

AUDIT DE LA SECURITE DES SYSTÈMES D'INFORMATION

Donatien KOUADIO | CISA
donatienk@yahoo.fr



Introduction et présentation générale

Audit de la sécurité des systèmes d'information

- ☐ Introduction et présentation générale
- ☐ Principes généraux des systèmes d'information
- ☐ Notions de base de la sécurité de l'information
- ☐ Processus d'audit des systèmes d'information
- ☐ Importance de la gestion de la sécurité
- ☐ Politique et administration de la sécurité des SI
- ☐ Analyse des risques
- ☐ Démarches de l'audit de sécurité
- ☐ Contexte législatif au Sénégal et dans la CDEAO
- ☐ Exercices & Cas Pratiques
- ☐ Certifications

Principes généraux

Principes généraux

Qu'est ce que la sécurité du système d'information?

- L'information est un actif précieux de l'entreprise.
 - Recherche et développement
 - Techniques de fabrication
 - Stratégie de l'entreprise
 - Données financières
 - Informations commerciales (tarifs, marges, propositions, ...)
 - Données personnelles (médicales, clients, salariés, ...)
 - etc.
- A ce titre, il faut la protéger contre :
 - La perte,
 - L'altération,
 - La divulgation.

Principes généraux

Qu'est ce que la sécurité du système d'information?

- L'information se présente sous de nombreuses formes :
 - Imprimée ou écrite sur papier,
 - Enregistrée sur support électronique, films ou bandes magnétiques,
 - Parlée lors de conversations, etc.
- Les organisations modernes sont de plus en plus dépendantes des systèmes informatiques et de télécommunication, qui sont eux-mêmes de plus en plus ouverts et répandus.
- Ces systèmes doivent donc être protégés contre :
 - L'indisponibilité,
 - L'intrusion.

Principes généraux

Le système d'information (rappel)

Le système d'information est constitué de l'ensemble des moyens matériels, logiciels, organisationnels et humains qui agissent entre eux afin de traiter, conserver ou communiquer de l'information.

Il comprend par exemple :

- Le système téléphonique et de télécopie (couramment appelé « fax »),
- La messagerie,
- Les ordinateurs (stations et serveurs) ainsi que leurs logiciels, fichiers et bases de données, et tous leurs supports (disques externes, CD-ROM, etc.),
- Le réseau (Intranet ou Extranet),
- Les imprimantes, et les broyeurs à papier,
- Les notes, comptes rendus, dossiers, mémos et documents divers,
- Les conversations, etc.

Notions de base de la sécurité des SI

Notions de base de la sécurité des SI

Introduction

- La sécurité n'est pas une affaire de spécialistes, mais relève de la responsabilité de chaque collaborateur, de chaque service et de chaque direction.
 - ⊕ Chacun manipule et utilise des informations et des ressources qui constituent le patrimoine de l'entreprise et, à ce titre, doit garantir leur protection.
- Toute démarche de sécurité doit être précédée d'une analyse des risques.
 - Identifier les enjeux de l'entreprise
 - Évaluer les impacts métier d'un sinistre.
- Axes d'expression de la sécurité :
 - Confidentialité
 - Intégrité
 - Disponibilité
 - **Preuve:** imputabilité, traçabilité, auditabilité, non-répudiation.

Notions de base de la sécurité des SI

Le rôle stratégique de l'individu

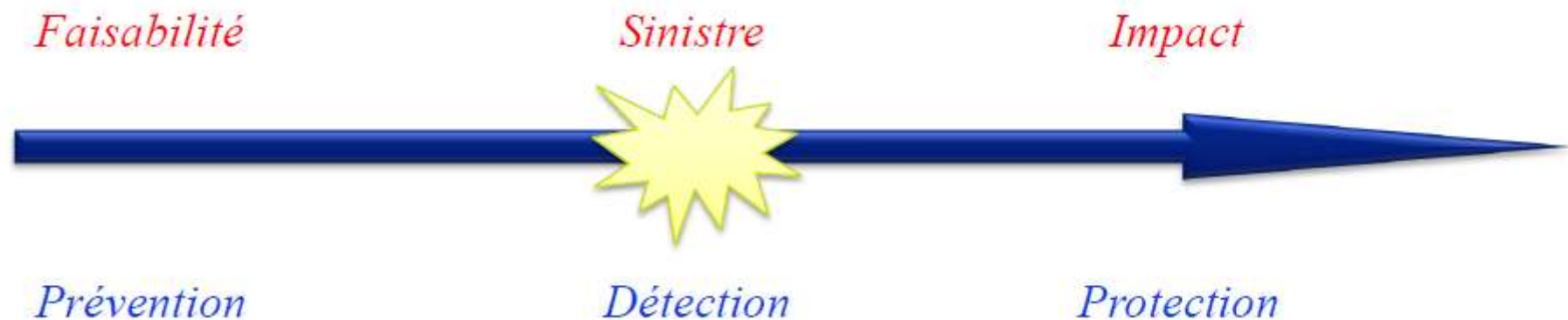
- L'individu joue le rôle central dans la sécurité de l'entreprise :
 - il manipule quotidiennement les actifs sensibles,
 - il applique les procédures définies,
 - il met en œuvre les moyens de sécurité,
 - il identifie les situations anormales,
 - il détecte les incidents,
 - il réagit même si aucune procédure n'adresse le cas rencontré.
- Un personnel responsable et vigilant est la clé d'une sécurité efficace.
 - Importance de la sensibilisation et de la formation (conduite du changement).

«La sécurité de la cité tient moins à la solidité de ses fortifications qu'à la fermeté d'esprit de ses habitants.» Thucydide

Notions de base de la sécurité des SI

Analyse de risques et mesures de sécurité

- **Analyse de risques :**
 - Faisabilité,
 - Impact financier,
 - Impact sur image de marque.
- **Mesures de sécurité :**
 - Prévention,
 - Détection,
 - Protection (ou réaction).



Notions de base de la sécurité des SI

Le vecteur DICT: Disponibilité

Tout système doit apporter les fonctions attendues dans les délais prévus, conformément au contrat de service défini avec les utilisateurs.

- La continuité de service doit être assurée quelles que soient les circonstances :
 - charge importante du système,
 - panne d'un composant,
 - défaillance d'un fournisseur (électricité, télécoms, etc.),
 - sinistre endommageant ou détruisant le système.
- Techniques de base liées à la disponibilité :
 - Systèmes de haute disponibilité, à tolérance de panne
 - Plan de Sauvegarde
 - Plan de Reprise d'Activité (PRA)
 - Gestion de la Crise

Les systèmes et les informations ne doivent être altérés à l'insu de leurs propriétaires.

- L'altération est une modification non autorisée préservant la vraisemblance des données ou le bon fonctionnement apparent des systèmes.
- L'altération peut provenir :
 - d'une erreur,
 - d'une infection par un virus,
 - d'un acte de malveillance.
- Les techniques de sécurité généralement employées ont davantage pour effet de détecter l'altération que de l'interdire.

Notions de base de la sécurité des SI

Le vecteur DICT: Confidentialité

L'information est protégée contre la divulgation à des tiers non autorisés.

- L'information doit être protégée à tout moment :
 - lors de son stockage (bases de données, disquettes),
 - lors de son transfert (réseaux),
 - lors de sa matérialisation (documents papier).

Notions de base de la sécurité des SI

Le vecteur DICT: Traçabilité (ou Preuve)

Le système doit permettre, chaque fois que nécessaire, d'enregistrer de manière incontestable toute action sur tout objet par tout auteur.

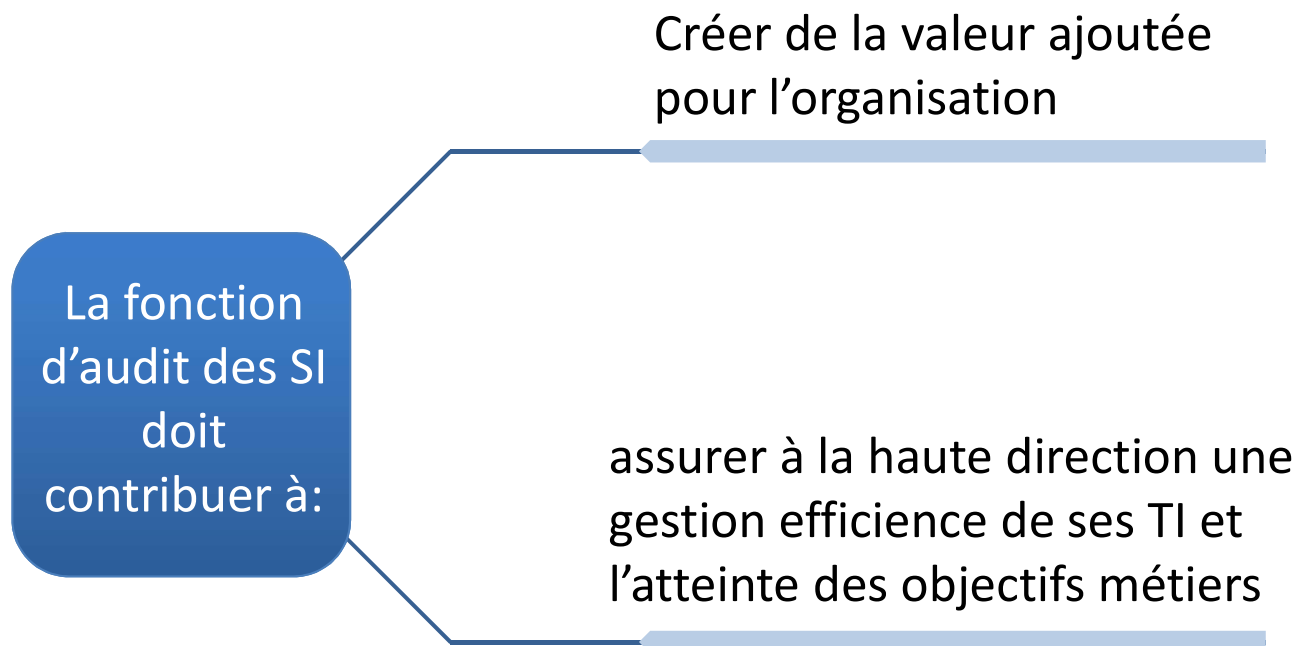
- Il doit permettre d'imputer toute opération à son auteur (**imputabilité**).
- Il doit permettre de reconstituer toutes les étapes permettant de passer d'une situation à une autre (**traçabilité**).
- Il doit permettre de vérifier la bonne application des procédures prévues (**auditabilité**).
- Il doit permettre de garantir l'identité des parties à une transaction (**non-répudiation**).

Processus d'audit des SI

Processus d'audit des SI

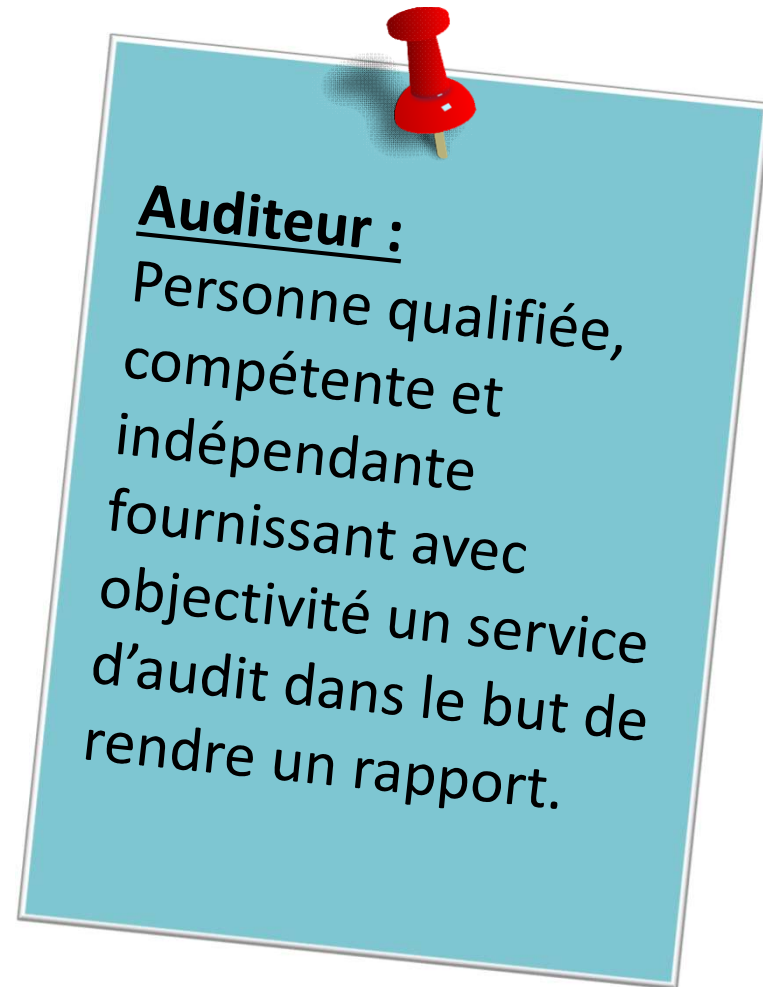
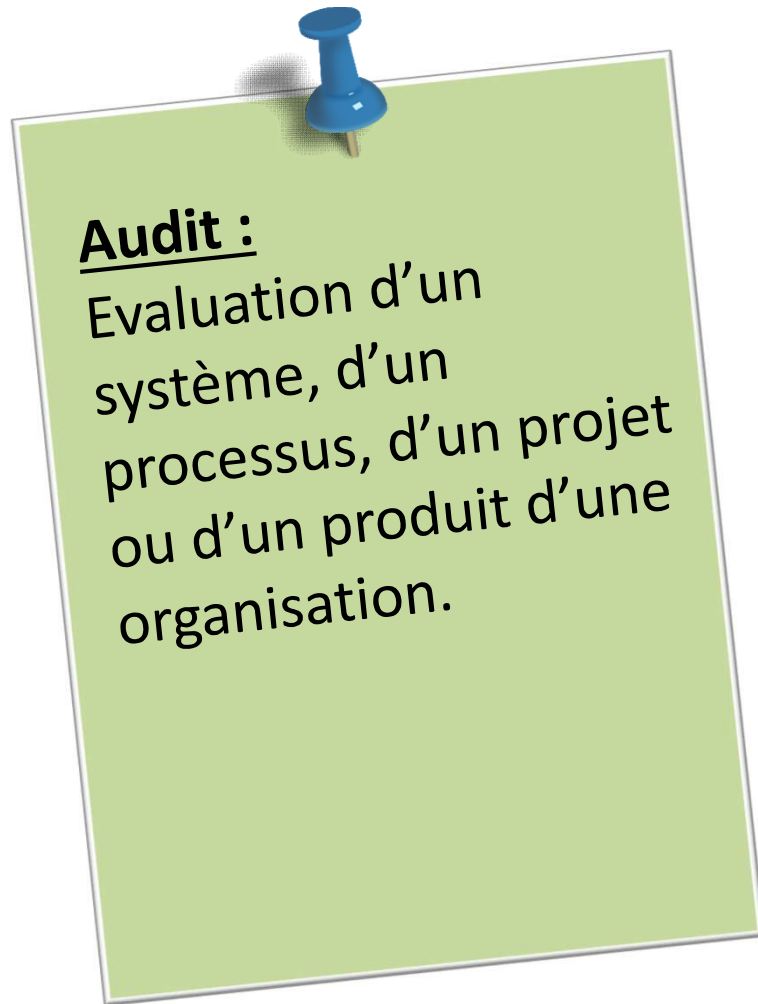
La fonction d'audit des SI

- doit être gérée et dirigée de manière à assurer que les différentes tâches exécutée et réalisée par l'équipe **répondent aux objectifs** de la mission, **tout en permettant à l'équipe de conserver son indépendance.**



Processus d'audit des SI

L'Audit et les Auditeurs



Processus d'audit des SI

Types d'Auditeurs



Interne:

Employé d'une organisation ayant pour rôle d'analyser et d'évaluer le système de contrôle interne.



Externe :

Auditeur provenant d'une firme d'audit indépendante de l'organisation auditée.

Processus d'audit des SI

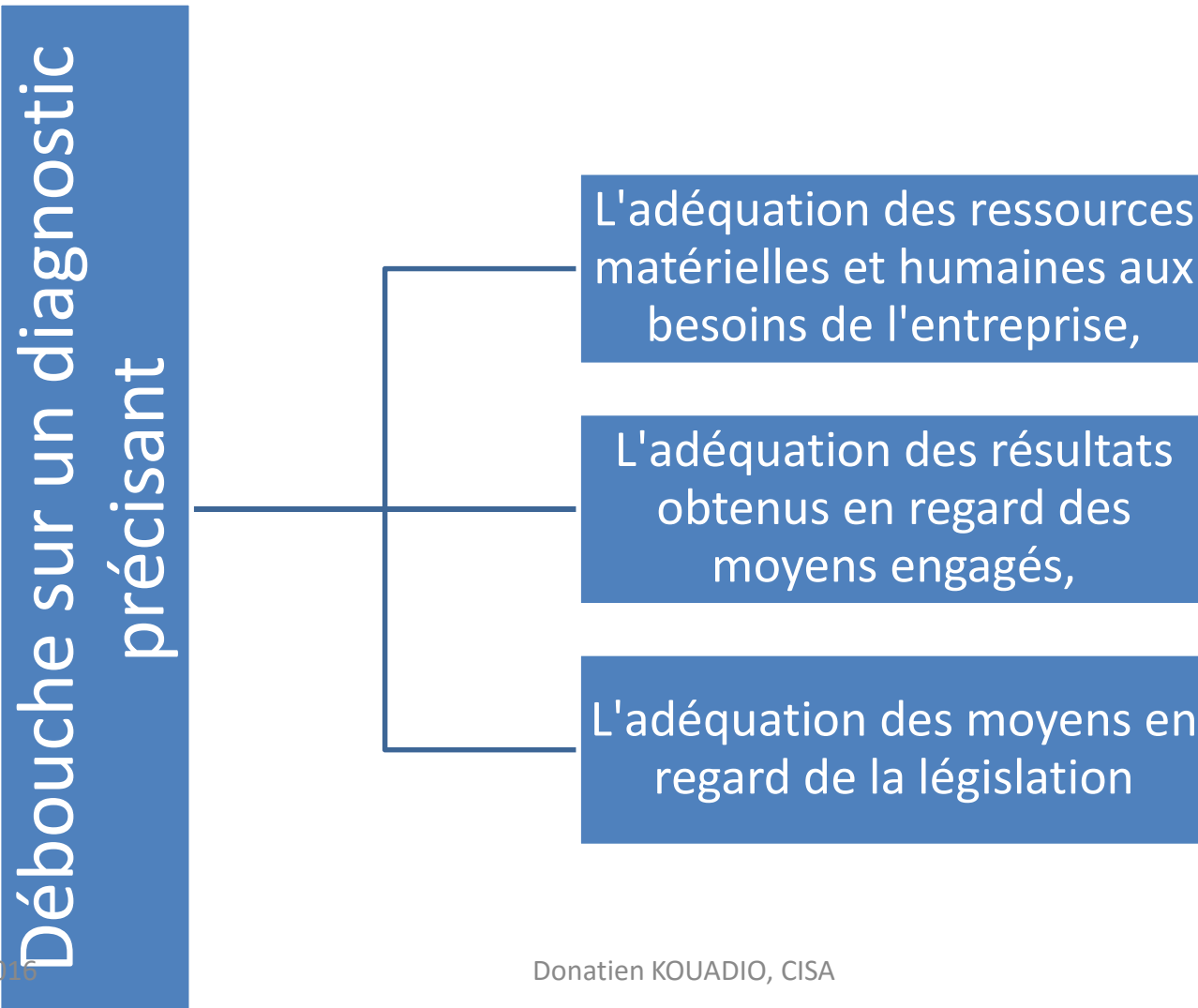
Qualifications de l'auditeurs



Processus d'audit des SI

Audit des SI / TI

- Analyse partielle ou exhaustive du fonctionnement d'un centre de traitement et de son environnement,




Processus d'audit des SI

Charte d'audit

Le rôle de la fonction d'audit des SI est établi par la Charte d'Audit. L'audit SI peut faire partie de l'audit interne en tant que groupe indépendant ou intégré à l'audit financier et opérationnel.

La charte d'audit doit énoncer clairement:



Les objectifs et les responsabilités de la direction pour la fonction d'audit des SI.

La délégation de pouvoir de la direction à la fonction d'audit.

L'autorité, la portée et les responsabilités globales de la fonction d'audit.

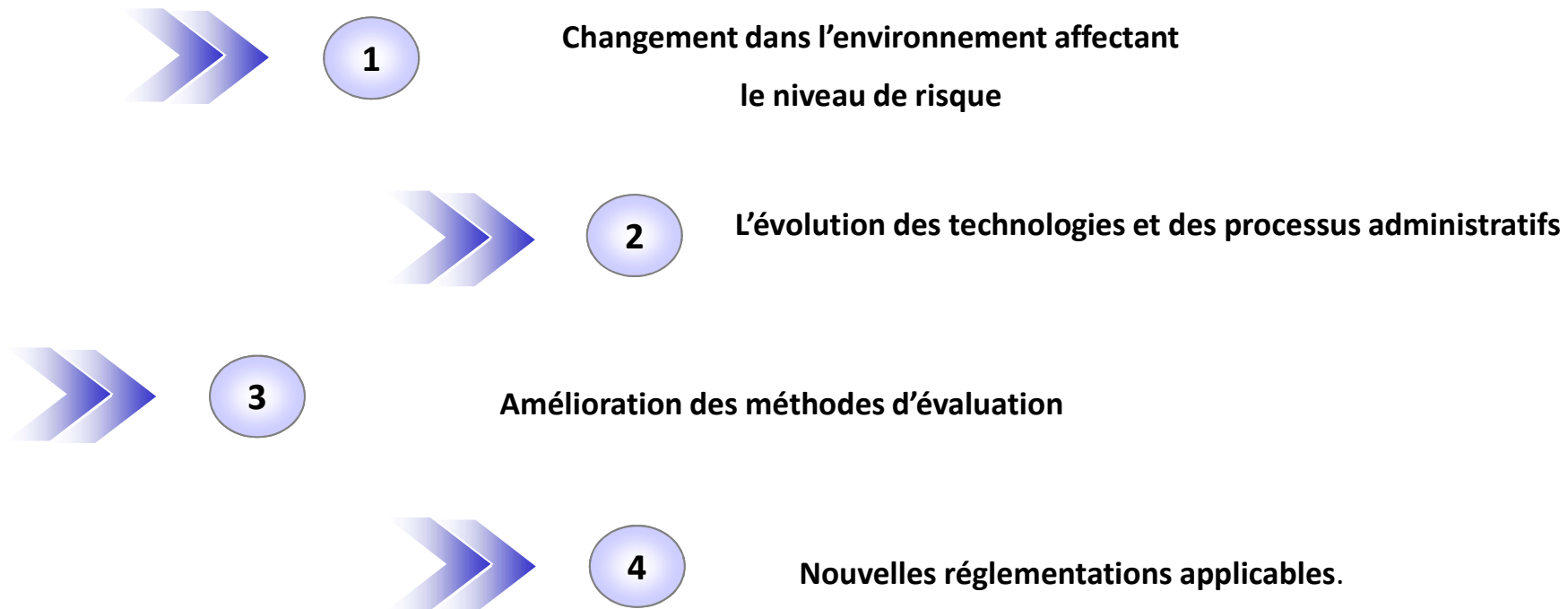
L'organisation de la fonction d'audit.

Processus d'audit des SI

Planning d'audit

- Court terme : Généralement dans un an.
- Long terme : Plus d'un an (5, 10, 15, ...)

Il est important dans la planification de tenir compte des question liées au risque, qui influenceront sur l'environnement technologique de l'organisation:



Processus d'audit des SI

Planning d'audit (Exemple)

Domaine à auditer	Période	Date dernier audit	Responsabilité
Procédures et politique d'enregistrement	Q1	Jamais	Auditeur Interne
Plan de continuité des affaires	Q2	2014	DSI, Consultant Sécurité
Gouvernance des SI	Q3	Jamais	Auditeur Interne
Sécurité de l'exploitation informatique	Q4	2006	DSI, Consultant Sécurité

Processus d'audit des SI

Compréhension de l'entité à auditer (1/2)

- Dans le cadre de la planification d'une mission, l'auditeur doit :

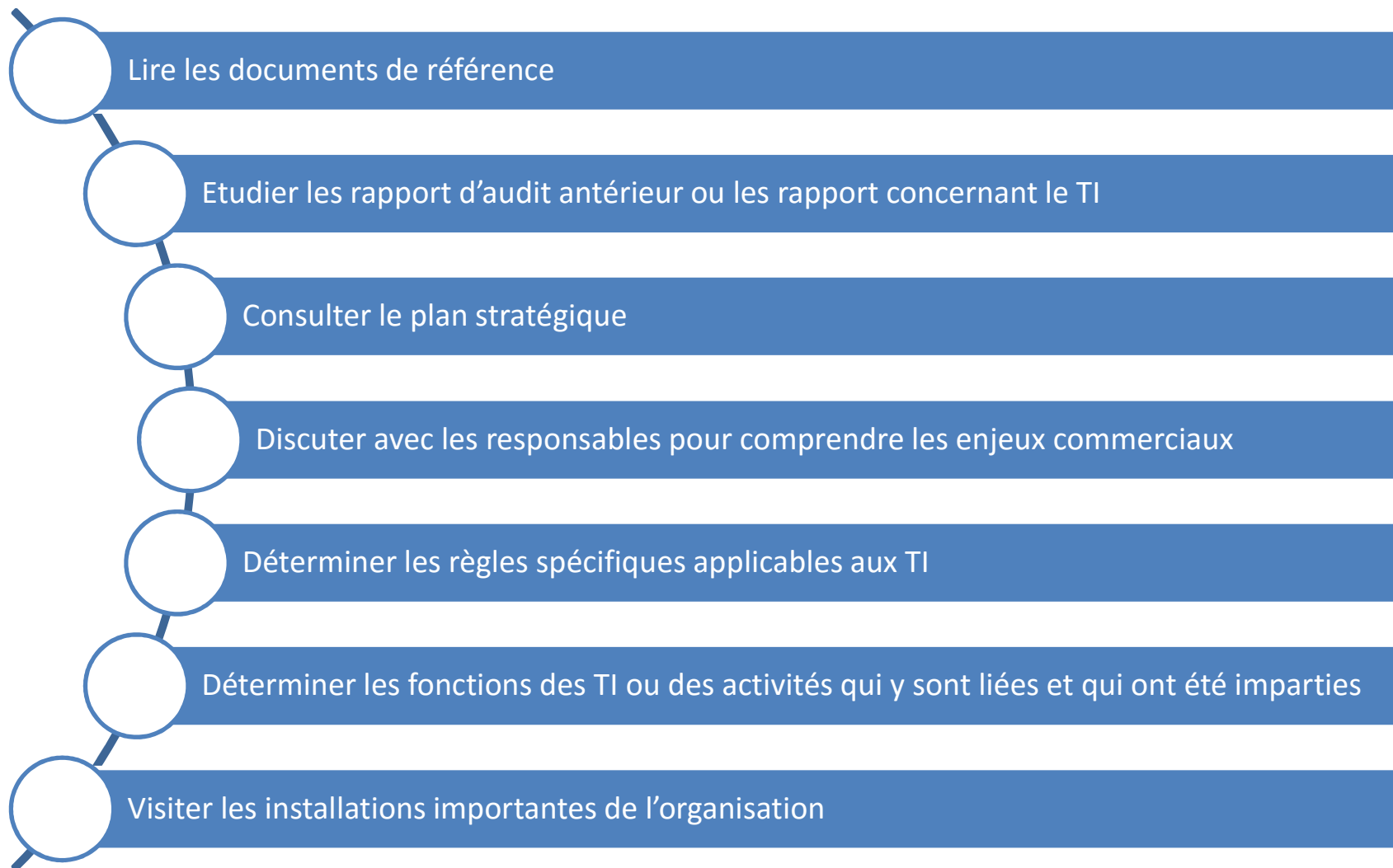
Posséder une bonne compréhension de l'environnement global qui fait l'objet d'un examen.

Créer un plan d'audit qui prend en considération les objectifs de l'entité concernée par le secteur qui fait l'objet d'un audit, ainsi que son infrastructure technologique.

Processus d'audit des SI

Compréhension de l'entité à auditer (2/2)

Les étapes à franchir pour acquérir une compréhension sont :



Processus d'audit des SI

Lois et réglementations

- Chaque organisation doit se conformer à un certain nombre d'exigences gouvernementales et externes, liées à la pratique et aux mesures de contrôle des systèmes d'information et la manière dont les ordinateurs, les programmes et les données sont conservées et utilisées.



- Exemple:
 - Cadre de mesures intégrée de réglementation interne, du COSO,
 - Accords de Bâle

Processus d'audit des SI

Etapes d'un audit typique

- 1- **Sujet d'audit:** Circonscrire la zone à auditer
- 2- **Objectif de l'audit:** Déterminer par exemple si des changements au code source d'un programme surviennent dans un environnement bien défini et contrôlé.
- 3- **Portée de l'audit:** Identifier les systèmes spécifiques, fonctions ou unités de l'organisation à inclure dans l'examen.
- 4- **Planification avant Audit:**
 - Acquérir la compréhension de la mission,
 - Identifier les habiletés techniques et les ressources nécessaires,
 - Identifier les sources d'information pour les tests ou les examens comme les dossiers fonctionnels, les politiques, les normes, les procédures fonctionnelles et les travaux d'audit précédents,
 - Identifier les emplacements ou les installations à auditer,
 - Réaliser une analyse des risques,
 - Prévoir la logistique du mandat.

Processus d'audit des SI

Etapes d'un audit typique

5- Procédures d'audit et de collecte de données:

- Tenir la réunion de lancement de la mission,
- Identifier et sélectionner l'approche d'audit pour vérifier et tester les contrôles,
- Identifier une liste d'individus à rencontrer,
- Identifier et obtenir les politiques de département, les normes et directives pour examen,
- Développer les outils d'audit et la méthodologie pour tester et vérifier les contrôles.

6- Procédures d'évaluation des tests ou des résultats d'examen

- Identifier les procédures d'examen de suivi,
- Identifier les procédures pour évaluer/tester l'efficacité opérationnelle,
- Identifier les procédures de test de contrôle,
- Examiner et évaluer la validité des documents, politiques et procédures.

7- Procédures de communication avec la direction

- Soumission du projet de rapport,
- Tenir la réunion de clôture.

8- Emission du rapport d'audit final

Processus d'audit des SI

Différents types de missions d'audit

Audit Interne

- Audit de l'organisation, de la planification et du pilotage des SI
- Audit des Systèmes et Réseaux
- Audit des coûts informatiques
- Audit des études informatiques
- Audit de la production informatiques
- Audit du plan de continuité d'activité
- Audit du parc informatique et du support utilisateur
- Audit de la sécurité des SI
- Audit des projets informatiques
- Audit applicatif

14/07/2019

Donatien KOUADIO, CISA

Audit Externe:

- Contrôles Généraux IT
- Revue des processus
- Analyse de données
- Revue de projets IT

Importance de la gestion de la sécurité de l'information

Importance de la gestion de la sécurité de l'information

Introduction

Objectifs de sécurité permettant de répondre aux exigences commerciales de l'entreprise:

- Assurer la disponibilité continue des SI;
- Assurer l'intégrité de l'information en transit ou stockée sur les systèmes informatiques de l'organisation;
- Préserver la confidentialité des données sensibles lorsqu'elles sont stockées et en transit;
- Assurer la conformité aux lois, aux réglementations et aux normes applicables à l'organisation;
- Assurer le respect des exigences de confiance et d'obligation en lien avec toute information reliée à un individu identifié ou identifiable;
- Assurer que les données sensibles sont protégées adéquatement pendant le stockage et le transport suivant les exigences de l'organisation.

Importance de la gestion de la sécurité de l'information

Éléments clés de la gestion de la sécurité de l'information

- Un système des TI équipé de dispositifs de sécurité ne sera protégé que s'il est adéquatement implémenté, géré, ainsi qu'utilisé, supervisé et révisé avec soin.
- Les objectifs de sécurité ne peuvent être atteints seulement en ajoutant des protections techniques et procédurales. Une attitude de culture de sécurité et l'attention de tous les employés, de la direction ainsi que de tous les fournisseurs de services externes et des utilisateurs/partenaires des TI externes dignes de confiance sont vitales pour atteindre les objectifs de sécurité.
- Les éléments clés connexes de la gestion de la sécurité de l'information sont les suivants :

Importance de la gestion de la sécurité de l'information

Éléments clés de la gestion de la sécurité de l'information

- **Leadership, engagement et soutien de la haute direction:** Support de la haute direction pour mise en place et maintien d'un programme de gestion de la sécurité de l'information.
- **Politiques et Procédures:** Correspondant aux objectifs d'affaire, ainsi qu'aux normes et pratiques de sécurité généralement acceptées.
- **Organisation:** Rôle et responsabilité de sécurité au sein de l'entreprise.

Importance de la gestion de la sécurité de l'information

Éléments clés de la gestion de la sécurité de l'information

- **Sensibilisation et éducation à la sécurité:** Tous les employés d'une entreprise et, si pertinent, les utilisateurs des tierces parties doivent recevoir une formation appropriée et des mises à jour régulières pour améliorer la sensibilisation à la sécurité et le respect des politiques et des procédures écrites.
- **Contrôle et conformité:** Les auditeurs des SI sont souvent mandatés pour évaluer régulièrement l'efficacité des programmes de sécurité d'une entreprise.
- **Gestion et intervention face aux incidents:** incluant la perte de la confidentialité, le compromis de l'intégrité de l'information, les dénis de service, l'accès ou non aux système, le vol ou le dommage aux systèmes, etc.

Importance de la gestion de la sécurité de l'information

Inventaire et classification des actifs informationnels

- Le contrôle efficace exige un inventaire détaillé des actifs informationnels.
- Une telle liste constitue la première étape dans la classification des actifs et dans l'établissement du niveau de protection devant être fourni pour chaque actif.
- L'inventaire doit inclure:
 - L'identification spécifique de l'actif
 - La valeur relative pour l'entreprise
 - L'emplacement
 - La classification de sécurité/risque
 - Le groupe d'actif
 - Le propriétaire de l'actif
 - Le détenteur de l'actif
 - Le niveau d'accès autorisé
 - L'étendue et la profondeur des contrôles de sécurité

Importance de la gestion de la sécurité de l'information

Inventaire et classification des actifs informationnels

- La classification des actifs informationnels réduit le risque et le coût de surprotection ou de sous-protection des ressources d'information en liant la sécurité avec les objectifs opérationnels.
- Les données doivent toujours être traitées comme un actif essentiel des SI.
- L'adoption d'un programme de classification et l'attribution de l'information à un niveau de sensibilité permet un traitement uniforme des données, par le biais de l'application par niveau de politiques et de procédures spécifiques plutôt que d'aborder chaque type d'information.

Importance de la gestion de la sécurité de l'information

Inventaire et classification des actifs informationnels

- Il s'avère très difficile de se conformer aux politiques de sécurité de l'information si les documents et les médias ne sont pas affectés à un niveau de sensibilité et que les utilisateurs ne sont pas informés de la manière dont ils doivent traiter chaque pièce d'information.

Information publique	Brochures de l'entreprise
Information privée	Politiques internes, procédures, message d'entreprise par courriel habituels, bulletin d'information, etc.
Information sensible	Etats financiers non publiés, secrets d'entreprise, etc.

Importance de la gestion de la sécurité de l'information

Autorisation d'accès au système

- Prérogative pour agir sur une ressource informatique. Cela fait référence à un privilège technique, par exemple la capacité de lire, de créer, de modifier ou de supprimer un fichier ou une donnée, d'exécuter un programme ou d'ouvrir ou d'utiliser une connexion externe.
- L'accès système aux ressources d'information informatisées est établi, géré, et contrôlé au niveau **physique** et/ou **logique**:
 - Les contrôles d'accès physiques restreignent l'entrée et la sortie du personnel d'un endroit comme un édifice à bureaux, une suite, un centre de données ou une salle qui contient des équipements de traitement de l'information tel qu'un serveur de réseau local.
 - Les contrôles d'accès logiques restreignent l'accès aux ressources logiques du système.

Importance de la gestion de la sécurité de l'information

Autorisation d'accès au système

- Les accès aux systèmes physiques ou logiques de n'importe quelle information automatisée doivent être basés sur un principe d'accès sélectif documenté dans lequel on retrouve une exigence d'affaires légitime basée sur le droit d'accès minimum et la séparation des tâches.
- Les changements de personnel et de départements, les efforts malveillants et tout simplement un manque de diligence entraînent un niveau d'autorisation inadéquat et peuvent avoir un impact sur l'efficacité des contrôles d'accès, d'où la nécessité d'un contrôle régulier.

Importance de la gestion de la sécurité de l'information

Contrôle d'accès obligatoire (MAC)

- Les accès sont entièrement définis dans la politique de sécurité de l'entreprise;
- L'accès est accordé par comparaison de la sensibilité de la ressource d'information et de la cote de sécurité de l'entité qui demande l'accès;
- Les utilisateurs ou les propriétaires de données ne peuvent modifier les filtres de contrôle d'accès;
- Ils sont prohibitifs, i.e. tout ce qui n'est pas expressément permis est interdit.

Importance de la gestion de la sécurité de l'information

Contrôle d'accès discrétionnaire (DAC)

- L'accès est accordé suivant l'identité du système demandant l'accès, ou du groupe auquel il appartient;
- L'accès peut être accordé ou modifié par le propriétaire de la donnée à sa discrétion;
- L'accès peut être hérité;
- Les contrôles d'accès discrétionnaires ne peuvent pas primer sur les contrôles d'accès obligatoires;

Importance de la gestion de la sécurité de l'information

Rôle des auditeurs et Gestion de la confidentialité

- Soutenir ou réviser l'analyse d'impact de confidentialité:
 - Déterminer la nature de l'information personnellement identifiable associé avec les procédés d'affaires.
 - Documenter la cueillette, l'utilisation, la divulgation et la destruction de l'information personnellement identifiable.
 - Assurer qu'il existe une imputabilité pour les problèmes de vie privée.
 - Identifier les exigences législatives, réglementaires et contractuelles en matière de vie privée pour en assurer la conformité.
 - Etre fondement de décisions éclairées sur la politique, les activités et la conception du système en fonction de la compréhension du risque de confidentialité.

Importance de la gestion de la sécurité de l'information

Rôle des auditeurs et Gestion de la confidentialité

- Donner l'assurance aux gestionnaires de la conformité des politiques aux lois et règlements:
 - Identifier et comprendre les exigences juridiques au sujet de la confidentialité dans les lois, réglementations et ententes contractuelles.
 - Vérifier si les données personnelles sensibles sont gérées correctement par rapport aux exigences.
 - Vérifier que les mesures de sécurité adéquates sont adoptées.
 - Réviser la politique de confidentialité de la gestion pour s'assurer qu'elle tient compte des lois et des règlements applicables concernant la confidentialité.

Importance de la gestion de la sécurité de l'information

Problèmes et exposition aux crimes informatiques (Menaces)

- Les systèmes informatiques peuvent être utilisés pour obtenir frauduleusement de l'argent, des biens, des logiciels, ou de l'information d'entreprise.
- Les crimes informatiques peuvent se produire sans que rien ne soit physiquement pris ou volé, et ils peuvent être effectués aussi facilement qu'en ouvrant une session à partir de la maison ou d'un restaurant.
- Les crimes qui exploitent l'ordinateur et les renseignements qu'il contient peuvent être dévastateurs pour la réputation, le moral et la permanence d'une entreprise. Il peut en résulter la perte de clients ou d'une part du marché, l'embarras de la direction et des procédures judiciaires entreprises contre l'entreprise.
- Les menaces à l'entreprise comprennent :

Importance de la gestion de la sécurité de l'information

Problèmes et exposition aux crimes informatiques (Menaces)

- **Les pertes financières:** Les pertes directes ou indirectes comme les frais encourus pour corriger l'exposition.
- **Les répercussions légales:** Si une entreprise n'est pas dotée de moyens de sécurité appropriés, elle peut être exposée à des poursuites de la part des investisseurs et des assureurs si une perte significative survient après une infraction de sécurité.
- **Les pertes de crédibilité ou d'avantages concurrentiels:** Des firmes de services comme les banques, les firmes d'épargne, de prêts et d'investissement, ont besoin de crédibilité et de la confiance du public pour maintenir leur avantage concurrentiel. Une infraction à la sécurité peut miner sérieusement la crédibilité, ce qui entraîne une perte d'affaire et de prestige.

Importance de la gestion de la sécurité de l'information

Problèmes et exposition aux crimes informatiques (Menaces)

- **Le chantage, l'espionnage industriel ou le crime organisé:** En ayant accès à l'information confidentielles ou à un moyen d'influencer négativement les activités informatiques, un auteur de crime peut extorquer des paiements ou des services d'une entreprise en menaçant d'exploiter les brèches de sécurité ou de divulguer publiquement les informations confidentielles de l'entreprise.
- **La divulgation d'informations confidentielles, sensibles ou embarrassantes:** Tel que mentionné précédemment, de tels événements peuvent endommager la crédibilité d'une entreprise et ses moyens de faire des affaires. Des actions légales ou réglementaires contre l'entreprise peuvent aussi être le résultat de la divulgation.
- **Le sabotage:** Quelques auteurs de crime ne veulent pas de gains financiers mais sont plutôt animés de sentiments divers tels que la haine ou le besoin de satisfaction personnelle.

Importance de la gestion de la sécurité de l'information

Problèmes et exposition aux crimes informatiques (Auteurs)

Les auteurs des crimes informatiques sont souvent les mêmes qui exploitent les expositions physiques, même si les aptitudes nécessaires pour exploiter les expositions logiques sont plus techniques et complexes.

Les auteurs possibles incluent :

- **Les pirates informatiques:** individus tentant de briser la sécurité du système de quelqu'un d'autre ou, d'y accéder sans en être invité.
- **Les pirates adolescents:** individus utilisant des scripts et des programmes écrits par d'autres pour effectuer leurs intrusions. Ils sont souvent incapables de les écrire par eux même.

Importance de la gestion de la sécurité de l'information

Problèmes et exposition aux crimes informatiques (Auteurs)

- **Les employés (autorisés ou non autorisés):** affiliés à l'entreprise et possédant un accès au système en raison de leurs responsabilités professionnelles, ces personnes peuvent causer un grand préjudice à l'entreprise.
- **Les employés des SI:** possèdent l'accès le plus facile aux renseignements informatiques puisqu'ils en sont responsables.
- **Les utilisateurs finaux:** personnel possédant souvent une grande connaissance de l'information au sein de l'entreprise et qui possède un accès facile aux ressources internes.
- **Les anciens employés:** peuvent avoir un accès aux systèmes si ce dernier n'a pas été automatiquement révoqué au moment de la cessation d'emploi, ou si le système possède des « portes dérobées ».

Importance de la gestion de la sécurité de l'information

Problèmes et exposition aux crimes informatiques (Auteurs)

- **Les tiers intéressés ou éduqués:** peuvent comprendre les concurrents, les terroristes, les pirates, etc.
- **Les employés temporaires:** par exemple le personnel d'entretien des bureaux possède un grand nombre d'accès physique et pourrait perpétrer un crime informatique.
- **Tierces parties:** fournisseurs, visiteurs, consultants, et d'autres tierces parties qui, par des projets, obtiennent l'accès aux ressources de l'entreprise et pourrait perpétrer un crime.
- **Les ignorants accidentels:** quelqu'un qui, sans le savoir, perpète une infraction.

Importance de la gestion de la sécurité de l'information

Méthodes et techniques d'attaque

- Attaque par altération
- Réseau zombie
- Attaque de force
- Déni de service
- Ecoute illégale
- Bombardement de courriel et pourriel
- Courriels frauduleux
- Code malveillant
- Enumération des ressources et furetage
- Attaque de l'homme du milieu
- Usurpation d'identité
- Analyse de réseau
- Réinjection de paquets
- Hameçonnage
- Talonnage
- Outils d'entretien à distance
- Saucissonnage
- War chalking, war driving, war walking

Importance de la gestion de la sécurité de l'information

Identification et Authentification

- Processus par lequel le système obtient d'un utilisateur son identité proclamée et les justificatifs d'identité nécessaires pour authentifier cette identité et valider les deux éléments d'information.
- Nécessaire pour établir la responsabilité de l'utilisateur.
- L'indentification permet de **connaître** l'identité d'un individu, alors que l'authentification permet de **vérifier** cette identité.
- Trois catégories d'authentification:
 - Ce que l'on connaît (ex. mot de passe)
 - Ce que l'on possède (ex. badge d'accès)
 - Ce que l'on est (ex. biométrie)
- L'authentification multifactorielle améliore le niveau de protection.

Importance de la gestion de la sécurité de l'information

Mot de passe forts

Au minimum, les règles suivantes doivent être appliquées afin de renforcer un mot de passe:

- Idéalement, être d'une longueur minimale de huit caractères;
- Exiger une combinaison d'au moins trois des caractéristiques suivantes : alpha, numérique, lettres majuscules et minuscules ainsi que des caractères spéciaux;
- Ne doivent pas être particulièrement identifiable à l'utilisateur (prénom, nom, nom de l'épouse, ...);
- Le système doit exiger des changements de mot de passe réguliers et ne doit pas permettre à d'anciens mots de passe d'être utilisés au moins un an après avoir été changé.

Importance de la gestion de la sécurité de l'information

Autorisation

- Le processus d'autorisation utilisé pour le contrôle d'accès exige que le système soit en mesure d'identifier les utilisateurs et de les différencier entre eux.
- Les règles d'autorisation spécifient qui peut avoir accès à quoi.
- Les restrictions d'accès au niveau des fichiers incluent généralement les fonctions suivantes:
 - Lire, demander les informations ou copier seulement;
 - Ecrire, créer, mettre à jour ou supprimer seulement;
 - Exécuter seulement;
 - Une combinaison des énoncés ci-haut.

Importance de la gestion de la sécurité de l'information

Sécurité d'un réseau local (Les Risques)

- Les LAN facilitent le stockage et l'extraction des programmes et des données utilisés par un groupe de personnes.
- Les logiciels destinés aux réseaux locaux ne procurent qu'un faible niveau de sécurité. L'accent étant mis sur les capacités et les fonctionnalités plutôt que sur la sécurité.
- Les risques associés à l'utilisation des réseaux locaux inclus entre autres :
 - La perte de l'intégrité des données suite aux modifications non autorisées;
 - Le manque de protection des données courantes;
 - L'exposition à des activités externes à cause d'une vérification limitée des utilisateurs;
 - L'infection informatique par des virus ou vers;
 - La divulgation inappropriée des données;
 - La violation des licences;
 - L'accès illégal par l'usurpation de l'identité d'un utilisateur du réseau local;
 - Le renfilage d'information relative à un utilisateur interne;
 - La mystification d'un utilisateur interne;
 - La destruction des données de journalisation et d'audit.

Importance de la gestion de la sécurité de l'information

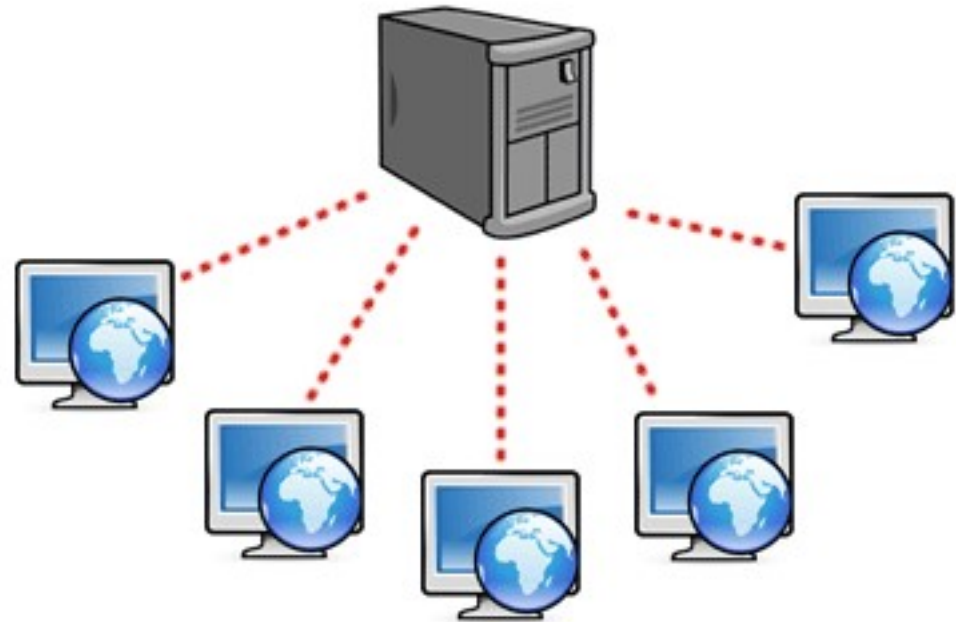
Sécurité d'un réseau local (Gestion de la sécurité)

- Les dispositions relatives à la sécurité du réseau local LAN dépendent du logiciel, de sa version et de son implantation.
- Les capacités de gestion de la sécurité du réseau normalement disponibles comprennent notamment :
 - La déclaration de la propriété des programmes, des fichiers et du stockage;
 - La restriction de l'accès à la consultation seule;
 - La mise en place du verrouillage des enregistrements et fichiers afin d'empêcher la mise à jour simultanée;
 - La mise en place des procédures d'ouverture de session par ID et mot de passe avec des règles relatives à la longueur, au format et à la fréquence de mise à jour du mot de passe;
 - L'utilisation de commutateurs pour implanter des politiques de sécurité des points d'accès, afin d'empêcher des hôtes inconnues de se brancher sur le réseau;
 - L'encryptage du trafic local en utilisant le protocole IPSec.

Importance de la gestion de la sécurité de l'information

Sécurité Client-Serveur

- L'environnement client-serveur désigne un mode de communication à travers un réseau entre plusieurs programmes ou logiciels: l'un, qualifié de client, envoie des requêtes; l'autre ou les autres qualifiés de serveurs, attendent les requêtes des clients et y répondent.
- Un système client-serveur possède de nombreux points d'accès.
- Les systèmes client-serveur utilisent des techniques réparties, ce qui accroît le risque d'accès aux données et au traitement.



Importance de la gestion de la sécurité de l'information

Sécurité Client-Serveur

- Les mesures de protection d'une architecture Client-Serveur comprennent:
 - Identification de tous les points d'accès;
 - Désactivation des lecteurs de disque et port USB ...;
 - Analyse de l'activité des utilisateurs connus et inconnus;
 - Cryptage des données sensibles;
 - Implémentation des méthodes d'authentification multifactorielles;
 - Formation des utilisateurs.

Importance de la gestion de la sécurité de l'information

Sécurité du réseau sans fil

- Dans le cas des réseaux sans fil, les objectifs principaux sont de garantir la confidentialité, l'intégrité, l'authenticité et la disponibilité.
- La garantie que les ressources ne sont utilisées qu'aux fins prévues fait aussi partie de la disponibilité.
- Les risques liés aux réseaux sans fil sont égaux à la somme des risques liés au fonctionnement d'un réseau câblé et des nouveaux risques introduits par la faiblesse des protocoles sans fil. Afin d'atténuer ces risques, une organisation doit adopter des mesures et des pratiques qui permettront de gérer ces risques.
- Les entités malveillantes possèdent de nombreux moyens pour accéder aux dispositifs sans fil. Ceux qui sont liés aux réseaux locaux sans fil (WLAN) comprennent, entre autres, trois formes de piratage Wi-Fi : les **war driving**, **war walking** et **war chalking**.

Importance de la gestion de la sécurité de l'information

Sécurité du réseau sans fil

- Les exigences de sécurité comprennent notamment :
 - **L'authenticité** : Une tierce partie doit être apte à vérifier que le contenu d'un message n'a pas été modifié en cours de transmission.
 - **La non-répudiation** : L'origine ou la réception d'un message précis doit être vérifiable par une tierce partie.
 - **La responsabilité** : Les actions d'une entité ne doivent être retraçables qu'à cette entité.
 - **La disponibilité** : Les ressources des TI doivent être disponibles au moment opportun afin de satisfaire les exigences de la mission ou pour éviter des pertes substantielles.

Politique et administration de la sécurité des SI: Introduction aux normes ISO 27000

La famille ISO 2700x

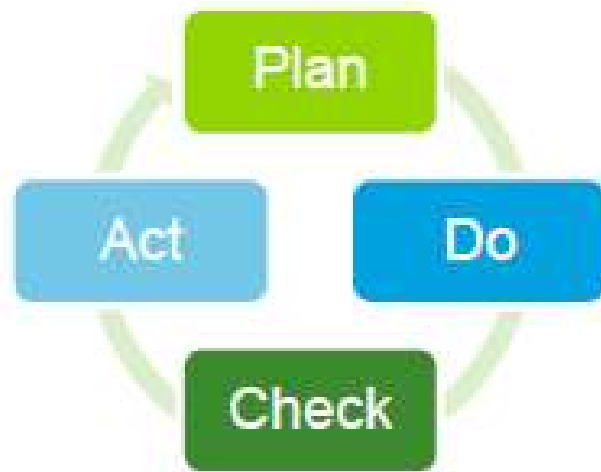


Quel cadre pour la mise en œuvre et l'audit de la sécurité de l'information?

La sécurité de l'information est régie principalement par deux normes:

- ISO 27001 : Cadre de gestion la sécurité
- ISO 27002 : Liste des contrôles (meilleures pratiques)

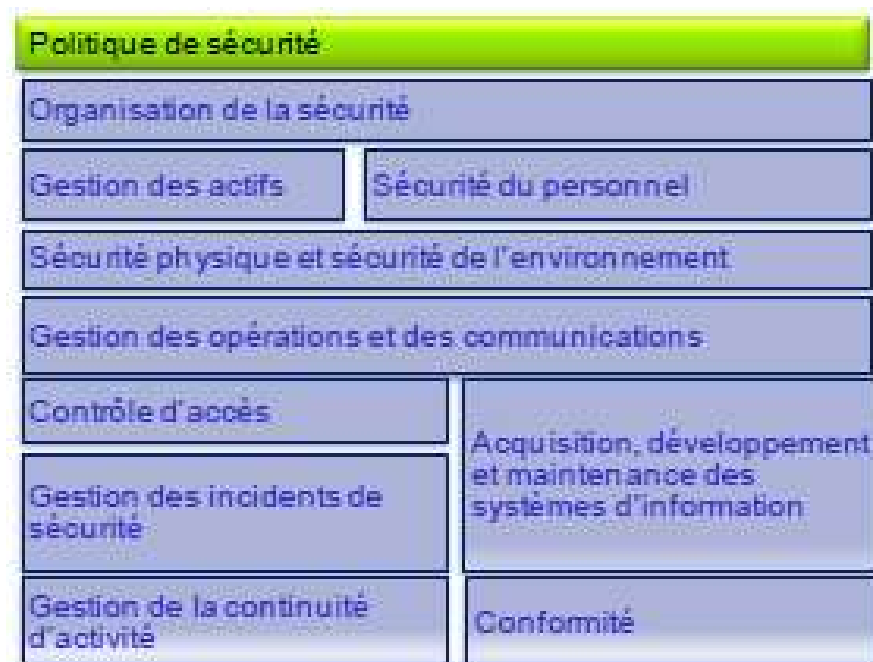
ISO 27001



Comment m'organiser pour gérer la sécurité?

14/07/2016

ISO 27002

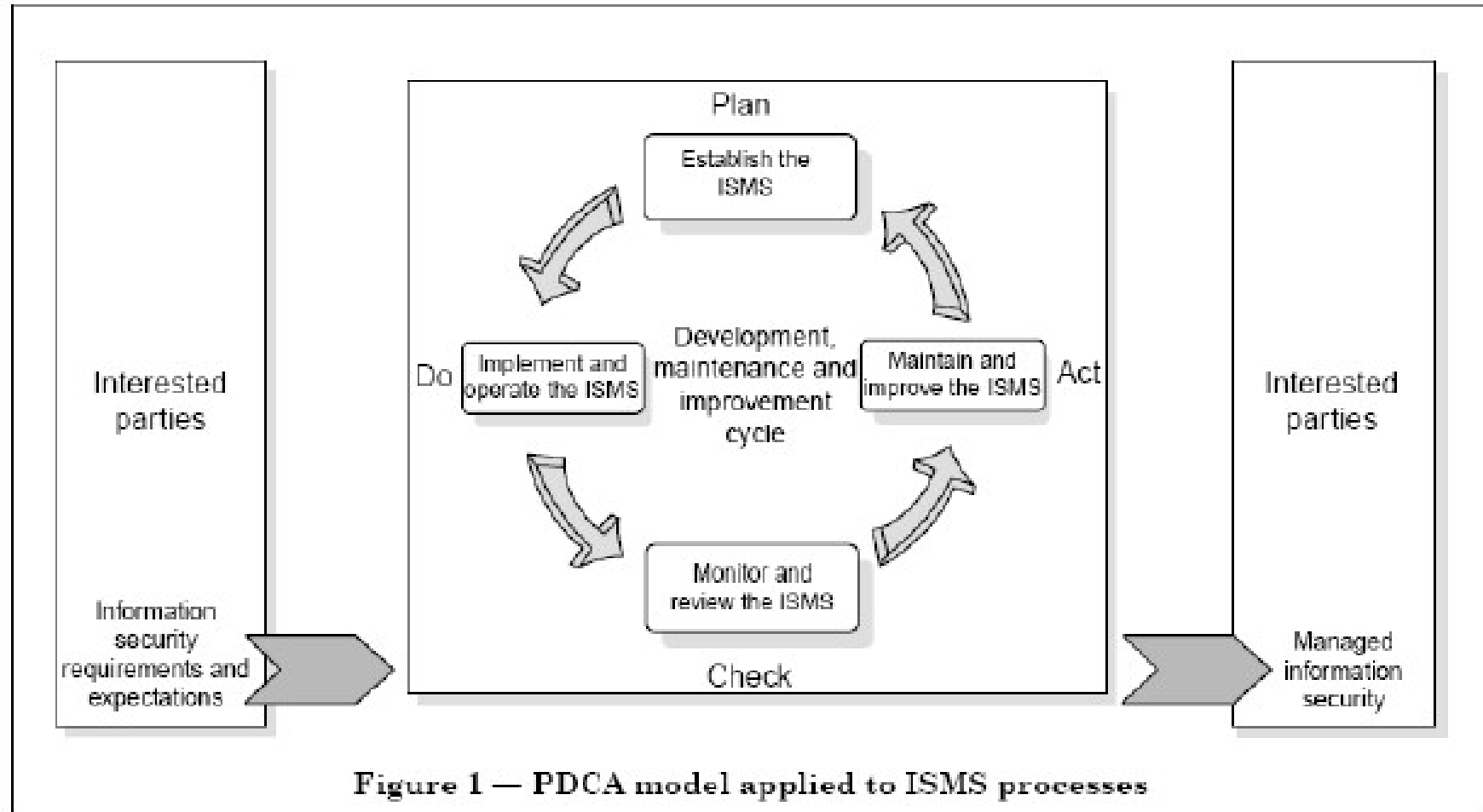


Quels sont les objectifs de contrôles pour:

- Mettre en œuvre la sécurité,
- Auditer la sécurité.

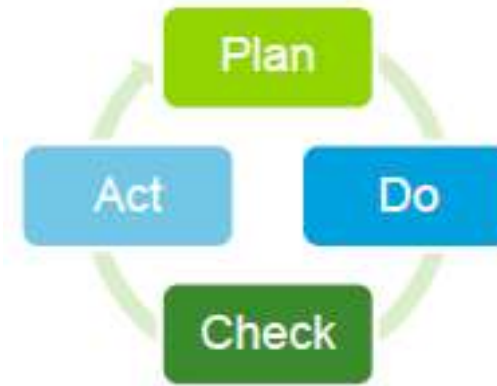
ISO 27001

Cycle de vie du système de gestion de la sécurité de l'information (SGSI)



ISO 27001

Certifier le système de gestion de la sécurité de l'organisation



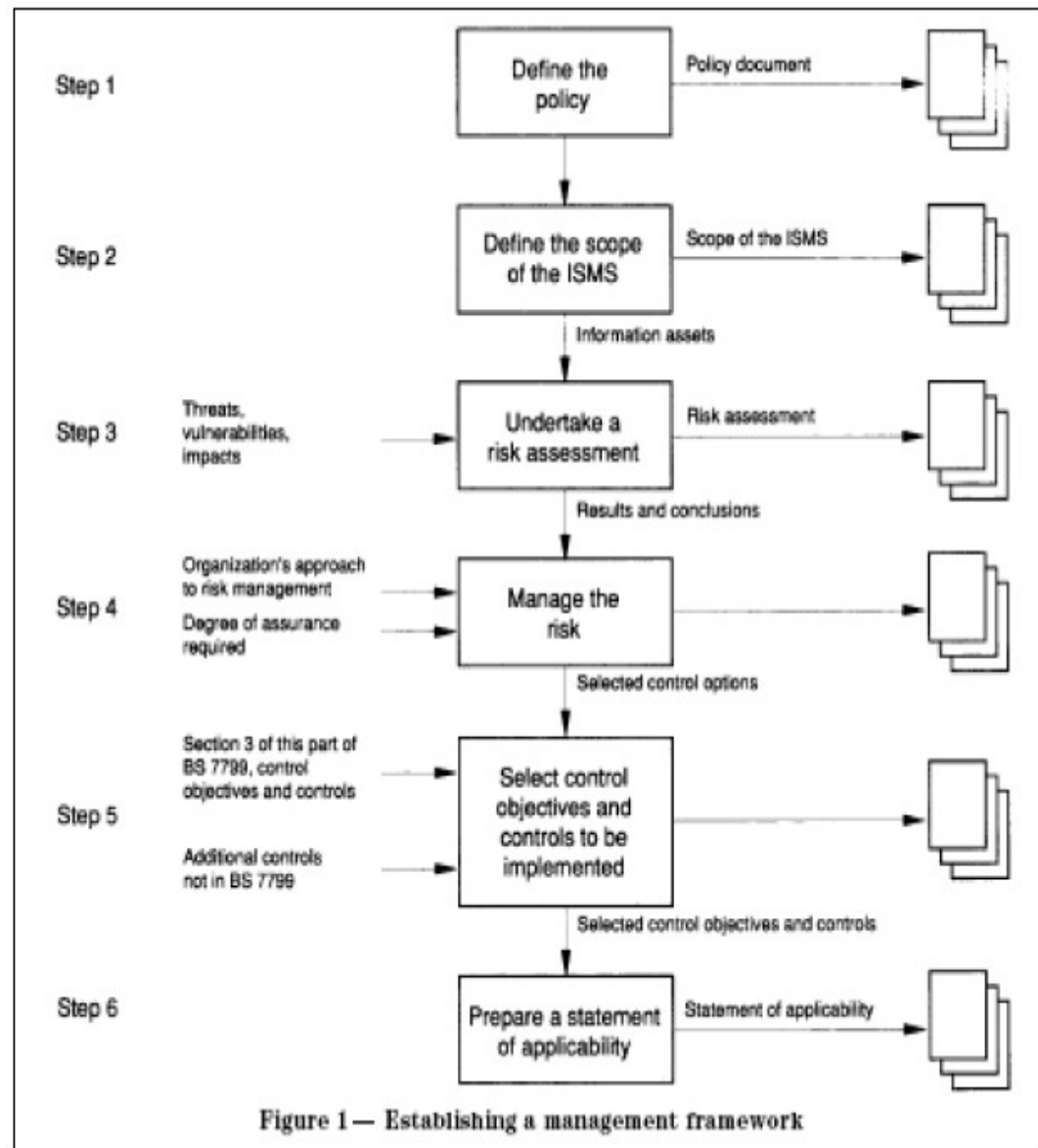
Mettre en place un système/cadre de gestion de la sécurité (ISMS)

1. Définir le périmètre sur lequel le système de gestion de la sécurité de l'information s'applique (Cœur d'activité de l'organisation)
2. Définir une politique de gestion de la sécurité (ISMS)
3. Définir une méthodologie d'évaluation des risques (elle doit produire des résultats comparables et reproductibles)
4. Identifier les risques
5. Evaluer les risques et identifier la méthode de gestion du risque
6. Sélectionner les contrôles de la norme ISO 27002 permettant pallier les risques
7. Faire approuver le dispositif
8. Préparer un «Statement of Applicability» : Liste des contrôles de la norme ISO 27002 qui sont applicable ou non à l'organisation (toute exclusion doit être justifiée)

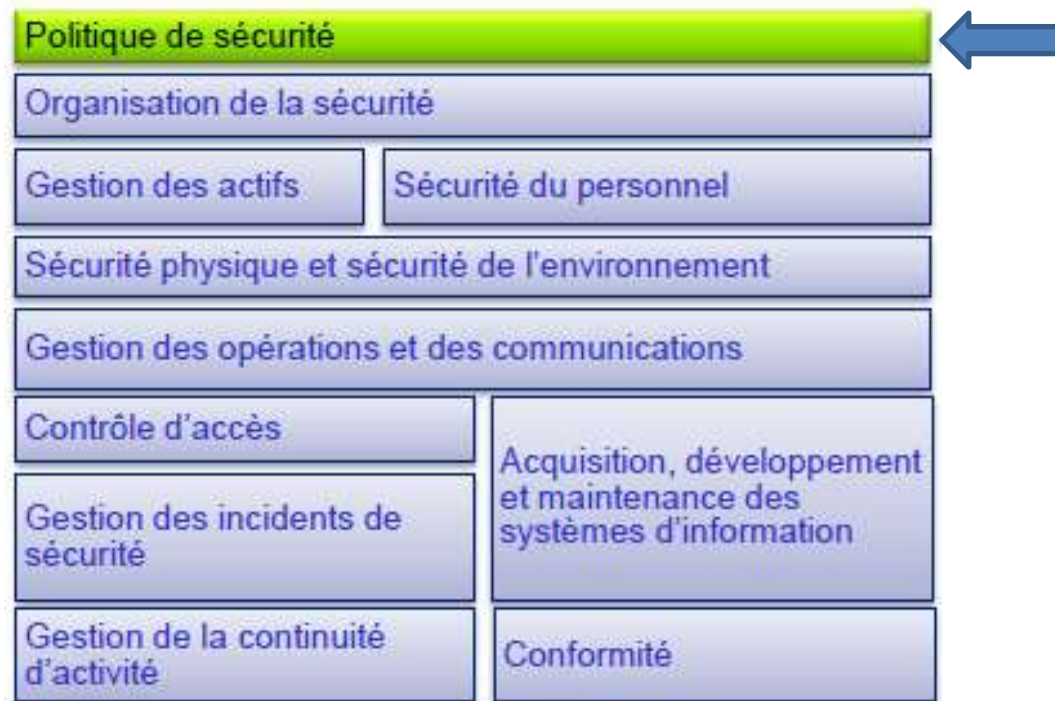
ISO 27001

Cadre de gestion de la sécurité

- La norme impose l'établissement d'un système de gestion de la sécurité de l'information (SGSI), décrit dans un cadre de gestion.
- Les objectifs et mesures de contrôle doivent être mis en œuvre et documentés.
- La documentation doit être contrôlée.
- Des registres matérialisant les contrôles doivent être maintenus.



« Chez nous, il n'y a rien à protéger »



Politique de sécurité:

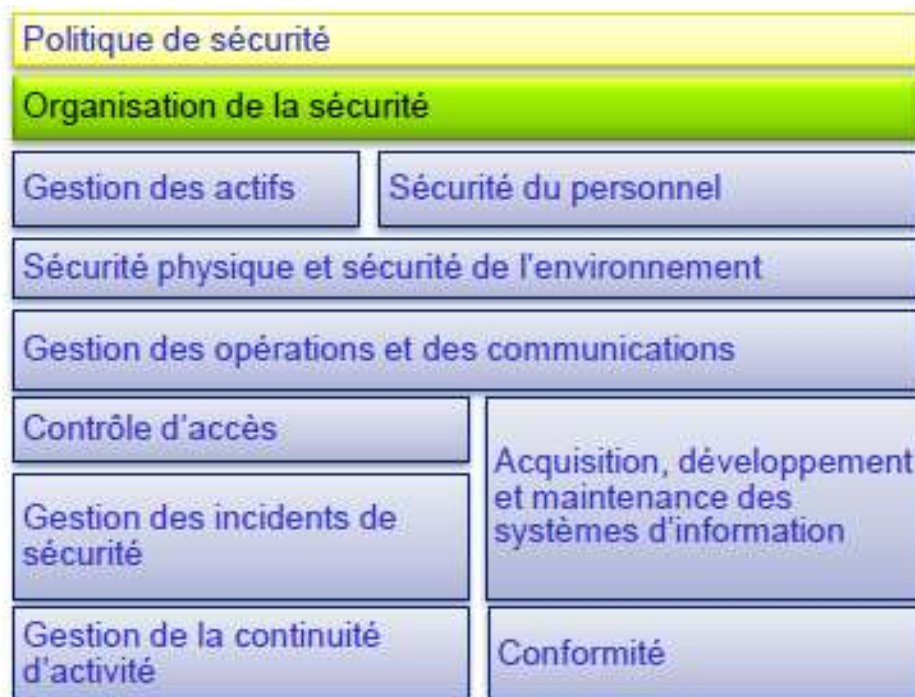
Une politique de sécurité informatique est un plan d'actions définies pour maintenir un certain niveau de sécurité. Elle reflète la vision stratégique de la direction de l'organisme en matière de sécurité informatique.



Par où commencer ?

- Obtenir un soutien de la direction dans le domaine de la sécurité de l'information.
- Formaliser des objectifs globaux de sécurité dans un document.
- Porter ce document à la connaissance de tous les employés.
- Un engagement de respect des règles de sécurité peut être formalisé et signé par chaque employé.

« C'est pas moi, c'est lui »



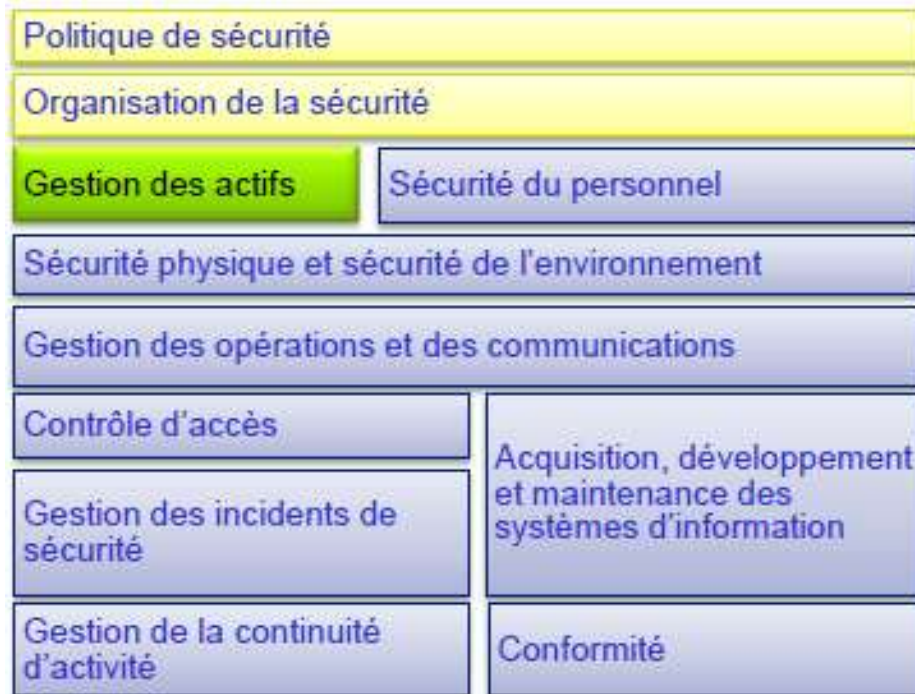
Organisation de la sécurité:

préciser les rôles et responsabilités des gestionnaires, utilisateurs, contractuels et fournisseurs de services, propriétaires d'actifs informationnels. Détailler également les mécanismes de sécurité à mettre en place pour assurer la sécurisation de l'accès des tiers aux informations et ressources de l'entreprise.

Par où commencer ?

- La nomination du (ou des) responsables est effectuée par la Direction.
- Formaliser les responsabilités relatives à la sécurité dans les fiches de postes.
- Les modalités d'accès aux ressources et aux locaux par des tiers doivent avoir été prédéfinies. Un engagement de respect des règles de sécurité peut être formalisé et signé par chaque sous-traitant.

« Qui s'occupe de ça? »



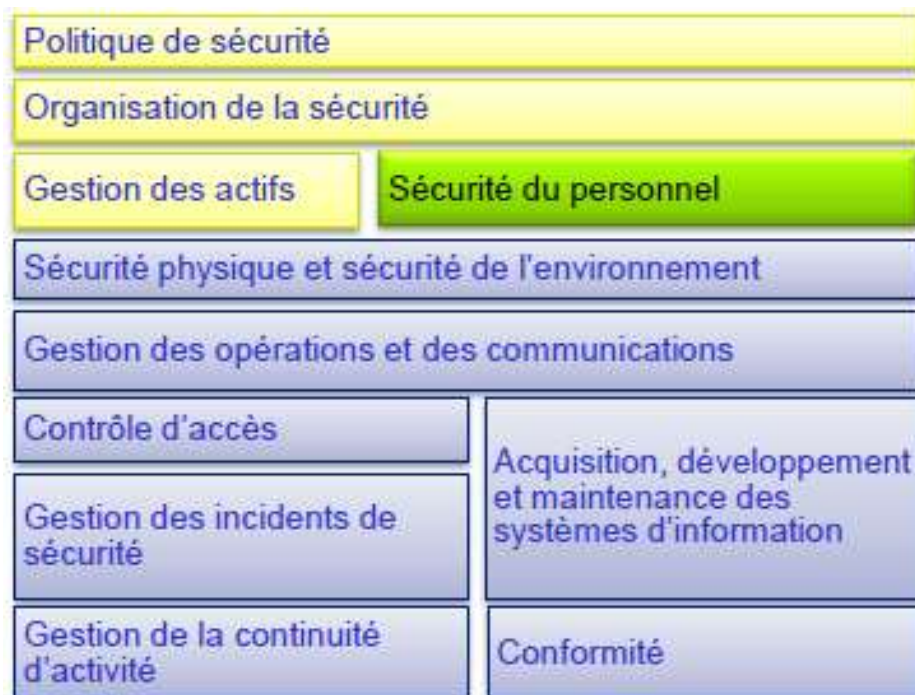
Gestion des actifs:

Procéder à l'inventaire des actifs informationnels; leur déterminer un propriétaire; les catégoriser; déterminer leur niveau de protection et établir les mesures de sécurité à mettre en place selon leur contexte d'utilisation.

Par où commencer ?

- Elaborer un inventaire des ressources majeures de l'entreprise. Cet inventaire peut contenir les actifs physiques (matériel informatique, moyen de communication, support amovible), les logiciels, les informations (bases et fichiers de données, contrats et accords, procédures opérationnelles ...), les services informatiques et de télécommunication, de support (climatisation, éclairage,...), les personnes et leur qualifications/savoir-faire/expériences, les valeurs immatérielles comme la réputation et l'image de l'organisme.
- Le niveau de classification doit permettre d'identifier le niveau d'importance de l'actif pour l'entreprise et par là-même, les mesures de protection appropriées.

« Je ne le savais pas »



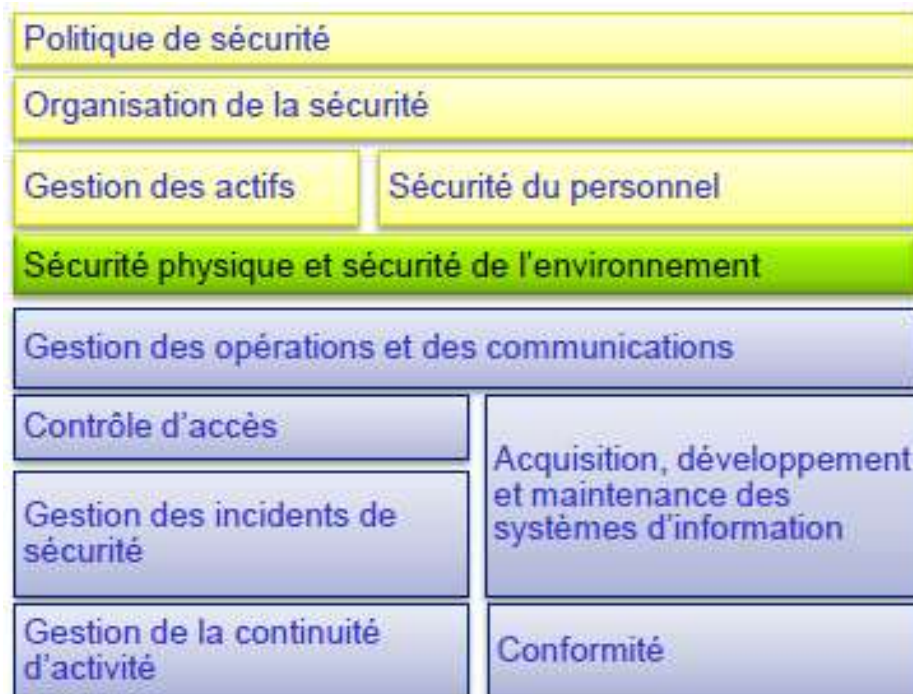
Sécurité du personnel:

Indiquer au personnel les bonnes pratiques à utiliser pour protéger les renseignements confidentiels et nominatifs, faire un bon usage de leur équipement informatique selon les normes et les règles et mettre en place un programme de sensibilisation à la sécurité de l'information de même qu'une procédure d'accueil des nouveaux employés.

Par où commencer ?

- La sensibilisation peut être effectuée au travers de publications (intranet, courriels, articles), d'une session de sensibilisation des nouveaux entrants, d'une formation périodique de tout le personnel, de dépliants, etc. Elle se fera dans le cadre du **programme de sensibilisation sur la sécurité de l'information**.
- Demander aux responsables de s'assurer que les personnes sous leur responsabilité ont été sensibilisées.
- Formaliser une procédure applicable lors du départ d'un collaborateur (Réattribution des responsabilités dans le domaine de la sécurité, retour des actifs, suspension des droits d'accès).

Toute sécurité commence par la sécurité physique



Sécurité physique et sécurité de l'environnement:

Préciser les mesures à mettre en place pour sécuriser le matériel et éviter les accès non autorisés dans les locaux, de même que les dommages pouvant affecter les actifs informationnels et les opérations quotidiennes.

Par où commencer ?

- Mettre en place un dispositif de contrôle d'accès aux zones contenant les ressources majeures de l'entreprise (clés, digicode, badge).
- Mettre en place un dispositif de protection contre l'incendie (porte coupe-feu, alarme incendie, dispositif d'extinction).
- Vérifier que l'activité ne se trouve pas dans une zone inondable en période d'hivernage.

La sécurité opérationnel au quotidien



Gestion des opérations et des communications:

Indiquer comment sécuriser les communications et les informations échangées avec les partenaires et clients; assurer la sécurité des réseaux de télécommunication, des systèmes d'exploitation et des applications.

Par où commencer ?

- Désactiver les services non utilisés des équipements informatiques (installation par défaut).
- S'équiper d'une solution de protection contre les codes malveillant et mobiles (antivirus sur les postes de travail, sur les serveurs, anti-virus de messagerie).
- Cloisonner les sous-réseaux (switch).
- Mettre en place des dispositifs de filtrage applicatif (pare-feu, proxy, IPS/IDS...).
- En cas d'utilisation de réseaux Wifi, utiliser WPA.

« Login: TOTO – Password: TOTO »



Contrôle d'accès:

Gérer et contrôler les accès logiques et physiques aux informations et ressources; détecter les activités non autorisées; préciser les règles à observer concernant l'identifiant et le mot de passe, de même que les autorisations reliées au profil d'accès.

Par où commencer ?

- Mettre en place une **stratégie de mot de passe** (longueur minimale de 8 caractères, obligation d'utiliser des caractères étendus, obligation de renouvellement tous les 3 mois, impossibilité de réutiliser un des trois derniers mots de passe).
- Activer les mises en veille après 2 minutes d'inactivité avec une protection par mot de passe.
- Bloquer l'accès à un compte après 3 tentatives d'accès infructueuses.
- Créer des **comptes nominatifs** (bannir les comptes génériques).
- Mettre en place une stratégie de moindre privilège.

La sécurité est d'autant plus coûteuse qu'elle est intégrée tardivement



Acquisition, développement et maintenance des systèmes d'information :

indiquer les règles de sécurité à observer ou à exiger dans l'acquisition, le développement, l'implantation et l'entretien d'applications et de logiciels.

Par où commencer ?

- Spécifier les exigences de sécurité dès l'origine du projet.
- Formaliser les règles d'ajout, de modification et de suppression de tout matériel ou logiciel sur le réseau de production.
- Mettre en place **une veille sur les vulnérabilités** (éditeur anti-virus, CERT,...).
- Mettre à jour** régulièrement les logiciels et les systèmes d'exploitation en téléchargeant les correctifs (de sécurité).

Limiter les dégâts et éviter de recommencer



Gestion des incidents de sécurité:

indiquer les comportements à adopter lors de la détection d'un incident ou d'un dysfonctionnement de sécurité; mettre en place un processus de gestion des incidents de sécurité.

Par où commencer ?

- Paramétrer les **fichiers de trace** (journaux) des équipements afin que soient enregistrés au moins les connexions infructueuses et les erreurs de fonctionnement.
- Analyser régulièrement les fichiers de trace des équipements.

« Ca n'arrive pas qu'aux autres »



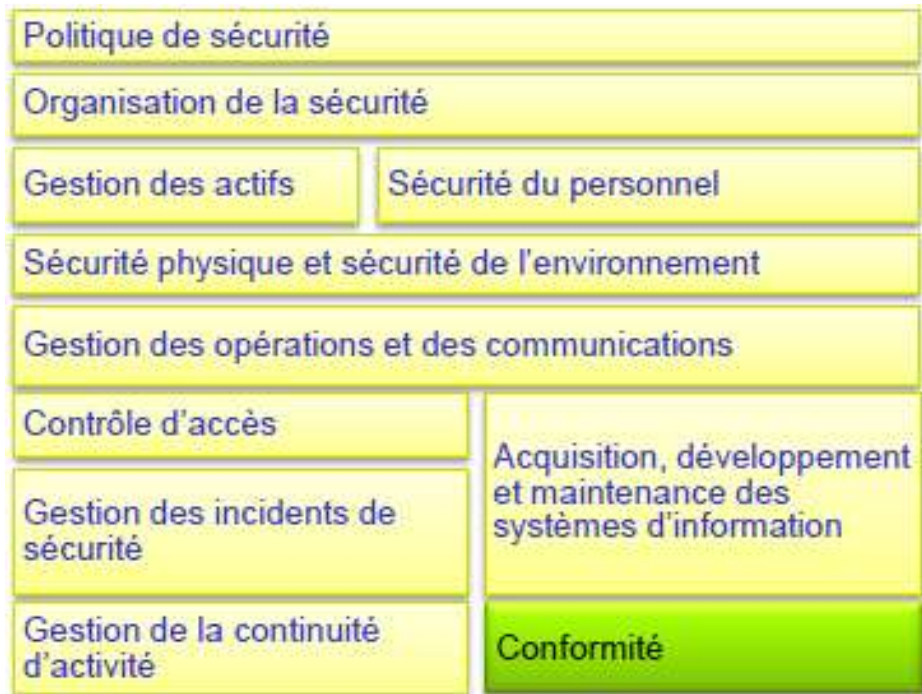
Gestion de la continuité:

décrire les façons de faire pour élaborer un plan de continuité et de relèvement des services, de même qu'un plan de sauvegarde des données et des applications de l'entreprise.

Par où commencer ?

- Sauvegarder régulièrement les données. Externaliser les données sauvegardées. Procéder à des tests de restauration.
- Identifier le temps d'indisponibilité maximal tolérable pour chaque processus de l'organisation.
- Identifier les principaux scénarios (2 ou 3) de risque auxquels pourrait être confrontée l'organisation (inaccessibilité des locaux, panne du principal serveur de production, panne électrique, etc.).
- Elaborer un plan d'action pour chacun des scénarios envisagés (en conformité avec le temps d'indisponibilité maximal tolérable).

« Nul n'est censé ignorer la loi »



Conformité:

Décrire comment s'assurer du respect des lois et des réglementations, ainsi que de l'efficacité des procédures, de même que des mesures de sécurité en place, en relation avec la politique de sécurité de l'information édictée par l'entreprise.

Par où commencer ?

- Identifier les exigences auxquelles l'organisation est soumise :
 - +Légales et réglementaires,
 - +Contractuelles,
 - +Sectorielles.
- Ne pas oublier les déclarations de la Commission de Protection des Données Personnelles (CDP), de la CDEAO, ni les licences des logiciels !

Mesures de contrôle ISO 27002

1. Politique de sécurité

2. Organisation de la sécurité

Infrastructure de la sécurité de l'information
Sécurité des accès par des tiers
Sous-traitance

3. Classification et contrôle des actifs

Responsabilités liées aux actifs
Classification de l'information

4. Sécurité du personnel

Sécurité dans la déf. Des postes et des ressources
Formation des utilisateurs
Réactions aux incidents de sécurité et aux mauvais fonctionnements

5. Sécu. physique et sécu. de l'environnement

Zones de sécurité
Sécurité du matériel
Mesures générales

6. Gestion des communications et des opérations

Procédures et responsabilités opérationnelles
Planification et recette des systèmes
Protection contre les logiciels pernecieux
Intendance
Gestion des réseaux
Manipulation et sécurité des supports
Échanges d'informations et de logiciels

7. Contrôle des accès

Exigences de l'entreprise concernant le contrôle des accès
Gestion des accès utilisateurs
Responsabilité des utilisateurs
Contrôle de l'accès aux réseaux
Contrôle de l'accès aux systèmes d'exploitation
Contrôle de l'accès aux applications
Surveillance des accès aux systèmes et de leur utilisation
Informatique mobile et télétravail

8. Développement et maintenance des systèmes

Exigences de sécurité des systèmes
Sécurité des systèmes d'applications
Mesures cryptographiques
Sécurité des fichiers
Sécurité des environnements de développement et de soutien

9. Gestion des incidents de sécurité

Signalement des événements de sécurité et faiblesses
Gestion des incidents de sécurité et des améliorations

10. Gestion de la continuité des activités de l'entreprise

Stratégie de continuité
Création et mise en œuvre des plans
Test et réévaluation des plans

11. Conformité

Conformité aux exigences légales
Examens de la politique de sécurité et de la conformité technique
Considérations concernant les audits des systèmes

Facteurs clés de succès

Pour assurer le succès de la gestion de la sécurité au sein d'une organisation:

- Définir une politique de sécurité correspondant à l'activité de l'organisation.
- Adopter une démarche de mise en œuvre de la gestion de la sécurité compatible avec la culture de l'organisation.
- S'assurer un soutien total et un engagement visible de la Direction.
- Bien comprendre les exigences de sécurité et bien évaluer les risques.
- Sensibiliser et informer efficacement tous les responsables et employés.
- Distribuer à tous les employés et à tous les fournisseurs les lignes directrices de la politique de sécurité et des normes de sécurité de l'information.
- Former de manière appropriée les acteurs de la sécurité.
- Mettre en place et faire vivre un système de mesure complet pour évaluer l'efficacité de la gestion de la sécurité de l'information et collecter les suggestions d'amélioration.

Panorama d'autres méthodes

- Schéma directeur de sécurité des systèmes d'information
 - MARION (Grands systèmes, Micro)
 - MEHARI (Architectures distribuées)
 - COBIT 5 *for Information security*
- Diagnostic de sécurité (audit / contrôle interne)
 - ERSI
- Critères d'évaluation
 - ITSEC et ISO 15408
- Méthodes de la DCSSI
- Norme de gestion et planification de la sécurité informatique et télécom
 - ISO 13335
- Modèle de maturité pour l'ingénierie de systèmes de sécurité
 - ISO 21827 (SSE-CMM)
- Norme organisationnelle et d'évaluation
 - BS 7799 / ISO 17799 / ISO 27001
- Référentiel de bonnes pratiques
 - ISF (Information Security Forum)

Analyse des risques

Analyse des risques

Définition

- **Risque** : La possibilité qu'une menace données exploite la vulnérabilité d'un actif ou d'un groupe d'actifs et cause ainsi un préjudice à l'organisation (ISO/IEC PDTR 13335-1).
- **Analyse de Risque (AR)** : Technique d'identification et d'évaluation des facteurs susceptible de compromettre un processus ou un objectif.
- L'AR = Evaluation -> Atténuation -> Ré évaluation.

Analyse des risques

Evaluer les contre-mesures

- **Analyse coût / bénéfiques** : Choisir les méthodes de gestion des risques adéquates en se basant sur :
 - Le coût de la mesure de contrôle en comparaison au degré de réduction du risque
 - La propension de la haute direction au risque
 - La/Les méthode(s) de réduction du risque privilégiée(s)

Analyse des risques

Objectifs et Besoins

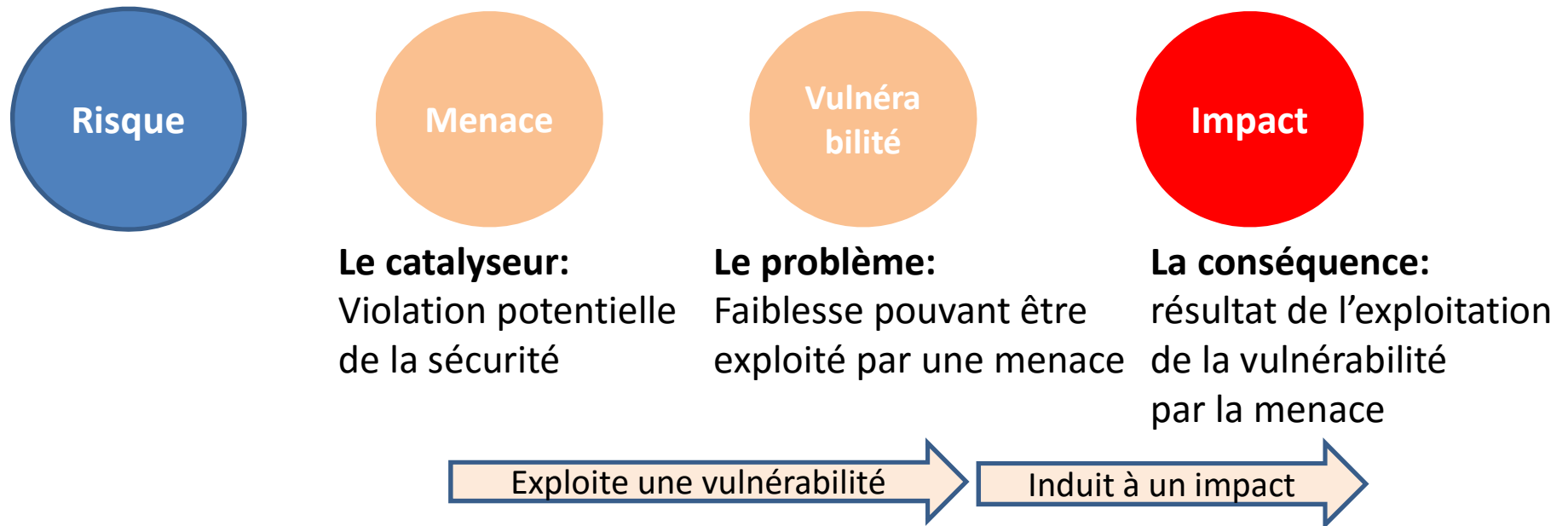
- **Identifier et évaluer les risques** en fonction des:
 - Types d'impact (Impacts métiers, financiers, clients, juridiques, image de marque, etc.)
- **Définir les mesures de sécurité** pour réduire les risques identifiés par l'implémentation des meilleures mesures de contrôle interne.
- **Garantir la continuité des activités**
- **Protéger contre les activités et tentatives de fraude**
- **Adapter les décisions stratégiques** en fonction du niveau de criticité des risques encourus
- **Etre en conformité** avec la réglementation en vigueur

Analyse des risques

Menace, vulnérabilité, impact, risque

- Le niveau de criticité de chaque risque est évalué comme suit

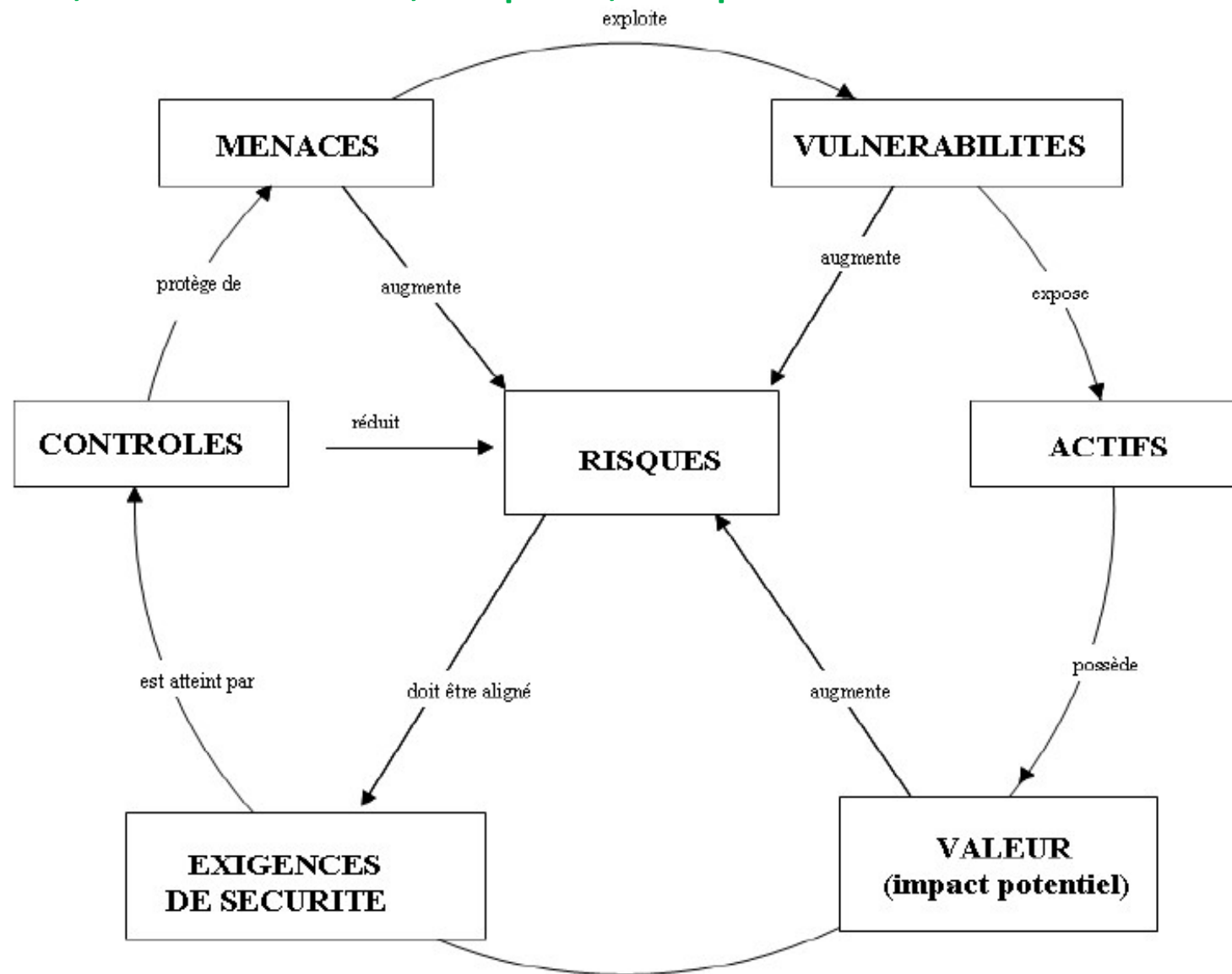
Risque = Probabilité d'occurrence (Menace x Vulnérabilité) x Impact



- Probabilité d'occurrence: Potentialité d'exploitation d'une vulnérabilité par une menace tout en prenant en compte les niveaux de couverture existants.

Analyse des risques

Menace, vulnérabilité, impact, risque



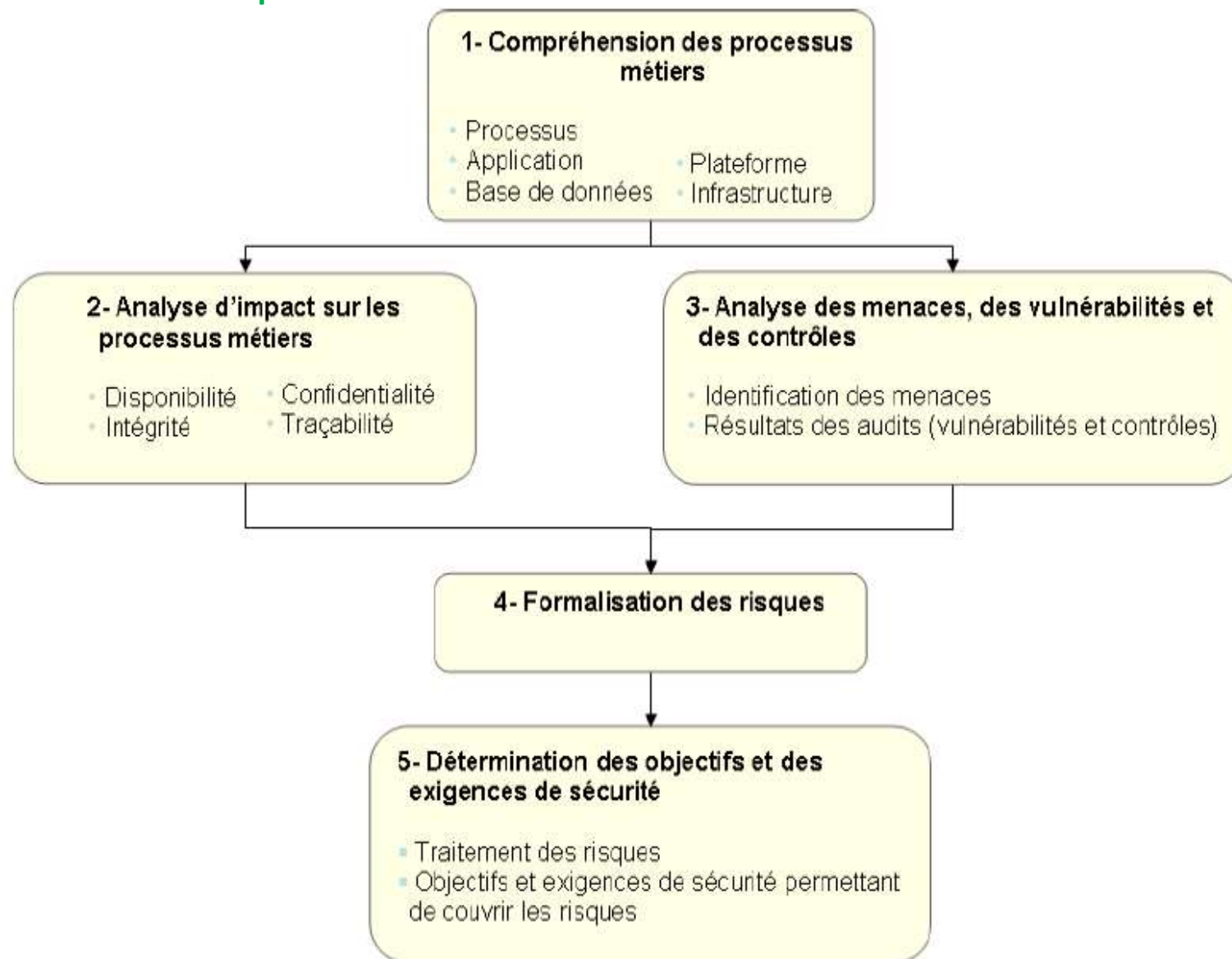
Analyse des risques

Traitement du risque

- **Objectif:** Réduire les risques à un niveau acceptable en fonction de leur impact.
- Le niveau de **risque résiduel** doit être inférieur aux critères prédéfinis d'acceptation de risques
- Les critères d'acceptation des risques sont basés sur l'analyse des coûts du traitement du risque face aux coût de reconstruction
- Le plan de traitement des risques consiste à la **mise en place de contre-mesures de sécurité**:
 - Contrôle sur la menace ou la vulnérabilité afin de limiter la cause du risque
 - Contrôles sur l'impact, afin de limiter la conséquence du risque.
- Il existe de nombreuses **contraintes** à prendre en compte dans le cadre de la mise en place des mesures de sécurité (financières, techniques, opérationnelles, légales, humaines)

Analyse des risques

Traitement du risque



Réponse au risques

Termes

TERME	DEFINITION
Appétit pour le risque	Le niveau de risque que le comité de direction est prêt à prendre pour l'entreprise dans le cadre du déroulement de sa mission.
Tolérance au risque	Le niveau acceptable de variation qu'une entreprise est prête à accepter pour tout risque particulier
Capacité à assumer le risque	Le niveau maximal de perte qu'une entreprise peut tolérer sans risquer de porter atteinte à son existence. Ainsi il diffère de l'appétit du risque qui se trouve être le niveau de risque souhaité par la Direction Général et le Comité de Direction.
Réponse au risque	Consiste à mettre en relief les risques inhérents dans l'entreprise, précise leurs effets et propose des réactions convenues face à chaque risque.
Risque résiduel	Risque actuel après choix et implémentation de la réponse au risque.

Réponse au risques

Objectif

- L'objectif de la mise en place d'une réponse au risque est de permettre un **alignement du risque avec l'appétit pour le risque** défini dans l'entreprise. En d'autres termes, une réponse doit être choisie de sorte que **le risque résiduel soit en deçà de la limite de tolérance**;
- L'évaluation de la réponse au risque n'est pas un effort unique. Il doit faire parti du processus de gestion du risque;
- Lorsque l'analyse de tous les scenari de risque identifiés ont montré un non alignement avec l'appétit du risque défini et le niveau de tolérance, une réponse est requise. Cette réponse peut être:
 - L'évitement
 - L'acceptation
 - Le partage
 - L'atténuation

Réponse au risques

Evitement du risque (1)

- L'évitement consiste à ne mener aucune activité susceptible d'engendrer un risque.
- L'évitement du risque s'applique lorsque les autres réponses au risque sont inadéquates. C'est le cas quand:
 - Il n'y a aucune réponse effective en terme de coût pouvant aider à réduire l'impact et la fréquence en deçà de la limite défini d'appétence au risque,
 - Le risque ne peut pas être partagé ou transféré,
 - Le niveau d'exposition est considéré comme inacceptable par la haute direction.

Réponse au risques

Evitement du risque (2)

- Quelques exemples d'évitement de risques liés aux Technologies de l'Information:
 - Délocaliser un centre de ressource dans une région avec moins de risques naturels,
 - Décliner la participation à un projet de grande envergure dont l'analyse de rentabilisation montre un risque notable d'échec,
 - Décide de ne pas utiliser une technologie particulière car non extensible.

Réponse au risques

Acceptation du risque (1)

- L'acceptation signifie que l'exposition à la perte est connue mais qu'aucune action n'est prise pour contrer un risque particulier.
- Ceci est différent de l'ignorance du risque.
- L'acceptation du risque signifie que le risque est connu c'ad que la haute direction a elle-même et pour des raisons valables, pris la décision de l'accepter ainsi.

Réponse au risques

Acceptation du risque (2)

- Quelques exemples d'acceptation de risques liés aux Technologies de l'Information:
 - Il peut y avoir risque qu'un projet ne fournisse pas les fonctionnalités métiers désirées, d'ici la date prévue de mise en production. La haute direction peut décider d'accepter le risque et poursuivre le projet.
 - Si un risque particulier est évalué comme étant extrêmement rare, avec un impact très important (voir catastrophique) et des approches de réduction très prohibitifs, la haute direction peut décider de l'accepter.

Réponse au risques

Partage/Transfert du risque (1)

- Le partage consiste à réduire la fréquence ou l'impact de risque en transférant ou en partageant une partie du risque.
- Parmi les techniques les plus usitées nous avons l'assurance et la sous-traitance. Ces techniques ne soulagent pas l'entreprise de la responsabilité du risque, mais elle font appel aux compétences d'une autre entité dans la gestion du risque et la réduction des conséquences financière si un événement négatif arrivait à se produire.

Réponse au risques

Partage/Transfert du risque (2)

- Quelques exemples de partage/transfert de risques liés aux Technologies de l'Information:
 - Une grande entreprise ayant identifié et évalué le risque d'incendie pour son infrastructure répartie dans plusieurs endroits du pays, envisage la souscription à une assurance afin de partager l'impact du risque. Elle a conclu que compte tenu de la localisation de ces sites, le cout incrémental d'une assurance n'était pas prohibitif. La souscription a finalement été faite.
 - Dans le cadre d'un projet d'envergure dans le domaine des TI, les risques du projet peuvent être partagé en sous-traitant le développement de l'application métier moyennant un cout fixe.
 - Certaines entreprises sous-traitent quelques un ou la totalité de leurs fonctions informatiques à des prestataires et partagent ainsi le risque.
 - Lorsque l'hébergement des applications est sous-traité, l'entreprise reste responsable de la protection des données clients, mais si le prestataire est négligeant et qu'une faille est exploitée, le risque (impact financier) peut être partagé avec le client.

Réponse au risques

Mitigation du risque

La mitigation désigne l'ensemble des mesures et moyens d'atténuation pour réduire la fréquence et / ou l'impact d'un risque.

Parmi les moyens de mitigation des risques nous pouvons citer:

- Le renforcement les pratiques de gestion du risque informatique global, à savoir, la mise en œuvre des processus de gestion des risques informatiques suffisamment matures tels que définis par les référentiels,
- L'introduction d'un certain nombre de mesures de contrôle visant soit à réduire la fréquence d'un événement indésirable ou l'impact commercial/financier d'un événement. Les contrôles permettent , dans le contexte de la gestion des risques, d'atténuer le risque.
- L'atténuation des risques est possible par d'autres moyens ou méthodes, par exemple, il existe des cadres de gestion informatique de renom et des normes capables d'aider.

Type de risques

- **Les accidents :**
 - Pannes matérielles ou logicielles,
 - Bris de machine accidentel (choc, chute, etc.),
 - Sinistre local : explosion, incendie, dégât des eaux,
 - Événements naturels : tempête, inondation, etc,
 - Perte de services essentiels : électricité, télécommunication, eau, etc.
- **Les erreurs :**
 - Erreurs d'utilisation,
 - Erreurs de conception des logiciels et des procédures d'application.
- **La malveillance :**
 - Vol de matériel,
 - Sabotage matériel,
 - Fraude (détournement de fonds, de biens ou de services),
 - Attaque logique,
 - Divulgence d'informations confidentielles,
 - Infraction aux lois (contrefaçon).

Type de contrôles

PREVENTIF	DETECTIF	CORRECTIF
Personnel qualifié	Message d'erreur	Procédure d'urgence
Séparation des tâches	Fonction d'audit interne	Procédure de sauvegarde
Contrôle d'accès		Procédure de reprise
Documents bien conçus		Maintenance
Logiciel de chiffrement		

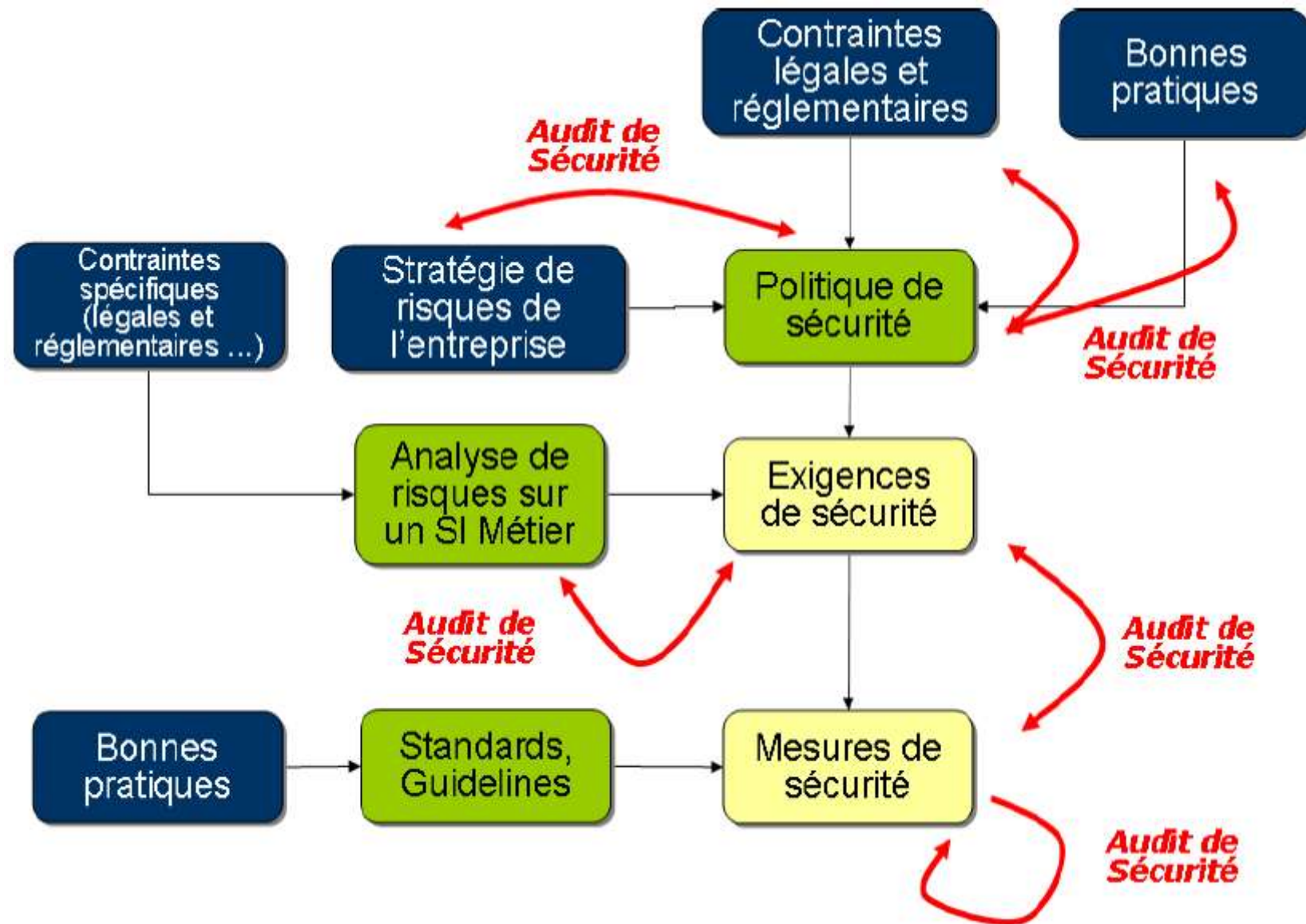


Démarche de l'audit de sécurité

L'audit de sécurité du SI

- **Définition:** *L'audit de sécurité du système d'information est un examen méthodique d'une situation liée à la sécurité de l'information en vue de vérifier sa conformité à des objectifs, à des règles ou à des normes.*
- Compte tenu du cadre de gestion de la sécurité de l'information, les audits de sécurité peuvent adresser des problématiques différentes comme par exemple :
 - Audit de la politique de sécurité,
 - ✓ Adéquation de la politique de sécurité à la stratégie de risques de l'entreprise, aux contraintes légales et réglementaires et aux bonnes pratiques,
 - Audit de la mise en œuvre de politique de sécurité,
 - ✓ Respect des exigences de sécurité au sein de l'entreprise au travers de la mise en œuvre de mesures de sécurité adéquates et pérennes,
 - Audit de l'efficacité des mesures de sécurité.
 - ✓ Test d'intrusion.

Types d'audit de sécurité



Exemples de risques à prendre en compte lors d'un audit

- Risques sur le patrimoine de l'entreprise
 - Vol d'actifs de l'entreprise,
 - Divulgence d'informations confidentielles,
 - Détournement de services,
 - Sabotage.
- Risque sur l'activité
 - Indisponibilité du poste de travail,
 - Indisponibilité du réseau ou du serveur.
- Risque sur l'intégrité du système d'information
 - Attaque virale,
 - Incohérence des données entre serveurs et stations,
 - Développements mal maîtrisés ou mal documentés,
 - Ouverture de failles dans la sécurité (connexions incontrôlée à Internet).
- Risque juridique
 - Infraction à la loi,
 - Copie illicite de logiciels,
 - Fraude informatique avec le matériel de l'entreprise.

Démarche d'audit de sécurité

1.Prise de connaissance

- Cartographier le système,
- Recenser les standards et règles.

2.Analyse des risques

- Évaluer les enjeux de la sécurité du système,
- Identifier des scénarios de menace et en évaluer l'impact sur l'entreprise.

3.Évaluation de la sécurité du système

- Vérifier que les contrôles mis en œuvre garantissent une couverture suffisante des risques.
- Des référentiels existent : ISO 27002, Cobit5 for Information Security, etc.

4.Élaboration de recommandations

- Pour chaque vulnérabilité identifiée et correspondant à un risque, proposer une recommandation corrective,
- Préparer les recommandations avec les personnels opérationnels de l'entreprise !

Démarche de l'audit de sécurité

1. Prise de connaissance

- **Collecter l'information**

- Documents de l'entreprise,
- Entretiens,
- Visite des locaux.

Informations à collecter:

- **Organisation :**

- politique de sécurité,
- normes et standards en vigueur,
- personnes et équipes impliquées dans l'exploitation du réseau et du parc micro (administration, maintenance, sécurité, support utilisateur),
- définition des responsabilités,
- procédures appliquées ou prévues (mode dégradé),
- plans (de sauvegarde, d'archivage, de secours, de reprise, etc.),
- interlocuteurs pour l'audit (informatique et utilisateurs).

- **Volumétrie :**

- nombre d'utilisateurs,
- volumes de données transmises,
- taille des données sauvegardées.

- **Matériels :**

- serveurs,
- stations de travail,
- équipements réseau (switch, routeurs),
- firewalls.

- **Logiciels :**

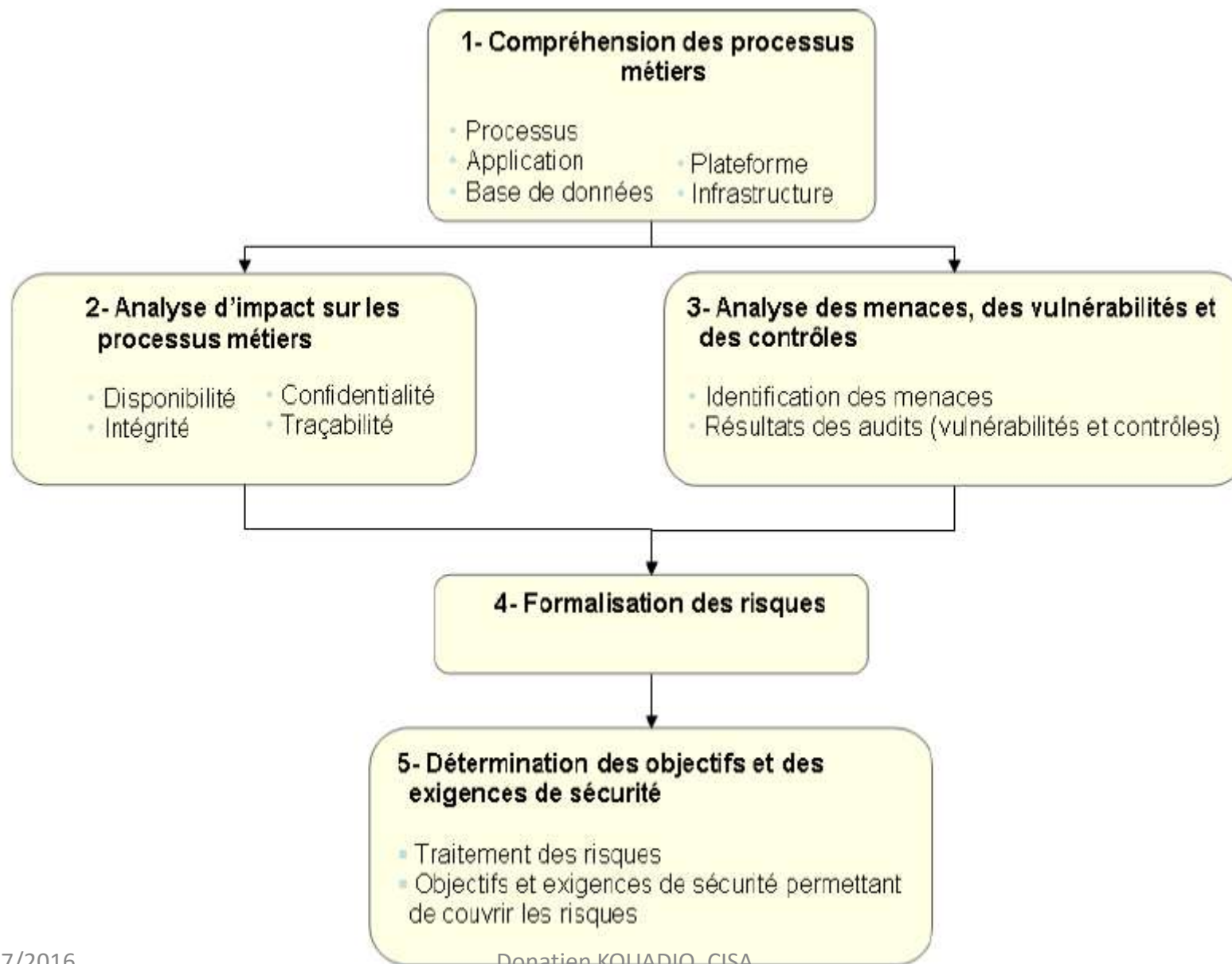
- systèmes d'exploitation,
- middleware,
- principales applications utilisées.

- **Communications :**

- architecture du réseau (topologie),
- plan de câblage,
- connexions avec l'extérieur.

Démarche de l'audit de sécurité

2. Analyse du risques



Etape 1 : Compréhension des processus métiers

- Les objectifs de cette étape sont de :
 - mettre en évidence l'ensemble des processus métiers et leurs interactions,
 - identifier les données intervenant à l'intérieur de ces processus,
 - identifier les composants (application, base de données, serveurs et infrastructure) nécessaires au déroulement des processus métiers.
- Description des processus et de leurs composants (applications, bases de données, serveurs, infrastructure).

Démarche de l'audit de sécurité

2. Analyse de risques

Etape 2 : Analyse d'impact sur les processus métiers

Niveau d'impact	Perte financière	Dégradation de la performance		Gestion		Obligation et Responsabilité			Métier	Juridique
Niveau d'impact	Impact financier maximum	Non respect des objectifs	Perte en jour/homme	Type d'événement	Tableau de bord enroulé ou non produit	Publicité négative	Mesures Réglementaires	Erosion de la base client	Délai de mise en œuvre de nouveau produit	Engagement juridique
5	>100m	10%+	1000+	Désastre	Plus d'un mois de délai, toute information incohérente	Image publique ruinée	Sanction grave	10%+ des ventes	Arrêt des projets stratégiques	Procès de plus d'un an
4	10m-100m	5% - 10%	500 - 1000	Crise	De 1 à 4 semaines de délai, de nombreuses erreurs	De nombreux articles dans la presse nationale et internationale	Sanction mineure	5% - 10% des ventes	Délai de plusieurs mois des projets stratégiques	Procès de plus de 6 mois
3	1m-10m	1% - 5%	100 - 500	Incident majeur	Délai de plusieurs jours, quelques informations erronées	De nombreux articles dans la presse	Infraction à la réglementation	1% - 5% des ventes	Délai de plusieurs semaines des projets stratégiques	Procès de plus d'1 mois
2	100K-1m	<1%	10 - 100	Interruption	Délai de plusieurs heures, quelques informations erronées	Quelques articles dans la presse	Pas d'impact réglementaire	<1% des ventes	Délai de plusieurs jours des projets stratégiques	Procès court / Amendes
1	50K-100K	0%	0 - 10	Inconvenient	Léger délai, pas d'erreur	Impact sur quelques clients	Pas d'impact réglementaire	0% des ventes	Embaras vis-à-vis du public	Demande de justification des clients
0	<50K	0%	0 - 10	Inconvenient	Léger délai, pas d'erreur	Pas d'impact	Pas d'impact réglementaire	0% des ventes	Pas d'impact	Pas d'impact

Etape 3 : Menaces, Vulnérabilités et Contrôles

- A l'issue de l'analyse de l'impact sur les processus métiers, une analyse des menaces, des vulnérabilités et des contrôles sera réalisée.
- En fonction des processus, données et composants du système d'information, une sélection des menaces pertinentes sera réalisée. Ces menaces sont caractérisées par leur type (naturel, humain, ou environnemental) et les causes possibles (accidentelle, intentionnelle).
- Analyse des vulnérabilités et des contrôles.

Démarche de l'audit de sécurité

2. Analyse de risques

Etape 3 : Menaces, Vulnérabilités et Contrôles

		Éléments menaçants						Critères de sécurité touchés		
		Type			Cause		Potentiel d'attaque	Disponibilité	Intégrité	Confidentialité
		Naturel	Humain	Environnemental	Accidentelle	Délibérée				
Méthodes d'attaque										
1	Incendie	+	+	+	+	+	2	+	+	
13	Perte des moyens de télécommunications			+	+	+	1	+		
19	Écoute passive		+	+		+	2			+
20	Vol de supports ou de documents			+		+	2			+
21	Vol de matériels			+		+	1	+		+
23	Divulgarion		+	+	+	+	1			+
26	Piégeage du logiciel			+		+	1	+	+	+
42	Atteinte à la disponibilité du personnel	+	+	+	+	+	1	+		

Démarche de l'audit de sécurité

2. Analyse de risques

Etape 3 : Menaces, Vulnérabilités et Contrôles

Une évaluation de la probabilité d'occurrence de la menace sera établie en fonction de l'existence de vulnérabilité et la présence de contrôle.

Menace	Potentialité
5	Très fréquent (devrait arriver de nombreuses fois durant le cycle de vie du système)
4	Fréquent (devrait arriver plusieurs fois durant le cycle de vie du système)
3	Probable (devrait normalement arriver durant le cycle de vie du système)
2	Peu probable (ne devrait normalement pas arriver durant le cycle de vie du système)
1	Très peu probable (ne devrait jamais arriver durant le cycle de vie du système)

Démarche de l'audit de sécurité

2. Analyse de risques

Etape 4 : Formalisation des risques

L'appréciation du risque encouru résulte de la probabilité de réalisation de la menace et du niveau de conséquences dommageables pour un ou l'ensemble des processus.

Conséquence dommageable pour l'institution ou une de ses activités	Probabilité de réalisation de la menace				
	Très peu probable (ne devrait jamais arriver durant le cycle de vie du système)	Peu probable (ne devrait normalement pas arriver durant le cycle de vie du système)	Probable (devrait normalement arriver durant le cycle de vie du système)	Fréquent (devrait arriver plusieurs fois durant le cycle de vie du système)	Très fréquent (devrait arriver de nombreuses fois durant le cycle de vie du système)
Désastre	2	3	3		
Crise	2	3	3	3	3
Incident	1	2	2	2	2
Interruption	1	2	2	2	2
Inconvénient	1	1	1	1	1

Démarche de l'audit de sécurité

2. Analyse de risques

Etape 5 : Objectifs et exigences de sécurité

- Dans un premier temps et en fonction de la stratégie de risques, une décision sera prise, pour chaque risque, quant à la gestion de ce risque:
 - le risque est négligeable,
 - le risque est acceptable,
 - le risque est inacceptable.
- Sur la base de ces résultats, des objectifs et des exigences de sécurité seront définis afin de réduire ou de supprimer les risques inacceptables.

Démarche de l'audit de sécurité

2. Analyse de risques

Etape 5 : Objectifs et exigences de sécurité

Les objectifs et les exigences de sécurité pourront être sélectionnés à partir du guide «**Outils pour le traitement des risques SSI**» de la méthode Ebios. Ce guide présente en particulier des exigences de sécurité issues des normes ISO 15408 et ISO 27002.

Politique de Sécurité			
Organisation de la Sécurité			
Classification et contrôle des actifs			
Sécurité du Personnel	Sécurité Physique et Sécurité de l'Environnement	Gestion des Communications et des Opérations	Développement et Maintenance des Systèmes
Contrôle des Accès			
Gestion de la Continuité des Activités de l'Entreprise			
Conformité			

3.2.7 BMA : Contrôle des accès (Chapitre 9)

3.2.7.1 BMA_EMA : Exigences de l'entreprise concernant le contrôle des accès (§9.1)

Code	Libellé
BMA_EMA.1.1	Les exigences professionnelles de maîtrise d'accès doivent être définies et documentées et l'accès doit être limité à ce qui est défini dans la politique de maîtrise des accès

3.2.7.2 BMA_GAU : Gestion des accès utilisateurs (§9.2)

Code	Libellé
BMA_GAU.1.1	Il doit y avoir une procédure officielle d'enregistrement et de désenregistrement des utilisateurs pour l'octroi de l'accès à tous les systèmes et les services informatiques multi-utilisateurs
BMA_GAU.2.1	L'attribution et l'utilisation de privilèges doivent être restreintes et maîtrisées
BMA_GAU.3.1	L'attribution des mots de passe doit être maîtrisée par un processus de gestion officiel
BMA_GAU.4.1	Un processus officiel de revue des droits d'accès des utilisateurs doit être exécuté à des intervalles réguliers

3.2.7.3 BMA_REU : Responsabilités des utilisateurs (§9.3)

Code	Libellé
BMA_REU.1.1	Les utilisateurs doivent suivre de bonnes pratiques sécurité lors de la sélection et de l'utilisation des mots de passe
BMA_REU.2.1	Les utilisateurs doivent veiller à ce que le matériel sans surveillance ait une

Démarche de l'audit de sécurité

3. Evaluation de la sécurité d'un système

- **Objectif** : s'assurer que les contrôles mis en œuvre au sein ou autour du système audité sont en mesure de garantir une couverture suffisante des risques pesant sur le système.
- Principaux points à contrôler :
 - Sécurité physique
 - Sécurité d'exploitation
 - Contrôle des accès et des habilitations (sécurité logique)
 - Audit et contrôle
 - Prise en compte de la sécurité dans les projets
 - Respect des lois

Démarche de l'audit de sécurité

4. Elaboration de recommandations

- **Objectif** : préparer les éléments du plan d'action sécurité.
- Pour chaque vulnérabilité identifiée et correspondant à un risque, proposer une action corrective.
- Hiérarchiser les recommandations en fonction de l'importance du risque (application des résultats de l'analyse de risque).
- Valider les recommandations avec les personnels opérationnels de l'entreprise

Menace/Vulnérabilité/identifiant du risque	Priorité	Type de traitement du risque	Recommandations	Responsable	Date de réalisation prévue

Contexte législatif

Contexte législatif

Les textes de base

La CEDEAO et la CDP procèdent progressivement à l'adoption d'une réglementation des TICs, via des déclarations de politique générale et régulations de la protection des données personnelles.

- **Propriété intellectuelle**
 - LOI n° 2008-12 du 25 janvier 2008 portant sur la Protection des données à caractère personnel
- **Signature électronique**
 - Acte additionnel A/SA.2/01/10 du 16 février 2010 sur les transactions électroniques
 - Règlement n°15/2002/CM/UEMOA du 23 mai 2002 relatif aux systèmes de paiement dans les états membres de l'Union Economique et Monétaire Ouest Africaine (UEOMA)
- **Cybercriminalité**
 - Directive C/DIR/1/08111 portant lutte contre la cybercriminalité dans l'espace de la CEDEAO
- **Cryptologie**
 - LOI n° 2008-41 du 20 août 2008 portant sur la Cryptologie

Propriété intellectuelle

- *Le traitement des données à caractère personnel est considéré comme légitime si la personne concernée donne son consentement. **Article 33***
- *Les données à caractère personnel doivent être traitées de manière confidentielle et être protégées conformément aux dispositions de l'article 71 de la présente loi, notamment lorsque le traitement comporte des transmissions de données dans un réseau. **Article 38***
- *Il est interdit de procéder à la collecte et à tout traitement qui révèlent l'origine raciale, ethnique ou régionale, la filiation, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, la vie sexuelle, les données génétiques ou plus généralement celles relatives à l'état de santé de la personne concernée. **Article 40***
- *Le responsable d'un traitement ne peut transférer des données à caractère personnel vers un pays tiers que si cet Etat assure un niveau de protection suffisant de la vie privée, des libertés et droits fondamentaux des personnes à l'égard du traitement dont ces données font ou peuvent faire l'objet. **Article 49***

Signature électronique

- *Une signature électronique créée par un dispositif de sécurité que le signataire peut garder sous son contrôle exclusif et qui repose sur un certificat numérique est admise comme signature au même titre que la signature manuscrite. **Article 35***
- Enjeux pour la sécurité :
 - protection signature contre falsification,
 - mentions du certificat : nom du signataire, date de début et de fin de la validité du certificat, limites d'utilisation du certificat.

Cybercriminalité

- *Constitue une infraction, au sens de la présente Directive, le fait de commettre un vol, une, escroquerie, un recel, un abus de confiance, une extorsion de fonds, un acte de terrorisme, ou une contrefaçon portant les données informatiques, les logiciels et les programmes. **Article 25***
- *L'écrit électronique est admis comme preuve en matière d'infraction à condition que puisse être dûment identifiée la personne dont il émane et qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité. **Article 32***
- *En cas de condamnation, la juridiction compétente peut prononcer la confiscation des matériels, des équipements, des instruments, des programmes informatiques ou des données ainsi que des sommes ou produits résultant de l'infraction et appartenant au condamné. **Article 29***

Cryptologie

- *Les prestataires de services de cryptologie à des fins de confidentialité sont responsables du préjudice causé dans le cadre desdites prestations aux personnes leur confiant la gestion de leurs conventions secrètes, en cas d'atteinte à l'intégrité, à la confidentialité ou à la disponibilité des données transformées à l'aide de ces conventions. **Article 18***
- *Les personnes assurant des prestations de cryptologie ou exerçant des activités de cryptologie disposent d'un délai de six (6) mois à compter de la date d'entrée en vigueur de la présente loi, pour régulariser leur situation auprès de la Commission nationale de cryptologie. **Article 21***
- *Quiconque aura fourni des prestations de cryptologie sans avoir obtenu préalablement l'agrément de la Commission nationale de cryptologie prévu à l'article 16 de la loi sur la cryptologie, sera puni d'un emprisonnement d'un an à cinq ans et d'une amende de 1.000.000 francs à 20.000.000 francs ou de l'une de ces deux peines seulement. **Article 2***

Nul n'est censé ignorer la loi

Certifications

Certifications



QCM DE REVISION