurité à appliquer sera fonction soit des **causes**, c'est à dire des **menaces** et **vulnérabilités** :

Causes	Types de Mesures
Exposition naturelle	Structurelles
Intention de l'agresseur	Dissuasives
Possibilité de sinistre	Préventives

- soit des **effets**, c'est à dire des **impacts** liés à la survenance du risque :

Effets	Types de Mesures
Détériorations	de Protection
Dysfonctionnements	Palliatives
Pertes Finales	de Récupération

Gestion des Ressources Humaines

- Les médias mettent beaucoup l'accent sur les **menaces externes** à une entreprise que représentent les hackers, cependant il existe une menace au moins aussi importante en interne sur les actifs informationnels, que ce soit par manipulations erronées ou frauduleuses.
- Le personnel d'une entreprise est au plus près des données et connaît bien les traitements, ainsi que les potentielles faiblesses des contrôles existants. Il est donc le plus à même d'exploiter ces vulnérabilités.
- Des mesures de sécurité appliquées aux emplois, telles que la séparation des tâches, la description précise des postes et missions, l'obligation de partir en congés, la rotation des postes, ainsi que les principes de besoin d'en connaître et de moindre privilège sont les principales parades destinées à diminuer les risques d'origine interne et malveillante sur les données.
- Le personnel doit aussi être qualifié et correctement formé pour l'emploi qu'il occupe pour prévenir au mieux les erreurs, les rôles et responsabilités clairement définis afin que les interactions entre services fonctionnent correctement et ne créent pas de failles.

Gestion des Ressources Humaines

- Il serait judicieux d'entreprendre un certain nombre d'actions avant qu'une personne soit affectée à un poste, surtout si celui-ci implique la manipulation de données ou d'éléments sensibles du système d'information.
  - Description précise du poste et des responsabilités
  - Vérification des références et des diplômes
  - Vérification des antécédents
  - Préparation d'engagements de confidentialité
  - Procédures de fin de contrat
  - Politique d'accès pour les fournisseurs, consultants, intérimaires

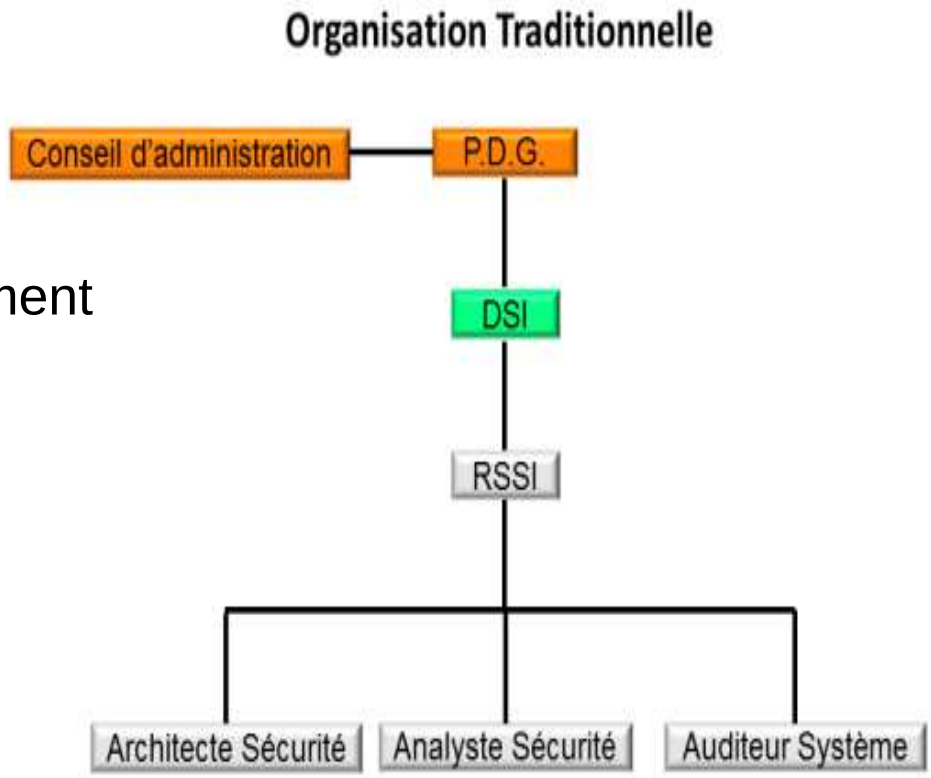
Éducation à la Sécurité, Formation et Sensibilisation

- Afin de limiter les risques d'origine interne, notamment ceux issus d'erreurs ou de négligences, une organisation devra à minima instituer un programme de sensibilisation à la sécurité du système d'information destiné à l'ensemble du personnel.
- Elle devra aussi élaborer un programme de formation sur des points précis afin d'approfondir les sujets auxquels certains personnels sont particulièrement exposés, par exemple :
  - La sécurité du poste de travail
  - Le traitement du courrier électronique et notamment les *spams* et le *phishing*
  - La conduite à tenir en cas d'incident
  - Le choix et la gestion des mots de passe
  - La sécurité physique
  - L'ingénierie sociale (*social engineering* en anglais)
  - La manipulation des données classifiées, quel que soit leur support
  - Les accidents, erreurs ou omissions

Organisation de la Sécurité

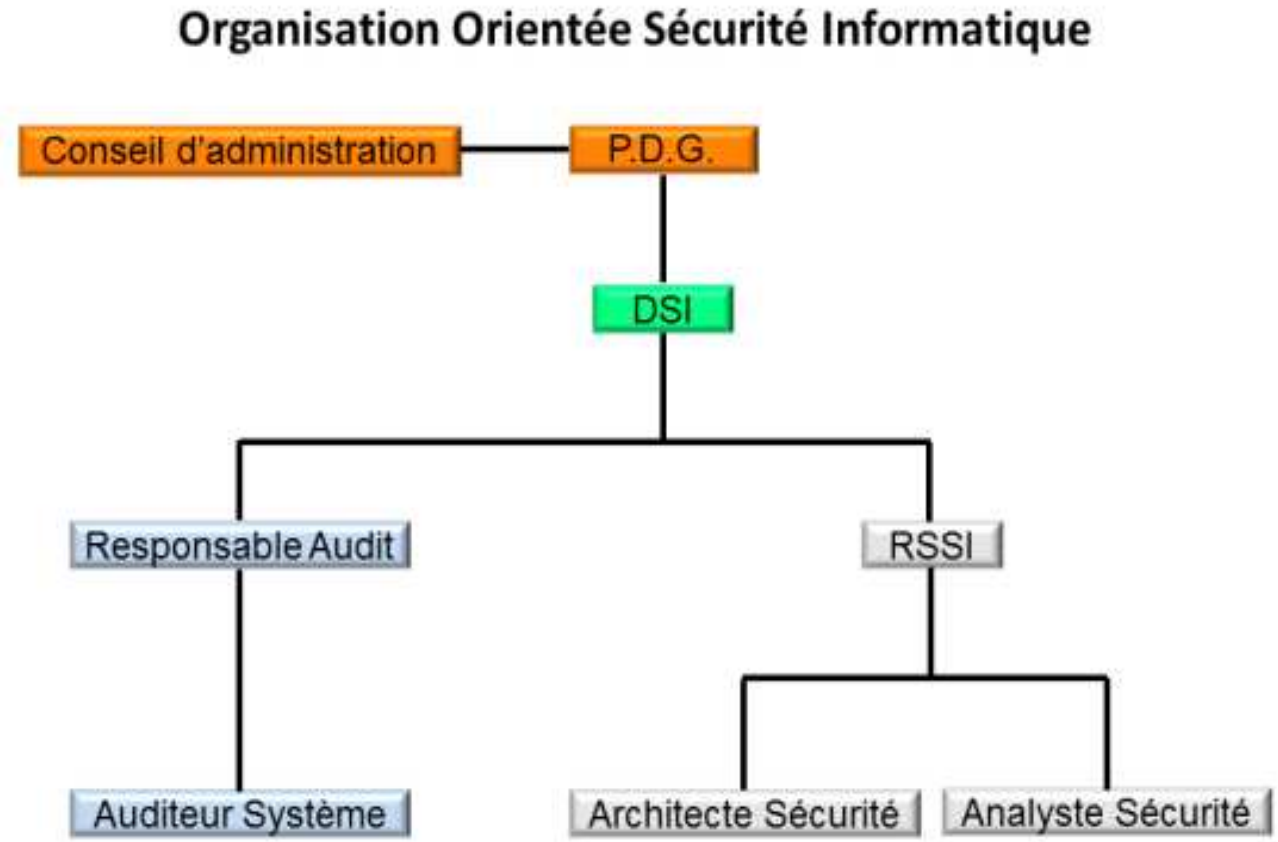
- L'organisation déployée pour assurer la sécurité des systèmes d'information varie grandement d'entreprise en entreprise, mais un certain nombre de modèles types se dessinent.

- Le poste de RSSI (Responsable de la Sécurité des Systèmes d'Information) a initialement été rattaché à la Direction des Systèmes d'Information (DSI).



Organisation de la Sécurité

- A l'usage, il a semblé prudent de séparer la fonction d'audit de l'administration de la sécurité, ce qui a donné un modèle de ce type.



Organisation de la Sécurité

- Enfin, de plus en plus, grâce à la mise en place de systèmes de gestions de la qualité et de la sécurité, la fonction d'audit s'est généralisée à l'ensemble des activités de l'entreprise et l'audit de la sécurité informatique a été détaché de la DSI pour rejoindre l'audit interne habituellement directement rattaché à la direction générale et/ou au conseil d'administration ou son équivalent.