Université de la Manouba
Institut Supérieur de Comptabilité et d'Administration des Entreprises

Audit des SI

Présenté par:
M.BILEL ERRAHMOUNI

© 2019

Contexte Général

- ✓ **Le SI revêt une importance capitale pour la pérennité de l'entreprise,**
- ✓ **L'accès à l'information dans le cadre des relations entreprises partenaires augmente les menaces et les vulnérabilités du SI,**
- ✓ **Les entreprises se trouvent désormais confrontées au contrôle efficace de la confidentialité, de l'intégrité et de la disponibilité de leurs informations,**
- ✓ **Face à ces menaces, l'expert comptable est confronté aux nouveaux risques liés à la SSI.**

Menaces et Vulnérabilités du SI

Menaces

Intégrité :

- Piégeage des systèmes (bombes logiques, cheval de Troie, ver, …)
- Modification des informations (modification de page Web,…)
- Intrusion en vue « d'attaque par rebond », sabotage matériel

Confidentialité :

- Accès non autorisée à des informations sensibles
- Usurpation d'identité, intrusion et écoute, des copies illicites,

Disponibilité :

- Vols d'équipements, actes de vengeance, destruction
- Virus et vers informatiques
- Accidents: incendies, inondations, pannes d'équipements, catastrophes naturelles. . .

Attaques :

- ✓ Déni de service (Deny of Service, DoS)
- ✓ Attaques sur les mots de passe
- ✓ Programmes malveillants
- ✓ Attaques par messagerie
- ✓ Attaques sur le réseau

Menaces et Vulnérabilités du SI (suite)

Vulnérabilités

Logiciels et matériels :

- ✓ Mauvaise conception
- ✓ Défaillances de l'alimentation électrique, de la climatisation ,
- ✓ Modification ou substitution des composants du système,…

Personnels :

- ✓ Manque de conscience professionnelle ou de formation, chantage
- ✓ Divulgation d'informations sensibles,
- ✓ Perturbations en cas de mouvements sociaux, …

Structurels :

- ✓ Absence d'une politique de SSI
- ✓ Procédures inefficaces ou inapplicables,
- ✓ Pertes de compétences ou de savoir-faire,…

Impacts internes :

- ✓ Les pertes de fonds,
- ✓ Les pertes de valeurs,
- ✓ Arrêts de l'activité provisoire ou définitive
- ✓ Le cas échéant, les pertes humaines,…

Impacts externes :

- ✓ La perte d'image de marque due à la notoriété du sinistre,
- ✓ La perte de confiance des partenaires,
- ✓ La perte de parts de marchés,
- ✓ La perte de compétitivité,…

Impacts financiers :

Pertes financières: coût de restauration ou remplacement des dégâts, diminution du CA, …

L'Expert Comptable face à la SSI

L'expert comptable peut assurer l'audit de la SSI dans le cadre d'un mission de CAC ou d'une mission de consulting.

Mission du CAC:

Selon ISA 315 § 2, le CAC doit acquérir une connaissance du contrôle interne de l'entité pour lui permettre d'évaluer le risque d'anomalie significative. Le SI est un composant du CI.

[illegible] contrôle interne dans l'entité

Environnement de Contrôle

Evaluation des Risques

S.I et communication

Invite le CAC à auditer la SSI

Surveillance

Activités de Contrôle

Composants du système de contrôle interne

L'Expert Comptable face à la SSI

Mission du CAC:

D'autre part, l'expert comptable est appelé à auditer la SSI eu regard au:

- ✓ **Information des dirigeants ou de l'organe de direction (Lettre à la direction § 6, 43, 63, 81 à 89 de ISA 315 et § 11- ISA 500),**
- ✓ **Rapport du CAC : opinion sur les états financiers (inexactitudes ou irrégularités relevées),**
- ✓ **Déclenchement de la procédure d'alerte (absence de plan de continuité, etc.),**
- ✓ **Révélation des faits délictueux (fraudes informatiques, etc…),**
- ✓ **Loi n° 2005-96 du 18 octobre 2005 relative au renforcement de la sécurité des relations financières (art 266 CSC opinion sur le CI),**
- ✓ **BALE II pour le secteur bancaire,**

L'Expert Comptable face à la SSI(suite 2)

Mission de consulting:

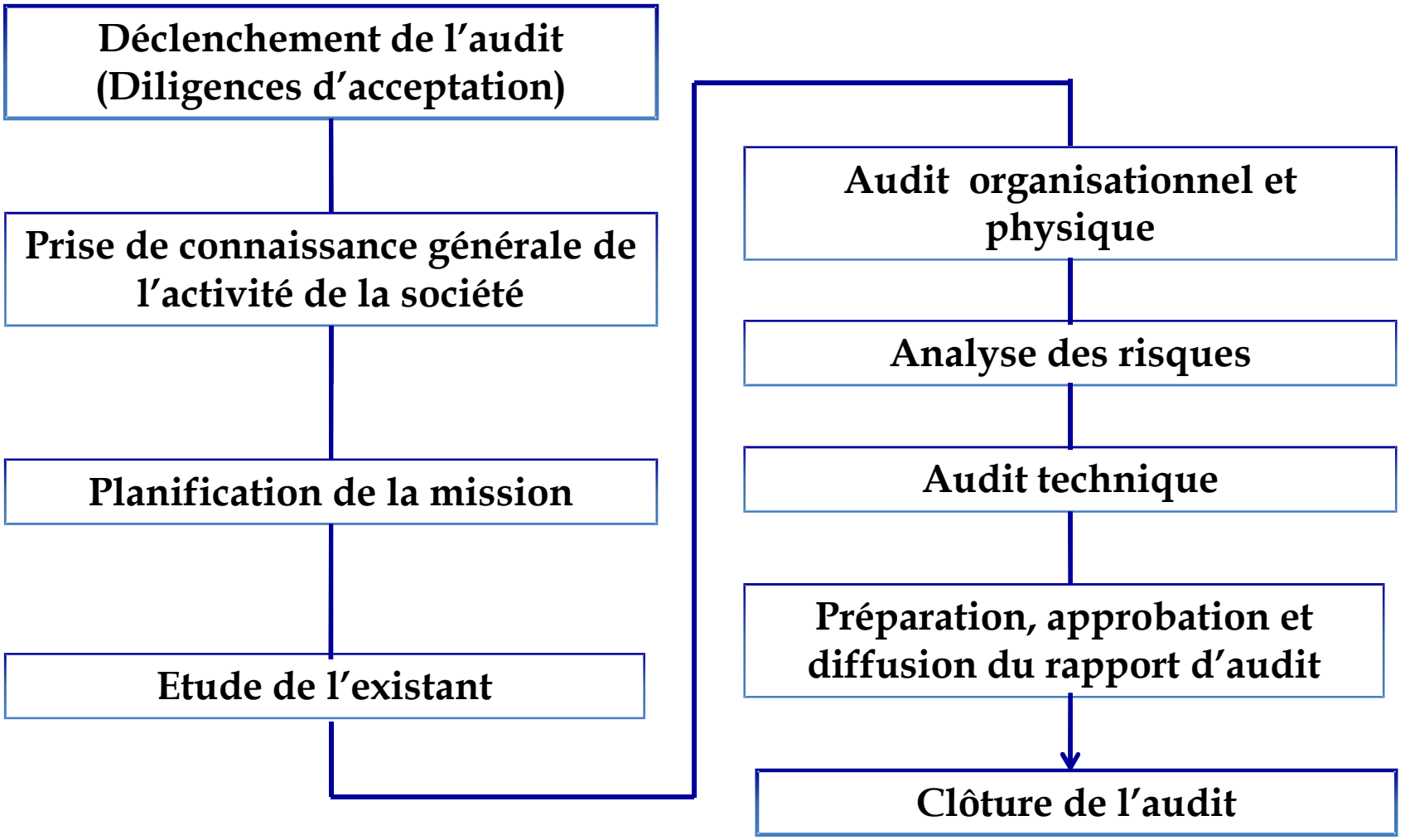
L'expert comptable, principal conseiller de la société, est en mesure d'assurer les nouvelles missions suivantes:

- ✓ **Audit de la SSI,**
- ✓ **Evaluer l'impact des menaces sur la Confidentialité, la Disponibilité et l'Intégrité,**
- ✓ **Evaluer le niveau de maturité de la SSI,**
- ✓ **Sensibiliser la direction aux menaces et aux vulnérabilités,**
- ✓ **Apporter des solutions et des conseils sur les moyens de protection,**
- ✓ **Elaboration et mise en place d'une politique de sécurité,**

Avantages liés à l'audit de la SSI

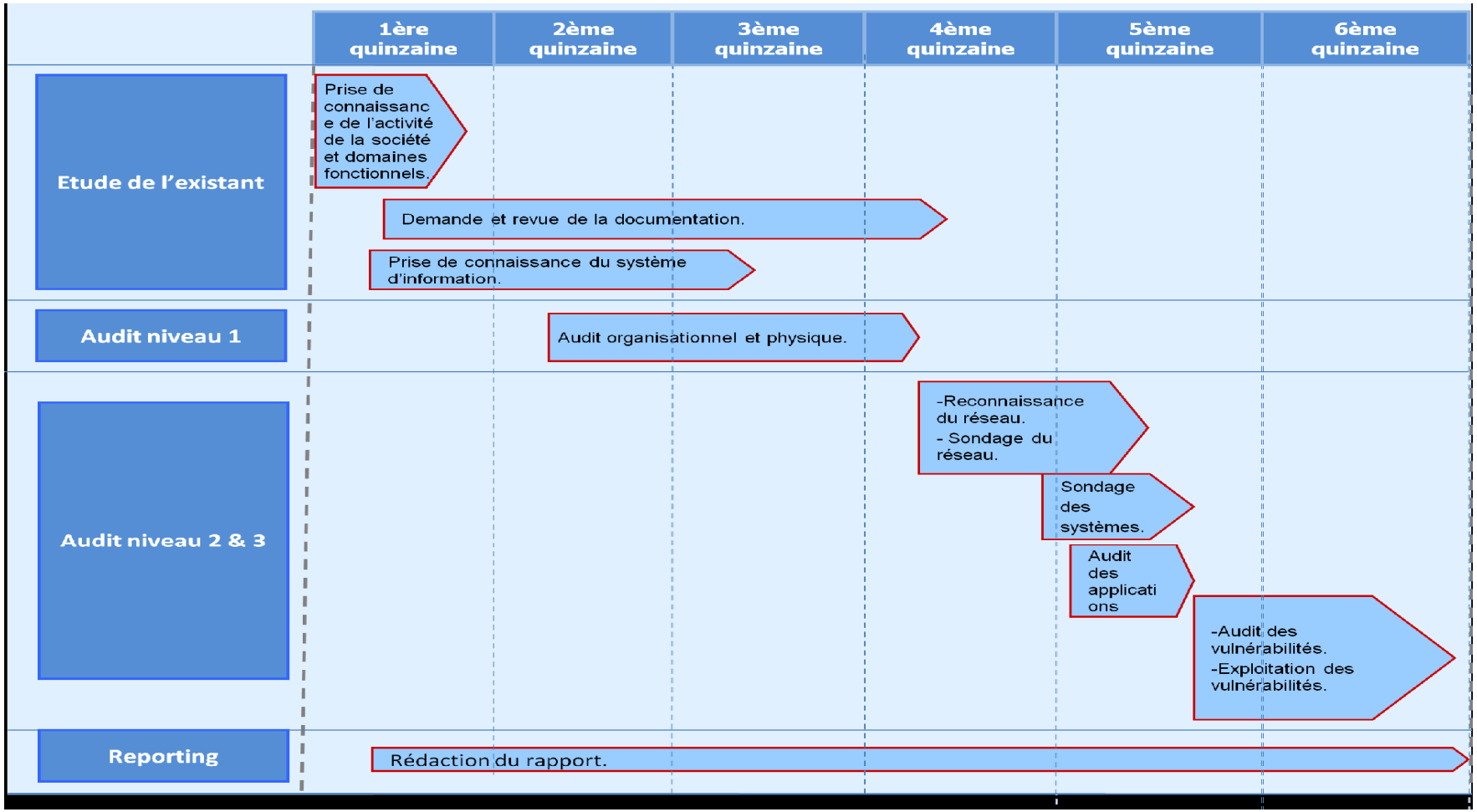
- ✓ **Maîtrise des menaces et des vulnérabilités du SI,**
- ✓ **Obtention de nouveaux éléments probants pour l'audit,**
- ✓ **Renforcement du rôle de l'expert comptable, principal conseiller de la société,**
- ✓ **Spécialisation dans un domaine complémentaire au métier de base de l'expert comptable.**

Démarche d'audit de la SSI

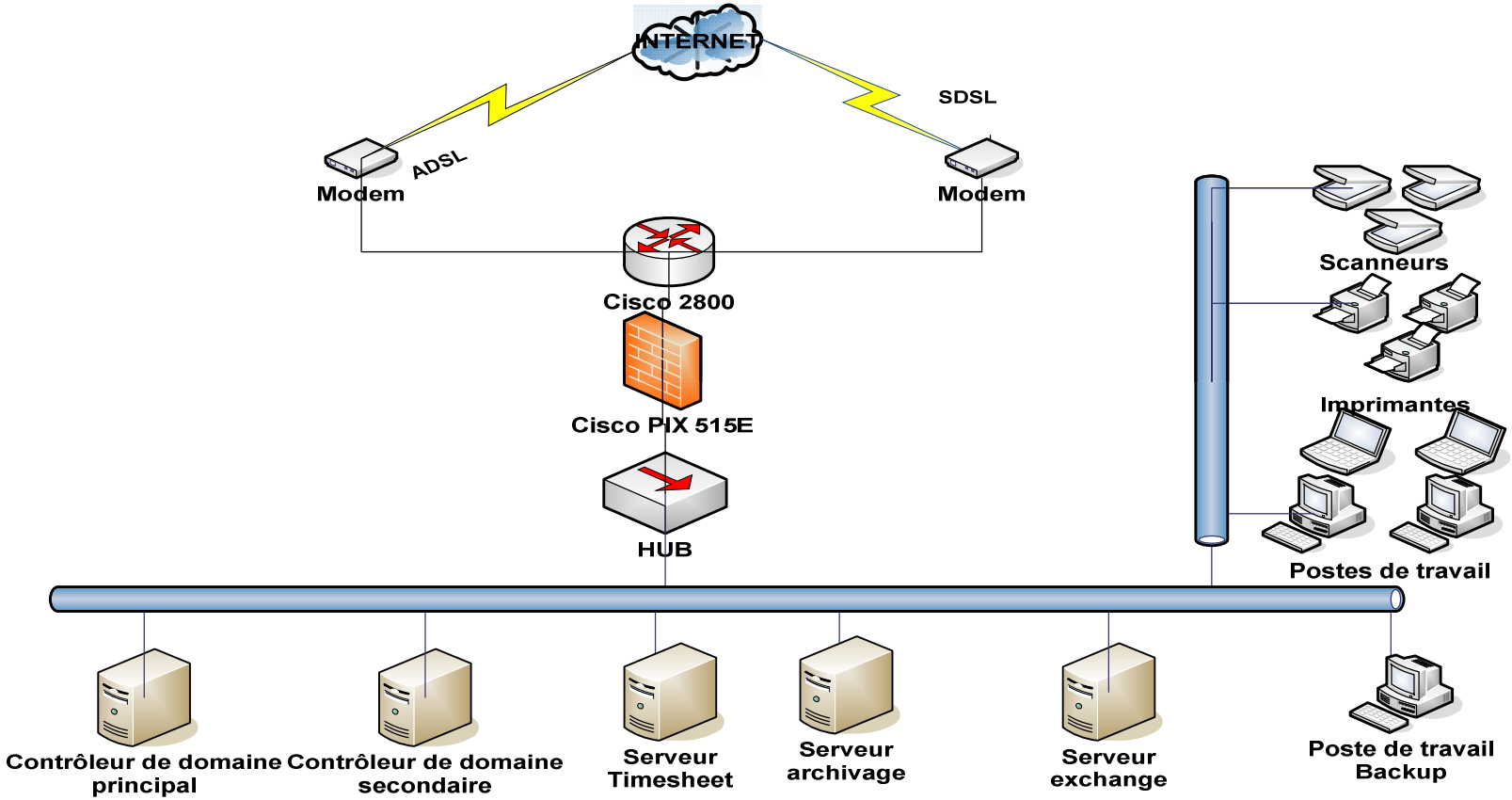


Démarche d'audit de la SSI
Planification de la mission

Le budget temps alloué à l'audit de la SSI dépend de la taille de la société et de la complexité de son SI, il est de 3 mois en moyenne pour les grandes entreprises. Il tiendra compte des aspects suivants :



Démarche d'audit de la SSI
Etude de l'existant



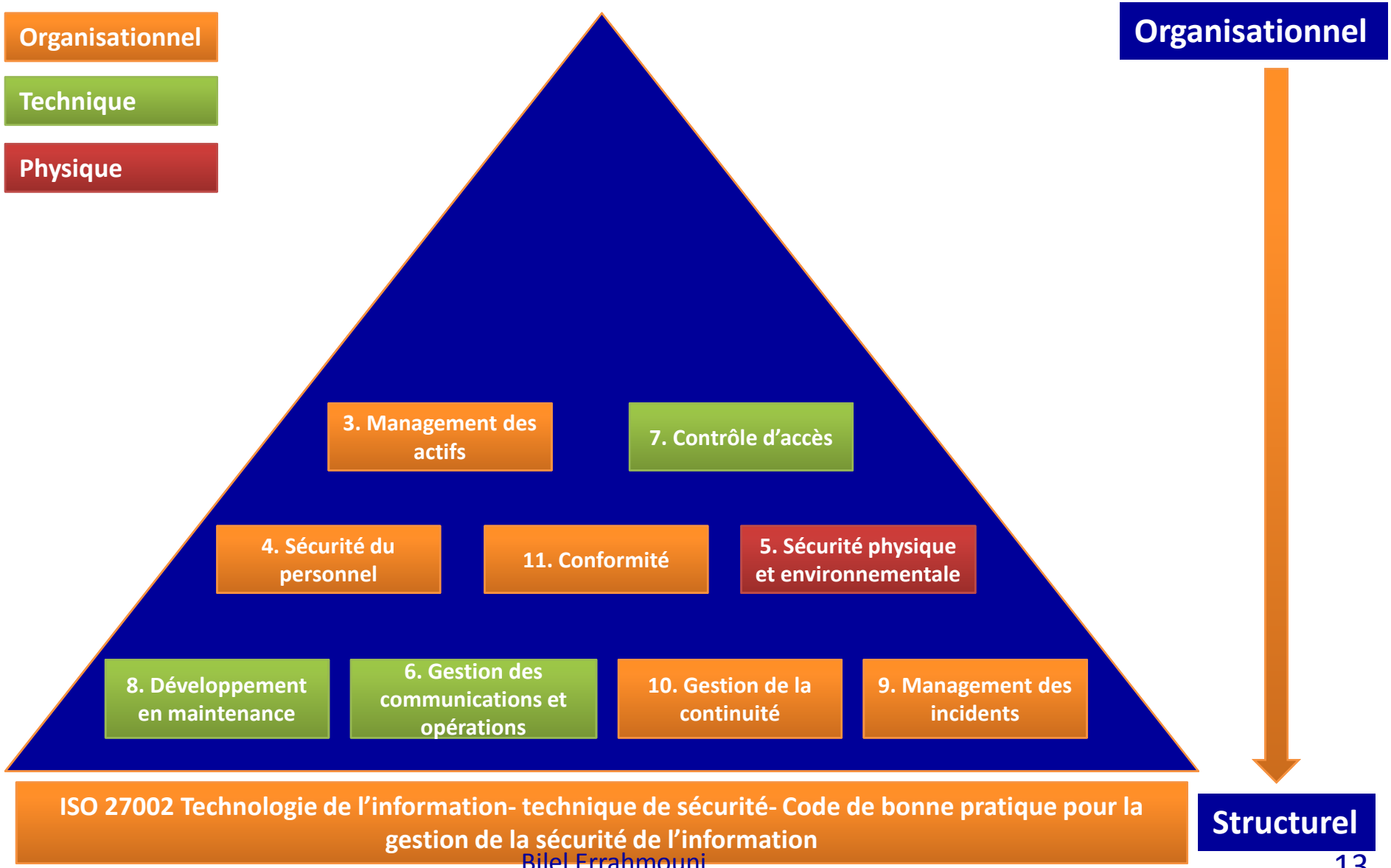
Architecture du réseau de la société

Démarche d'audit de la SSI
Audit organisationnel et physique

- ✓ Réalisation d'un questionnaire classé selon les 11 chapitres de l'ISO 27002 et comportant 39 objectifs et de 133 mesures de sécurité .

Niveau 1 → La mesure est ni implémentée ni planifiée
Niveau 2 → La mesure est planifiée
Niveau 3 → La mesure est partiellement mise en œuvre
Niveau 4 → La mesure est entièrement mise en œuvre

Démarche d'audit de la SSI
Référentiel : NORME ISO 27 002



Politique de sécurité

5.1 Politique de sécurité de l'information

Objectif: Élaborer un document appelé « document de la politique

de sécurité » qui traitera tous les aspects de sécurité.

5.1.1 Document de la politique de sécurité de l'information

✓Description brève de la politique de sécurité, principes, objectifs et exigences.

✓Définition des responsables de la mise en place du système et attribution des rôles.

✓Ce document doit être approuvé par la Direction et communiqué au personnel.

5.1.2 Examen et évaluation

Il doit être tout de même revu périodiquement pour faire face aux nouveaux risques.

Un processus de révision doit être défini pour maintenir la politique

Vérifier périodiquement : l'efficacité de la politique, coût englobant et changements technologiques

Démarche d'audit de la SSI
Audit organisationnel et physique

<u>Organisation de la sécurité:</u>

6.1 Organisation interne

Objectif: Bien gérer le système de sécurité de l'information à

l'intérieur de l'organisation.

Afin d'assurer une bonne gestion il convient de :

✓Établir un cadre organisationnel pour déclencher et contrôler la mise en place du système de sécurité d'information

✓Motiver et réunir la Direction afin d'approuver la politique et d'attribuer les rôles et les responsabilités

✓Designer les intervenants externes spécialistes en sécurité.

Démarche d'audit de la SSI
Audit organisationnel et physique

Organisation de la sécurité:

6.2 Intervenants Externes

Objectif: Assurer la sécurité des informations auxquelles les tierces personnes ont accès.

Pour cela il faut :

✓Identifier les risques entraînés par l'accès des tierces personnes et commencer par implémenter les contrôles nécessaires avant d'attribuer les droits d'accès.

✓Fixer les exigences en matière de sécurité lors de l'ouverture du système d'informations pour donner l'accès aux clients potentiels

✓Définir les niveaux de sécurité exigés par l'organisation dans les contrats signés par les tierces personnes.

Démarche d'audit de la SSI
Audit organisationnel et physique

Management des actifs:

7.1 Responsabilités liées aux actifs

Objectif: Protéger les actifs de l'entreprise.

Afin de réaliser cet objectif l'organisation doit :

✓Faire des inventaires: Identifier et valoriser ses avoirs afin de bien définir les niveaux de sécurité.

✓Désigner un responsable pour chaque ressource inventoriée

✓Etablir les règles de l'utilisation acceptable des informations et des actifs de l'organisation

7.2 Classification des informations

Objectif: Assurer que les avoirs en information disposent d'un

niveau approprié en sécurité.

Pour cela il faut :

✓Définir les lignes directrices de la classification des informations de manière à indiquer : le besoin, la priorité et le degré de protection de l'information.

✓Définir un système d'étiquetage et de traitement de l'information conformément à la classification adoptée.

Démarche d'audit de la SSI
Audit organisationnel et physique

Sécurité des ressources humaines:

8.1 Avant emploi

Objectif: Assurer que le personnel, les contractuels et les tierces

parties assument leurs responsabilités et qu'ils sont appropriés aux

rôles auxquels ils sont assignés dans le but de réduire les risques

de vol, de fraude, ou de mauvaise utilisation des ressources

Pour cela il faut définir avant le recrutement de nouvelles personnes :

✓Les rôles et les responsabilités de chaque poste tels que décrits dans la politique de sécurité

✓Les vérifications nécessaire au moment de la demande d'emploi conformément aux lois et aux exigences de l'entreprise

✓Les responsabilités de l'employé en matière de sécurité de l'information dans leurs conditions d'emploi

Démarche d'audit de la SSI
Audit organisationnel et physique

Sécurité des ressources humaines:

8.2 Pendant l'emploi

Objectif: S'assurer que les utilisateurs sont conscients des

menaces qu'encoure la sécurité des informations et qu'ils sont

équipés pour soutenir la politique de sécurité de l'organisation au

cours de leur travail et pour réduire la risque des erreurs humaines.

Pour cela il faut contrôler les points suivants :

✓La gestion des responsabilités quant à l'application des exigences de sécurité de l'organisation

✓L'éducation et la formation à la sécurité de l'information et aux mises à jour des politiques et des procédures de l'organisation

✓La mise en place d'un processus disciplinaire en cas de viol des procédures et des politiques de sécurité

Démarche d'audit de la SSI
Audit organisationnel et physique

Sécurité des ressources humaines:

8.3 Terminaison ou changement d'emploi

Objectif: S'assurer que les employés, les contractuels et les tierces

parties quitte l'organisation ou changent d'emploi d'une manière

ordonnée

Pour cela il faut contrôler les points suivants:

✓Définir clairement les responsabilités de l'employé suite à la terminaison ou au changement de l'emploi

✓Exiger le Retour des actifs lors de l'achèvement des contrats

✓Supprimer les droits d'accès des employés qui ont quitté l'établissement

Démarche d'audit de la SSI
Audit organisationnel et physique

Sécurité physique et sécurité de l'environnement:

9.1 Zones de Sécurité

Objectif: Prévenir les accès non autorisés et les chevauchements

entre les activités de l'organisation.

Afin de réaliser cet objectif, l'organisation doit :

✓Définir les périmètres de sécurité physique.

✓Contrôler les accès physiques.

✓Sécuriser les locaux, les bureaux et les équipements.

✓Protéger les biens contre les menaces externes et environnementales

✓Appliquer les mesures supplémentaires dans les zones de sécurité

✓Isoler les zones de livraison et ceux de chargements

Démarche d'audit de la SSI
Audit organisationnel et physique

Sécurité physique et sécurité de l'environnement:

9.2 Sécurité du matériel

Objectif: Prévenir la perte, les endommagements et les compromis qui peuvent provoquer l'interruption de l'activité de l'entreprise.

Afin d'assurer la sécurité de son matériel, l'organisation doit vérifier:

✓L'emplacement et la protection des équipements

✓La stabilité de l'alimentation électrique

✓La sécurité du câblage

✓La maintenance du matériel

✓La mise au rebut ou la réutilisation du matériel en toute sécurité

✓La possibilité du transport des équipements en dehors du site uniquement sous autorisation

Démarche d'audit de la SSI
Audit organisationnel et physique

Gestion des communications et des opérations:

10.1 Procédures et responsabilités opérationnelles

Objectif: Assurer le fonctionnement correct et la protection des

communications et des opérations sur les informations

Afin de réaliser ces objectifs, l'entreprise doit assurer la:

✓Documentation de toutes les procédures opérationnelles

✓Documentation des modifications apportées aux systèmes

✓Division des responsabilités de façon à réduire l'utilisation non autorisée ou abusive de l'information

✓Séparation des infrastructures de développement et des infrastructures opérationnelles

10.2 Gestion des services délivrés par les tiers

Objectif: Implémenter et maintenir le niveau de sécurité approprié lors de la délivrance des services conformément aux accords signés avec les tiers désignés pour délivrer ces services.

Afin de réaliser ces objectifs, l'entreprise doit veiller à ce que:

✓Les livraisons des biens ou des services se font selon les exigences contenues dans les contrats signés avec tiers

✓La supervision et la revue se font systématiquement sur les services délivrés

✓Les changements apportés aux services livrés par tiers sont gérés de façon à assurer la maintenance et l'amélioration des procédures de sécurité en fonction de la criticité du système

10.3 Planification et recette des systèmes

Objectif: Minimiser le risque des défaillances du système.

Afin de réaliser cet objectif, l'entreprise doit assurer:

✓La planification des capacités en surveillant les demandes d'augmentation en capacités et en évaluant les besoins futurs de capacité afin d'assurer la disponibilité et le stockage adéquat de l'information

✓L'établissement des critères d'acceptation des nouveaux systèmes d'informations et des nouvelles versions ainsi que l'effectuation des tests adéquats avant l'acceptation du système

10.4 Protection contre les codes pernicieux et mobiles

Objectif: Protection de l'intégrité des programmes et des informations.

Afin de réaliser cet objectif, l'entreprise doit assurer:

✓Le contrôle contre les codes pernicieux

✓Le contrôle contre les codes mobiles

10.5 Sauvegarde

Objectif: Maintenir l'intégrité et la disponibilité des informations.

Afin de réaliser cet objectif, l'entreprise doit assurer:

✓La préparation des copies de sauvegarde des informations et des logiciels essentiels de l'entreprise à intervalles réguliers

10.6 Gestion de la sécurité des réseaux

Objectif: Assurer la protection de l'information au niveau du réseau et la protection de l'infrastructure qui la supporte.

Afin de réaliser cet objectif, l'entreprise doit assurer:

✓La mises en place des mesures de contrôle des réseaux pour maintenir la sécurité dans les réseaux informatiques

✓Sécurité des services réseaux pour garantir que les exigences de sécurité des services réseaux sont identifiés et pris en considération lors de l'exploitation du réseau

10.7 Manipulation des supports

Objectif: Prévention contre les modifications, les suppressions ou la destruction des supports et contre l'interruption des activités de l'organisation.

Afin de réaliser ces objectifs, l'entreprise doit assurer:

✓La gestion des supports amovibles

✓Les procédures nécessaires pour la mise au rebut des supports de manière sûre

✓Les procédures de manipulation de l'information

✓La sécurité des documentations des systèmes contre des accès non autorisés

Démarche d'audit de la SSI
Audit organisationnel et physique

10.8 Échanges d'informations

Objectif: Maintenir la sécurité de l'information et l'échange des programmes au sein de l'organisation et avec les entités externes

Afin de réaliser cet objectif, l'entreprise doit établir:

✓Une politique ou procédures d'échange d'informations

✓Un accord sur les échanges des informations et des logiciels entre l'entreprise et des entités externes

✓Protection des supports physiques en transit

✓Protection des messages électroniques

✓Protection des systèmes d'informations liés au commerce

10.9 Services du commerce électronique

Objectif: Assurer la sécurité des services du commerce

électronique et leur utilisation sécurisée.

Afin de réaliser cet objectif, l'entreprise doit assurer:

✓La protection du commerce électronique contre les activités Frauduleuses

✓La protection des informations lors des transaction On-Line contre les problèmes de transmission, de routage et des altérations ou duplications non autorisées

✓La protection des informations disponibles publiquement contre les modifications non autorisées

Démarche d'audit de la SSI
Audit organisationnel et physique

10.10 Supervision

Objectif: Détecter les activités non autorisées sur le système.

Afin de réaliser cet objectif, l'entreprise doit réaliser:

✓Les audits des journaux qui enregistrent les activités et les évènements de sécurité à des intervalles réguliers

✓La supervision des systèmes et la revue des résultats des activités de supervision

✓La Protection des journaux contre les accès non autorisés

✓Les journaux qui archivent les activités des administrateurs et des opérateurs

✓La consignation des défauts par l'archivage des fautes commises dans des fichiers logs

✓La synchronisation des horloges afin d'assurer l'exactitude des journaux d'audit

Démarche d'audit de la SSI
Audit organisationnel et physique

Contrôle des accès

11.1 Exigences du service pour le contrôle des

accès

Objectif : contrôler l'accès aux informations.

L'accès *à l'information devrait être contrôlé sur la base des* exigences de l'activité et celle du degré de sécurité. Pour assurer cet objectif l'organisation doit définir une politique et des règles de contrôle d'accès.

11.2 Gestion des accès utilisateurs

Objectif: Prévenir l'accès non autorisé au système d'information.

Pour assurer la gestion des accès, l'organisation doit :

✓Mettre en place une procédure formelle à fin de contrôler l'attribution du droit d'accès. Cette procédure devrait couvrir tout le cycle d'un utilisateur: enregistrement d'un nouvel utilisateur, suppression de compte, et modification des droits d'accès.

Démarche d'audit de la SSI
Audit organisationnel et physique

✓Gérer les privilèges de façon à ce que l'attribution et l'utilisation de privilèges soient restreintes et contrôlées. L'utilisation non appropriée de privilèges système contribue souvent à des défaillances dans les réseaux multi-utilisateurs.

✓Bien gérer les mots de passe des utilisateurs: l'attribution des mots de passe devrait prendre en considération: l'engagement du personnel de préserver la confidentialité du mot de passe, l'attribution des mots de passe avec une manière sécurisée (délai d'expiration).

✓Revoir régulièrement les droits d'accès des utilisateurs afin de maintenir un contrôle efficace.

11.3 Les responsabilités des utilisateurs

Objectif : Empêcher les accès non autorisés ainsi que l'atteinte ou

le vol des informations

Afin d'empêcher les accès non autorisés, les utilisateurs doivent:

✓Coopérer pour assurer la sécurité

✓Porter des attentions particulières pour maintenir leurs mots de passe confidentiels et leurs équipements sans surveillance sécurisés.

✓Adopter une politique de bureaux et d'écrans dégagés pour les papiers et les supports d'enregistrements afin de protéger les informations contre des accès non autorisés et les pertes

11.4 Contrôles des accès aux réseaux

Objectif : Protéger les services réseaux des accès non autorisés.

L'organisation doit mettre en place une politique de contrôle d'accès aux services du réseau:

✓Faire des chemins d'accès renforcés si nécessaire

✓Authentifier les utilisateurs externes

✓Authentifier les nœuds

✓Protéger les ports distants

✓Segmenter le réseau en plusieurs domaines logiques

✓Contrôler les connexions réseaux a l'aide des tables de routage et des passerelles.

Démarche d'audit de la SSI
Audit organisationnel et physique

11.5 Contrôles des accès aux systèmes

d'exploitation

Objectif: Empêcher l'accès non autorisé aux ordinateurs.

Les procédures au niveau du système d'exploitation devraient être capables de:

✓Vérifier l'identité de chaque utilisateur et si possible le localiser.

✓Mettre en place un système de gestion des mots de passe.

✓Enregistrer les accès réussis et non réussis.

✓Programmer l'arrêt automatique des systèmes placés dans des endroits publics après une certaine période d'inactivité.

✓Restreindre la durée d'accès aux systèmes. Si c'est possible.

11.6 Contrôle de l'accès aux applications

Objectif: Empêcher l'accès aux informations et aux applications

systèmes.

Pour réaliser cet objectif, l'organisation doit:

✓Contrôler l'accès des utilisateurs selon une politique définie

✓Isoler les applications sensibles.

11.7 Informatique mobile et télétravail

Objectif: Assurer la sécurité de l'information lors de l'utilisation des équipements mobiles et du télétravail.

A fin de réaliser cet objectif, il faut :

✓Mettre en place une politique formelle pour tenir compte des risques impliqués par le travail avec des unités informatiques mobiles, et à travers des infrastructures de communications différentes

✓Contrôler les activités et la sécurité physique du site de télétravail ainsi que les moyens de communication.

Maintenance, Développement et acquisition des systèmes d'information

12.1 Exigence de sécurité des systèmes d'informations

Objectif: S'assurer que la sécurité est intégrée dans les systèmes d'information. Ceci comprend :

Analyse et spécification des exigences de sécurité (y compris les besoins de plans d'urgences) qui devraient être déterminées dans la phase appropriée du projet, comme elles doivent être documentées et faire partie du système d'information.

12.2 Correction des processus dans les applications

Objectif: Prévenir la perte, la modification, et la mauvaise utilisation des données utilisateurs dans les applications.

Pour assurer le bon fonctionnement des applications II faut:

✓Contrôler les données d'entrée des applications afin de s'assurer de leur intégrité.

✓Implémenter un contrôle de traitement interne afin de détecter toute altération des données

✓Implémenter des messages d'authentification afin de détecter les changements non autorisés ou la corruption des messages électroniques transmis.

✓Contrôler les données de sortie afin de s'assurer que le processus de stockage d'information est intact et approprié

12.3 Mesures cryptographiques

Objectif: Protéger la confidentialité, l'authenticité et l'intégrité de l'information en utilisant des moyens cryptographiques.

✓Les systèmes cryptographiques devraient être utilisés pour les informations à risque pour les quelles les autres mesures n'assurent pas une protection adéquate.

✓Mettre en place un système de gestion des clés afin de permettre l'utilisation de techniques cryptographiques basées sur un ensemble convenu de normes, de procédures et de méthodes sûres.

12.4 Sécurité des fichiers systèmes

Objectif: Assurer la sécurité des fichiers systèmes

Afin de réaliser cet objectif l'organisation doit établir:

✓Contrôle des logiciels opérationnels lors de leur implantation sur les systèmes. Les systèmes opérationnels ne doivent pas contenir le code source des applications (si possible).

✓Protection des données d'essai des systèmes

✓Contrôle de l'accès aux codes et aux bibliothèque des programmes sources

Démarche d'audit de la SSI
Audit organisationnel et physique

12.5 Sécurité des environnements de développement

et de maintenance

Objectif: Maintenir la sécurité des applications et des informations lors du développement et de la maintenance.

Pour maintenir leur sécurité l'organisation doit:

✓S'assurer que tous les changements effectués sur les systèmes (ou applications) ne touchent pas la sécurité du système

✓Effectuer régulièrement un examen technique sur les modifications apportées aux progiciels et établir des restrictions sur les modifications apportées aux progiciels (uniquement par le vendeur)

✓Prévenir les fuites d'information

✓Protéger le développement des logiciels sous-traités

12.6 Gestion des vulnérabilités

Objectif: Réduire le risque résultant de l'exploitation des vulnérabilités techniques

Pour cela l'organisation doit assurer:

✓Le contrôle et l'évaluation régulières des vulnérabilités techniques

✓La prise en considération de ces vulnérabilités par les mesures et les corrections nécessaires

Démarche d'audit de la SSI
Audit organisationnel et physique

Management des incidents de la sécurité de l'information

13.1 Signalisation des événements de la sécurité de l'information et ses faiblesses

Objectif: Assurer que les évènements et les faiblesses de la sécurité de l'information associés aux systèmes sont communiqués de manière à permettre l'accomplissement des actions correctives à temps.

Pour cela l'organisation doit sensibiliser les employés à la:

✓Signalisation des évènements de la sécurité de l'informations le plus rapidement possible

✓Signalisation des faiblesses de sécurité dans les systèmes et les services

13.2 Gestion des incidents de la sécurité de l'information et améliorations

Objectif: Assurer qu' une approche consistante et efficace est appliquée dans la gestion des incidents de sécurité de l'information

La gestion des incidents de sécurité commence par :

✓Etablir les procédures nécessaires pour répondre rapidement et efficacement aux incidents de sécurité

✓Etude des incidents de sécurité de l'information en surveillant et quantifiant les coûts et les volumes des incidents de sécurité afin de déterminer l'impact qu'auront ces interruptions

✓Collecte des éléments de preuve suite à un incident de sécurité

Démarche d'audit de la SSI
Audit organisationnel et physique

Gestion de la continuité des activités de l'entreprise
14.1 Aspects de la sécurité de l'information dans la gestion de la continuité des activités de l'entreprise

Objectif: Empêcher les interruptions des activités de l'entreprise et protéger les processus critiques des effets de la majorité des défaillances du système d'informations ou des désastres et d'assurer leur reprise à temps

Pour cela l'organisation doit procéder à :

✓Introduction de la sécurité de l'information dans le processus de gestion de la continuité des activités de l'entreprise

✓Continuité des activités de l'entreprise et recensement des risques en identifiant les interruptions des activités de l'entreprises avec leur impact et leur probabilité d'occurrences

✓Développement et mise en oeuvre des plans de continuité incluant la sécurité de l'information

✓Etablissement d'un cadre de planification de la continuité des activités de l'entreprise

✓Essai, maintien et réévaluation des plans de continuité des activités de l'entreprise

La Conformité

15.1 Conformité aux exigences légales

Objectif : Eviter toute infraction des lois criminelles, civiles, statutaires, et réglementaires.

La conception, le fonctionnement, l'utilisation et la gestion des systèmes d'information peuvent être soumis aux exigences légales et règlementaires de la sécurité.

Les actions suivantes doivent être effectuées:

✓Identification des lois applicables : Les exigences ainsi que les responsabilités répondant à des exigences devraient être identifiées, explicitement définies et documentées.

✓Préservation du droit de la propriété intellectuelle, c'est-à-dire préservation du copyright des produits développés par le personnel de l'entreprise ou des logiciels achetés.

Démarche d'audit de la SSI
Audit organisationnel et physique

✓Protection des enregistrements organisationnels: les documents importants de l'organisation doivent être protégés des pertes, de la destruction et de la falsification

✓Protection des données et des informations privées du personnel.

✓Prévention de l'utilisation mal intentionnée de l'information et des outils: il faut donner une autorisation formelle aux employés pour l'utilisation des équipements et bien définir les périmètres de l'utilisation.

✓Réglementation des mesures cryptographiques

Démarche d'audit de la SSI
Audit organisationnel et physique

15.2 Conformité avec la politique de sécurité et les

standards et la conformité technique

Objectif: Assurer la conformité du système avec la politique de sécurité et avec les standards.

Le système de sécurité d'information doit être revu régulièrement pour:

✓Vérifier l'application des procédures et mesures de sécurité au niveau du système d'information, utilisateurs, Direction et au niveau des fournisseurs du système conformément à la politique de sécurité et aux standards.

✓Vérifier la conformité technique des équipements par les outils ou les logiciels appropriés (faire des tests par rapport aux normes de mise en oeuvre de la sécurité).

Démarche d'audit de la SSI
Audit organisationnel et physique

15.3 Considérations sur les audits des systèmes d'informations

Objectif: Maximiser l'efficacité et minimiser les interférences entre les systèmes d'informations et les processus d'audit.

Le contrôle d'audit des systèmes d'informations doit obéir aux conditions:

L'audit système devrait être planifié afin de minimiser les risques de perturbations des processus de l'entreprise et ce en fixant les paramètres suivants :

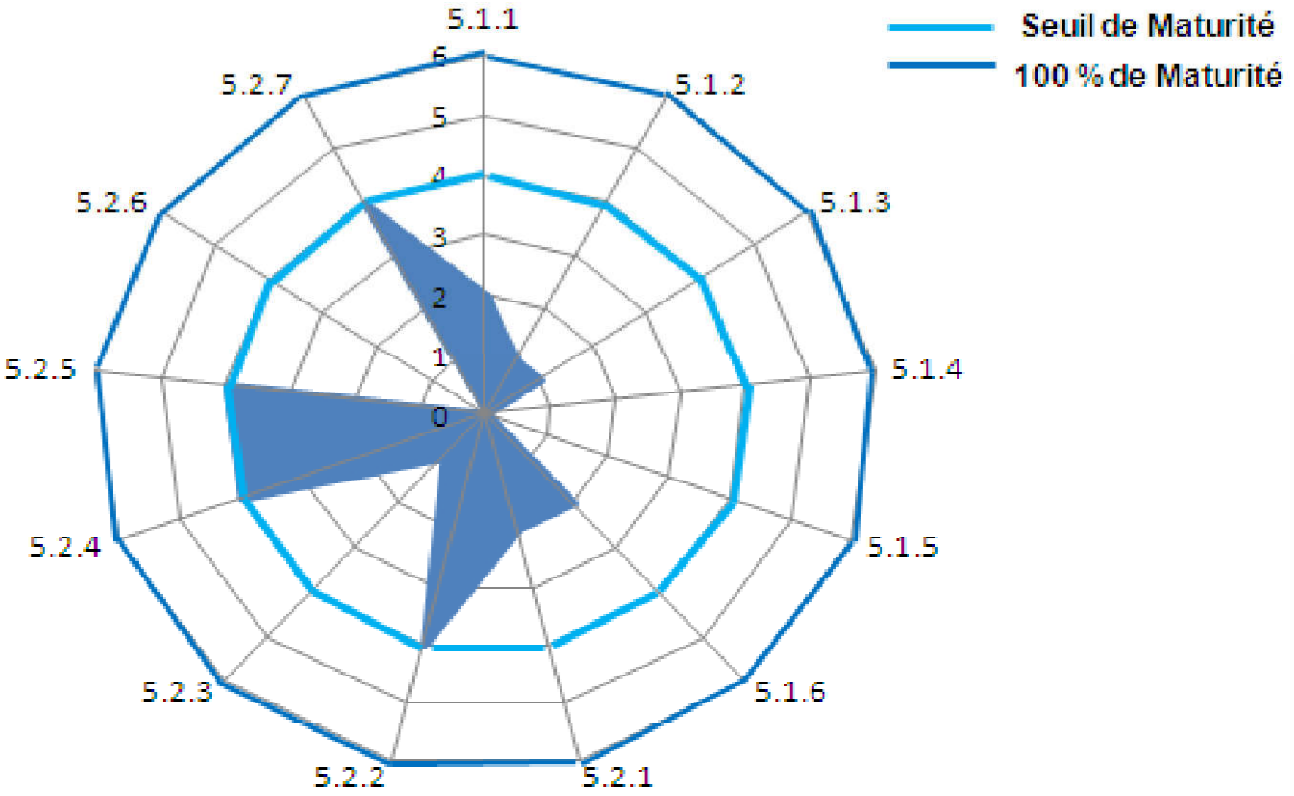
- Le domaine d'application de l'audit
- La manipulation des informations et des données lors de l'audit en lecture seule (si besoin d'écriture, alors travailler sur des copies)
- Les ressources IT pour l'exécution des contrôles doivent être identifiées explicitement et doivent être valables
- La supervision et la journalisation de tout accès.

✓L'accès et l'intégrité des outils d'audit doivent être protégés afin d'empêcher toute atteinte ou toute utilisation abusive éventuelle .

Démarche d'audit de la SSI
Audit organisationnel et physique

5 Sécurité physique et de l'environnement	Entièrement mise en œuvre	Partielement mise en œuvre	Planifié	Pas implémenté ni planifié
5.1 Zones de sécurité				
5.1.4 - Protection contre les menaces externes et environnementales : Existe-t-il une protection physique des biens de l'établissement contre les incendies, le feu et d'autres formes de désastres?				
5.1.6 - Accès public, zone de livraison et de chargement : Est-ce que les zones de livraison et de chargement sont contrôlées et, si possible, isolées des infrastructures de traitement de l'information afin d'éviter tout accès non autorisé?				
5.2 - Sécurité du matériel				
5.2.2 - Alimentation électrique : Est-ce que les équipements sont protégés contre les pannes de courant ou les autres anomalies électriques?				
5.2.3 - Sécurité du câblage : Est-ce que les câblages électriques et de télécommunications transmettant des données ou supportant des services d'information sont protégés contre les interceptions ou les dommages?				
5.2.5 - Sécurité du matériel utilisé à l'extérieur des locaux : Est-ce que les procédures de sécurité sont appliquées sur le matériel utilisé à l'extérieur en prenant en considération les conditions du travail en dehors des locaux de l'établissement ?				

Démarche d'audit de la SSI
Audit organisationnel et physique (suite 2)

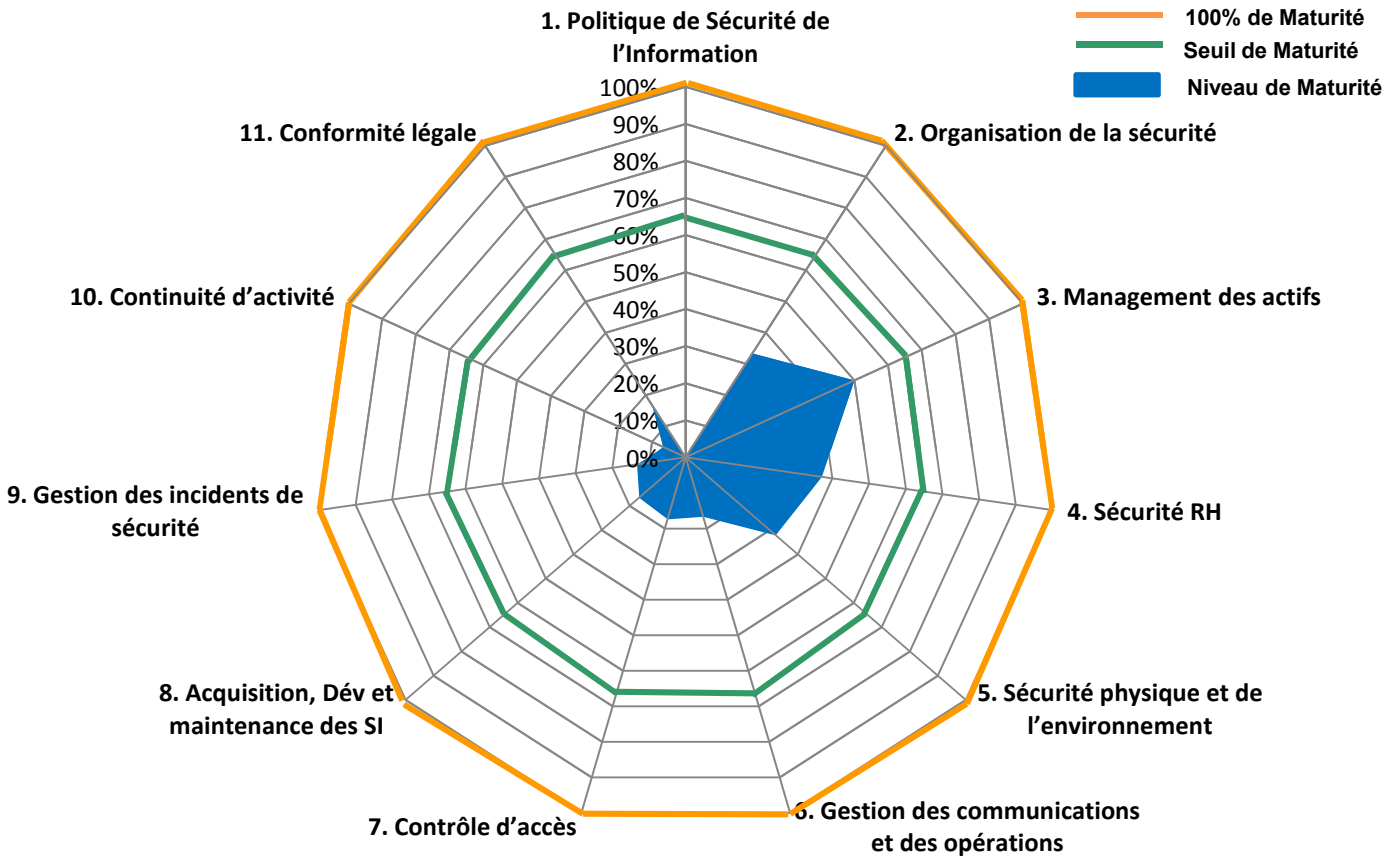


5 Sécurité physique et de l'environnement

Démarche d'audit de la SSI
Audit organisationnel et physique (suite 3)

Chapitres de l'ISO/CEI 27002	Moyenne	Seuil de Maturité
1. Politique de Sécurité de l'Information	00,00%	65%
2. Organisation de la sécurité	33,33%	65%
3. Gestion des biens	50,00%	65%
4. Sécurité RH	37,04%	65%
5. Sécurité physique et de l'environnement	32,05%	65%
6. Gestion des communications et des opérations	16,67%	65%
7. Contrôle d'accès	17,36%	65%
8. Acquisition, Développement et maintenance des SI	16,67%	65%
9. Gestion des incidents de sécurité	13,33%	65%
10. Continuité d'activité	06,67%	65%
11. Conformité légale	16,67%	65%

Démarche d'audit de la SSI
Audit organisationnel et physique (suite 4)



Rosace du niveau de maturité du système par rapport à la norme ISO 27002 : 2005

Démarche d'audit de la SSI
Analyse des risques

La démarche :

1. **Identification des menaces et des vulnérabilités,**
2. **Déterminer une échelle des risques,**
3. **Déterminer une classification (disponibilité, intégration, confidentialité) des menaces spécifiques au système,**
4. **Déterminer une classification des actifs critiques de l'entreprise,**
5. **Déterminer l'impact des différentes menaces sur la SSI.**

Démarche d'audit de la SSI
Analyse des risques (suite)

De nombreuses méthodes d'analyses de risque ont été développées: Marion, MEHARI, EBIOS, …

Risque = Menace*Impact*Vulnérabilité

	Menace	Vulnérabilité	Impact				Calcul du Risque	Niveau de Maturité
			Disponibilité	Intégrité	Confidentialité	Légalité		
Accident physique								
Incendie	1,00	2,00	1,00				2,00	4,00
Inondation								
Tempête								
Pertes des données								
Crash du serveur								
Effacement involontaire de fichiers								
Altération de support amovible								

Démarche d'audit de la SSI
Audit technique

L'audit technique s'attache à identifier les vulnérabilités du SI.

L'audit technique portera principalement sur 3 parties :

-Phase 1 : Audit de l'architecture du système
-Phase 2 : Audit de la résistance du système
-Phase 3 : Audit de l'architecture de sécurité existante
-Phase 4 : Audit de l'opacité du réseau depuis l'extérieur

Outils d'audit technique:

Partie	Outil utilisé	Description
Audit de l'architecture Réseau & système	Network View	Outil compact de découverte et de management de réseau pour la plate forme Win32
Audit de la résistance du système aux failles connues	Nessus	c' est un scanner de vulnérabilité qui signale les faiblesses potentielles sur les machines testées.
Tests d'intrusion	Metasploit	Metasploit Framework est un logiciel permettant l'exploitation d'un système, c'est un outil d'intrusion.

Démarche d'audit de la SSI
Audit technique

-Phase 1 : Audit de l'architecture du système
Cette phase consiste à reconnaitre les différents éléments physiques et logiques du système d'information de l'établissement. L'audit de l'architecture du système comprend essentiellement les parties suivantes :
•Reconnaissance du réseau et du plan d'adressage.
•Sondage des systèmes
•Sondage du réseau

-Phase 2 : Audit de la résistance du système
La seconde phase de l'audit technique comporte un audit de la résistance du système face aux failles connues, grâce à une analyse automatisée des vulnérabilités au niveau de tous les composants du réseau audité grâce à un ensemble d'outils de scan permettant la mise au point d'une démarche efficace.

Démarche d'audit de la SSI
Audit technique

-Phase 3 : Audit de l'architecture de sécurité existante

L'objectif de cette phase est d'expertiser l'architecture technique déployée et de mesurer la l'efficacité des configurations des équipements réseaux et la politique de sécurité définie.

-Phase 4 : Audit de l'opacité du réseau depuis l'extérieur

Démarche d'audit de la SSI
Recommandations et plan d'action

- ✓ **Dégager des insuffisances au niveau des mesures organisationnelles et techniques par rapport aux différentes clauses des normes de sécurité,**
- ✓ **Proposer des recommandations:**
  - o **Recommandations d'ordre organisationnel et physique**
  - o **Recommandations techniques**
- ✓ **Elaborer un plan d'action,**
- ✓ **Proposer une architecture réseau améliorée et sécurisée.**

MERCI POUR VOTRE ATTENTION