IAE LIMOGES
École Universitaire
de Management

Master 2 — Audit des risques informatiques

"I've hacked into our bank account."

Objectifs & Introduction — P-F. Bonnefoi

Version du 3 décembre 2018

Programmation de l'UE

Volume horaire 15h

Agenda

- mercredi 17 octobre 16h30-18h30
- la suite ? dans ADE !

Examen écrit d'1h, *documents non autorisés*

Ressources

Un site Web

`http://p-fb.net/master-2/cca.html`

dessus :

- ▷ les supports de cours ;
- ▷ les annales d'examen ;
- ▷ *une version imprimée des supports sera également distribuée*.

Contact

bonnefoi@unilim.fr
Laboratoire XLIM, 123 av Albert Thomas, bureau 421

Programme du DSCG

Sécurité des Systèmes informatiques

- Mise en place d'une **architecture de confiance** :
  - Comprendre le fonctionnement d'une infrastructure à clé publique ;
  - certificat numérique, signature électronique.
- Prendre les dispositions pour garantir la **continuité de l'activité** :
  - surveillance des processus ;
  - analyse des risques ;
  - mise en place d'outils de protection techniques et juridiques.

Programme de l'UE

- **Présentation des risques informatiques** :
  - le panorama de la «cybercriminalité» et des menaces ;
  - fonctionnement d'un réseau local ;
  - protection du réseau et du poste de travail ;
  - analyse des risques et proposition d'une politique de sécurité.
- **Introduction à la cryptographie et application** :
  - chiffrement symétrique et asymétrique ;
  - Fonction de hachage ;
  - Signature électronique ;
  - Certificat et infrastructure de confiance ;
- **Partie pratique** :
  - utilisation des certificats et chiffrement/signature du courrier électronique.

But de l'enseignement

Présenter la sécurité dans le cadre des échanges électroniques qu'ils soient **synchrones** (communication directe avec un serveur, comme un serveur Web par exemple) ou **asynchrone** (remise de courrier, stockage de document).

Les points abordés sont :

- **l'authentification** des interlocuteurs ou propriétaires ;
- la garantie de **confidentialité** et **d'intégrité** ;
- la **signature électronique** et la non répudiation ;
- la mise en place de la confiance au travers des **certificats** et des **infrastrutures à clé publiques** ;
- les **obligations légales** et le référentiel national d'usage ;
- les **risques** et les **atteintes** possibles à la fiabilité de ces opérations ;
- l'utilisation dans le cadre de son **activité professionnelle** et des règles administratives.

Objectifs

Maîtriser son **identité électronique** et celle de ses interlocuteurs et assurer la **sécurité de son travail dématérialisé**.

l'ISO, Organisation internationale de normalisation, «*International organization for standardization*»

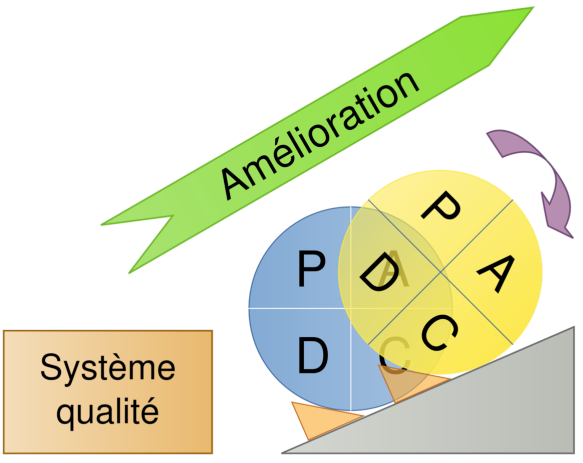
- organisation internationale, créée en 1947 ;
- composée de représentants des organismes de normalisation nationaux d'environ 150 pays ;
- produit des normes internationales dans les domaines industriels et commerciaux.

Différentes normes, IS, «*International Standard*» :

- IS 9000 : consacrée à la définition d'un «*système de management*» :
  - établir une politique et fixer des objectifs :
    - référentiel écrit ;
    - ensemble de mesures organisationnelles et techniques destinées à mettre en place un certain contexte organisationnel et à en assurer la pérennité et l'amélioration ;
  - vérifier que l'on a atteint les objectifs fixés :
    - réaliser un *audit* qui consistera à comparer le référentiel à la réalité pour relever les divergences, nommées *écarts* ou *non-conformités*.
    - sans référentiel, l'auditeur en peut réaliser sa mission ;
      mais il existe de nombreux référentiels…
- IS 9001 : consacrée aux systèmes de management de la qualité et aux exigences associées ;
- IS 14001 : consacrée aux systèmes de management de l'environnement ;
- IS 27001 : consacrée aux **systèmes de management de la sécurité de l'information** ;
- IS 19001 : directives à respecter pour la conduite de l'audit d'un système de management.

Système de management de la sécurité de l'information ou SMSI

- s'applique à un SMSI ;
- fournie un schéma de certification pouvant être appliqué au SMSI au moyen d'un audit ;
- s'appuie sur une approche *par processus* : exemple du PDCA, «*Plan, Do, Check, Act*» :



  - phase **Plan** :
    - définir le champ du SMSI,
    - identifier et évaluer les risques,
    - produire le document (*Statement of applicability*, SOA) qui énumère les mesures de sécurité à appliquer ;
  - phase **Do** :
    - affecter les ressources nécessaires,
    - rédiger la documentation,
    - former le personnel,
    - appliquer les mesures décidées,
    - identifier les risques résiduels ;
  - phase **Check** : audit et revue périodiques du SMSI, qui produisent des constats et permettent d'imaginer des corrections et des améliorations ;
  - phase **Act** :
    - prendre les mesures qui permettent de réaliser les corrections et les améliorations dont l'opportunité a été mise en lumière par la phase Check,
    - préparer une nouvelle itération de la phase Plan.

Le SMSI a pour buts de :

- **maintenir et d'améliorer la position** de l'organisme qui le met en œuvre du point de vue :
  - de la compétitivité,
  - de la profitabilité,
  - de la conformité aux lois et aux règlements,
  - de l'image de marque.
- **protéger les actifs «assets»** de l'organisme, définis au sens large comme *tout ce qui compte pour lui*.

Le vocabulaire du SMSI est fournie dans l'IS 27000.

Les mesures de sécurité énumérées dans la phase Plan peuvent être prises dans le **catalogue** de «mesures» et «bonnes pratiques» proposé par l'IS 27002.

IS 27001 impose une **analyse des risques**, mais **ne propose aucune méthode** pour la réaliser :

- **liberté de choisir** une méthode pour le SMSI, à condition que :
  - elle soit documentée ;
  - elle garantisse que les évaluations réalisées avec son aide produisent des résultats **comparables** et **reproductibles**.

Exemples de méthodes d'analyse des risques :

- **IS 27005**, méthode d'analyse fournie par l'ISO ;
- **EBIOS®**, «*Expression des Besoins et Identification des Objectifs de Sécurité*» : méthode d'évaluation des risques en informatique, développée par l'**Agence nationale de la sécurité des systèmes d'information** (ANSSI).
- **MEHARI**, «*Méthode harmonisée d'analyse des risques*» : méthode visant à la sécurisation informatique d'une entreprise ou d'un organisme. Elle a été développée et est proposée par le **Club de la Sécurité de l'Information Français**, CLUSIF.

Pour obtenir une certification IS 27001

- définir le champ du SMSI ;
- en formuler la politique de management ;
- préciser la méthode d'analyse de risques utilisée ;
- identifier, analyser et évaluer les risques ;
- déterminer les traitements qui seront appliqués aux différents risques, ainsi que les moyens d'en vérifier les effets ;
- attester l'engagement de la direction de l'organisme dans la démarche du SMSI ;
- rédiger le *Statement of Applicability* (SOA) qui sera la charte du SMSI et qui permettra de le soumettre à un audit.

Les différents IS

- IS 27001 : système de management de la sécurité des systèmes d'information (SMSI) ;
- IS27000 : vocabulaire SSI ;
- IS 27002 : catalogue de mesures de sécurité : `https://fr.wikipedia.org/wiki/ISO/CEI_27002`
- IS 27003 : implémentation du SMSI ;
- IS 27004 : indicateurs de suivi du SMSI ;
- IS 27005 : évaluation et traitement du risque ;
- IS 27006 : certification du SMSI ;
- IS 27007 : audit du SMSI.

L'historique et l'évolution de la législation

- juillet 2002, USA : **loi Sarbanes-Oxley**, «*SOX*» : impose aux entreprises qui font appel au capital public (cotées en bourse) toute une série de règles comptables et administratives destinées à assurer la traçabilité de leurs opérations financières, pour garantir plus de transparence pour les actionnaires (éviter les comptes truqués comme dans le cas du scandale «Enron») ;
- 1er août 2003, France : **loi du sur la sécurité financière** (LSF) qui concerne principalement trois domaines :
  - modernisation des autorités de contrôle des marchés financiers ;
  - sécurité des épargnants et des assurés ;
  - contrôle légal des comptes ainsi que la transparence et le gouvernement d'entreprise. *Cette loi française ne concerne pas seulement les sociétés cotées, mais toutes les sociétés anonymes*.
- 2004, **dispositif réglementaire européen «Bâle 2»** qui concerne les établissements financiers.

La loi Sarbanes-Oxley concerne la sécurité du système d'information : elle impose aux entreprises des procédures de contrôle interne, de conservation des informations, et de garantie de leur exactitude :

- *la continuité des opérations ;*
- *la sauvegarde et l'archivage des données ;*
- *l'externalisation et son contrôle.*

Les normes par secteurs d'activité

Standards et référentiels à suivre afin d'assurer la sécurité de l'activité

- Secteur publique (Autorité administrative)
- Banque (CFONB, PCI-DSS, Bâle II)
- Assurance (Pack assurance, Solvabilité, CPR)
- Santé (HAS/DGOS, PSSIE, PGSSE_S, hôpital numérique) «*Haute Autorité de Santé/direction générale de l'Offre de soins*», «*Politique de sécurité des systèmes d'information de l'Etat*», «*Plan Générale de Santé, Sécurité et Environnement*»
- Industrie (Sevezo, CFR 21)
- Environnemental (ISO 14001) «Management environnemental»
- Alimentaire (ISO 22000) «Management de la sécurité des denrées alimentaires»
- Transaction web (21188 :2006) «Infrastructure de clé publique pour services financiers – Pratique et cadre politique»

Connaître, appliquer et respecter les normes qui s'appliquent aux différents secteurs d'activité de l'entreprise permet de se protéger contre les ***risques juridiques****.*