JSLC

INFORMATION SECURITY RISK MANAGER

GESTION DES RISQUES & NORME ISO 27005

SOMMAIRE

SOMMAIRE

PARTIE 1

PRÉSENTATION GÉNÉRALE DE LA NORME ISO 27005

SOMMAIRE PARTIE 1:

Introduction à la Sécurité de l'Information

Qu'est ce que l'information pour l'entreprise ?

L'information est un actif qui a de la valeur pour une organisation et doit donc, en conséquence, être protégé de manière adéquate.

Quelles sont les formes de l'information dans l'entreprise ?

- Manuscrites ou imprimées.
- Numériques.
- Transmises par courrier ou par courrier électronique.
- Diffusées par vidéo conférence.
- Verbales.

Les étapes de la vie de l'information

CREATION | TRAITEMENT | DIFFUSION | CONSERVATION | FIN DE VIE

Valeur

ACQUISITION
SAISIE

TRAITEMENT

STOCKAGE

ARCHIVAGE

DESTRUCTION

TRANSFERT

DUPLICATION

IMPRESSION

ENVOI

Temps

Introduction à la Sécurité de l'Information

Protéger l'information

« Quelle que soit la forme des informations, ou les moyens de partage ou de stockage, l'information doit toujours être correctement protégée. »

(ISO 27002)

Il s'agit de protéger l'information notamment en terme de :

- **Disponibilité** : Assurer que les utilisateurs autorisés ont accès à l'information et aux actifs associés quand ils en ont besoin.
- **Intégrité** : La capacité de maintenir la véracité et la complétude des actifs.
- **Confidentialité** : Assurer que l'information n'est accessible qu'aux individus, entités ou processus qui y sont autorisés.

Introduction à la Sécurité de l'Information

- Qu'est ce qu'un risque ?

« Possibilité qu'une **menace** donnée exploite les **vulnérabilités** d'un **actif** ou d'un groupe d'actifs et nuise donc à l'organisation ».

Introduction à la Sécurité de l'Information

Qu'est qu'un actif ?

« Tout élément représentant de la valeur pour l'organisme » *(ISO 27001)*

Les actifs primordiaux

- Processus et activités métier
- Informations

Les actifs supports

- Matériels : serveurs, poste de travail, clé usb, imprimante, ect.
- Logiciels : applications, systèmes d'exploitation, Système de gestion de BDD, etc.
- Réseaux : interconnections électroniques ou téléphoniques, etc.
- Personnel : compétences stratégiques
- Site : locaux, batiments, etc.
- Structure de l'organisme : procédures, circuit de validation, etc.

Introduction à la Sécurité de l'Information

Qu'est ce qu'un processus ?

Un processus est un ensemble d'activités gérées et organisées dans le temps, permettant la transformation d'éléments d'entrée en éléments de sortie.

Qu'est ce qu'une activité ?

Ensemble de taches bien définies qui mettent en œuvre le processus.

Exemple de Processus : vente des produits en magasin

Exemples de Tâches : enregistrement du produit par le caissier, paiement du client

Introduction à la Sécurité de l'Information

Qu'est ce qu'une menace ?

Les menaces sont des évènements susceptibles d'endommager les actifs tels que des informations, des processus et des systèmes et, par conséquent, des organismes.

Les menaces peuvent être d'origine naturelle ou humaine et peuvent être accidentelles ou délibérées.

Exemples de menaces

Incendie

Phénomène sismique

Panne d'alimentation en électricité

Etc.

Vol de supports ou de documents

Erreur d'utilisation

Dysfonctionnement du logiciel

Introduction à la Sécurité de l'Information

Qu'est ce qu'une vulnérabilité ?

Les vulnérabilités sont les éléments pouvant être exploités par les menaces pour nuire aux actifs ou à l'organisme.

Exemples de vulnérabilités

Menaces	Actif	Vulnérabilités
Vol de supports	Matériel	Manque de prudence lors de la mise au rebut
Erreur d'utilisation	Logiciel	Formation insuffisante à la sécurité
Espionnage à distance	Réseau	Transfert de mots de passe en clair

Gestion des risques SI - Définition

- Qu'est ce que la gestion du risque ?

« Ensemble d'activités coordonnées visant à diriger et piloter un organisme vis-à-vis du risque »

(ISO 73 : 2002)

Gestion des risques SI - Activités

Il convient que la gestion des risques contribue à :

- l'identification des risques,
- l'appréciation des risques en termes de conséquences sur les activités métier et de vraisemblance,
- la communication et la compréhension de la vraisemblance et des conséquences de ces risques,
- l'établissement d'un ordre de priorité pour le traitement du risque,
- la priorisation des actions afin de réduire les occurrences des risques,
- l'implication des parties prenantes lors de la prise de décisions relatives à la gestion du risque et l'information sur l'état de la gestion du risque,
- l'efficacité de la supervision du traitement du risque,
- la surveillance et le réexamen réguliers des risques et du processus de gestion de risque,
- la capture de l'information afin d'améliorer l'approche de gestion du risque,
- la formation des dirigeants et du personnel sur les risques et les actions à entreprendre pour atténuer.

Gestion des risques SI – Domaines d'application

- La gestion des risques SI peut s'appliquer :
  - À un organisme dans son ensemble,
  - À toute partie distincte d'un organisme : *un département, un lieu physique, un service,*
  - À tout un système d'information existant ou prévu
  - À des mesures de sécurité particulières : *la planification de la continuité d'activité par exemple.*

ISO/IEC 27005 - Objet

La norme ISO 27005 fournit des lignes directrices relatives à la gestion des risques en sécurité de l'information.

- Elle présente un ensemble d'activités pour la gestion des risques, leurs objectifs et leurs entrées-sorties mais ne fournit aucune méthodologie spécifique.

ISO/IEC 27005 - Utilisation

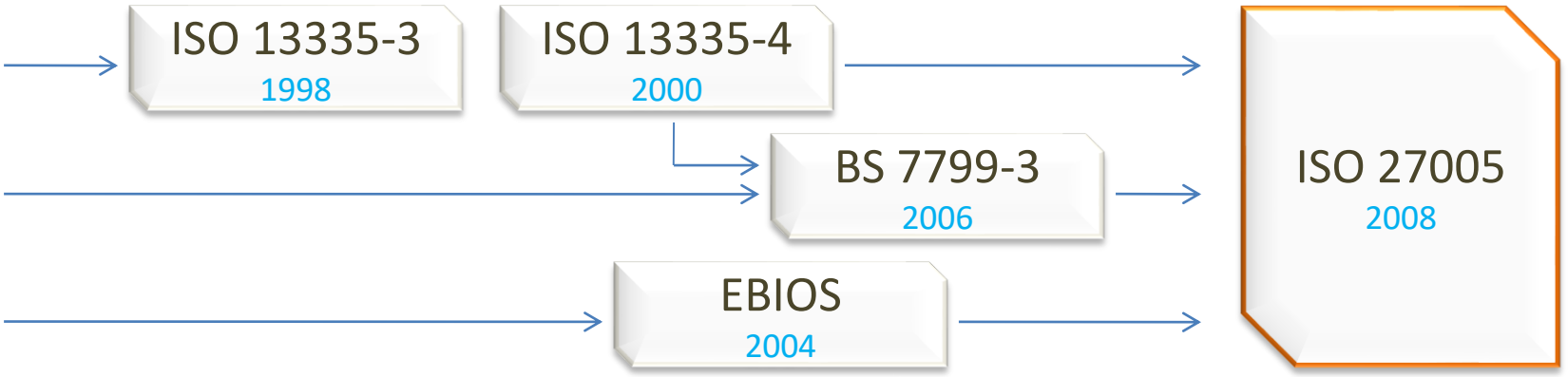
- La norme fournit un cadre qui permet de constituer sa propre méthodologie.
- Plusieurs méthodologies existantes se sont déjà alignées sur la norme. Exemples : MEHARI 2010, EBIOS 2010
- Votre méthodologie de gestion des risques SI peut être une méthodologie interne et personnalisée, alignée sur la norme 27005 sans être pour autant fondée sur une méthodologie connue.

ISO/IEC 27005 - Contexte

Famille de normes 2700X

27000	Principes et vocabulaires
27001	Exigences SMSI
27002	Bonnes pratiques SSI
27003	Guide d'implémentation d'un SMSI
27004	Métriques et mesures
27005	Gestion des risques SI
27006	Exigences audits/certification
…	…

ISO/IEC 27005 - Historique



- **ISO/IEC 13335**
  Guide pour la gestion de la sécurité des technologies de l'information et de la communication.

- **BS7799-3**
  Guide pour l'appréciation des risques de sécurité de l'information

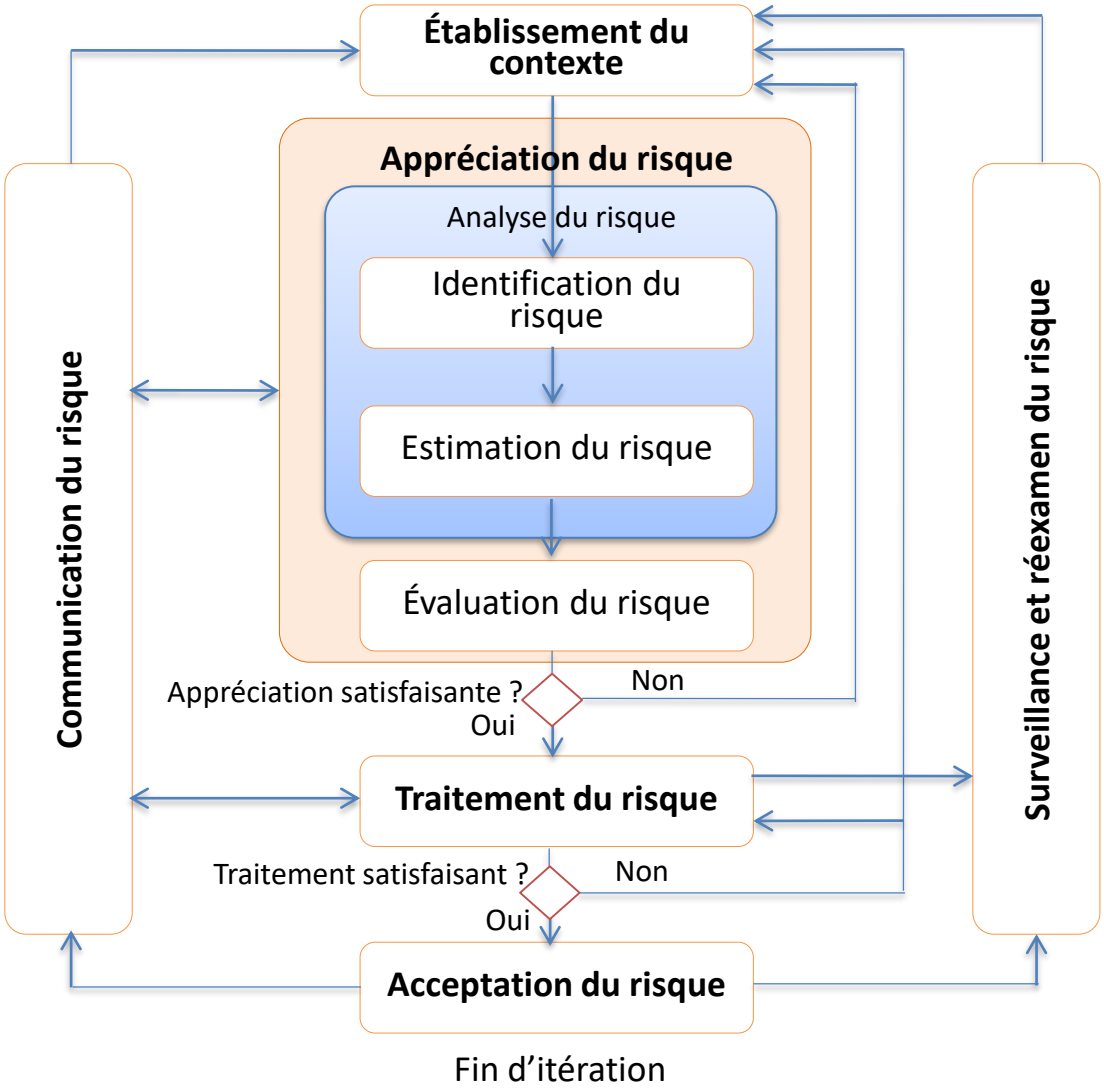
- **EBIOS**
  Expression des Besoins et Identification des Objectifs de Sécurité

ISO/IEC 27005 – La gestion des risques SI

- La norme propose une gestion des risques sous la forme d'un processus continu.

- Une approche systématique qui permettrait d'approfondir et d'affiner l'appréciation des risques à chaque itération et de s'assurer que le risque est apprécié de manière appropriée.

ISO/IEC 27005 – Son processus de gestion des risques SI



PARTIE 2

DESCRIPTION DU PROCESSUS DE GESTION DES RISQUES

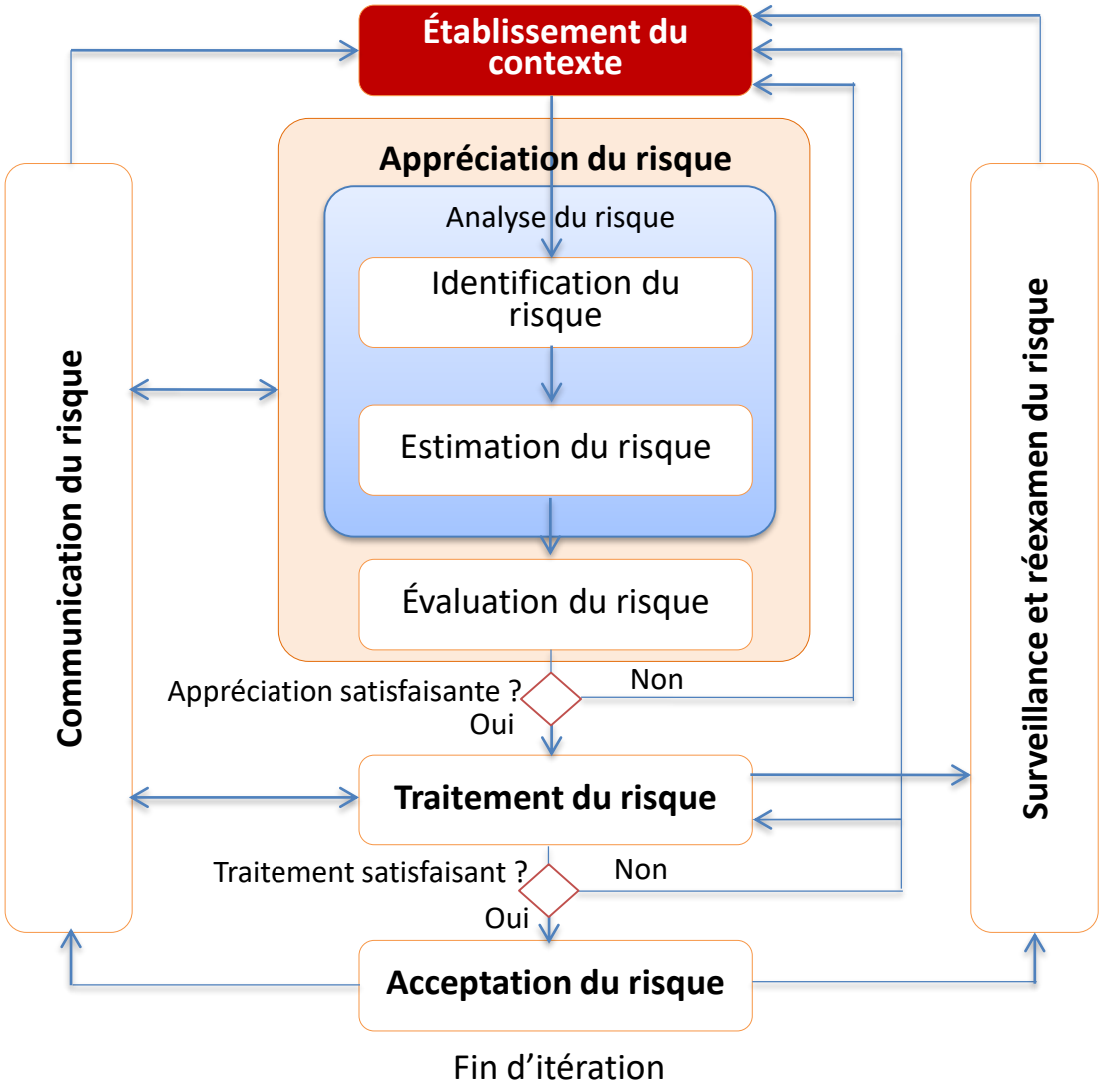
SOMMAIRE PARTIE 2

Le processus de gestion du risque se décompose en 6 activités :

- Etablissement du contexte
- Appréciation du risque
- Traitement du risque
- Acceptation du risque
- Communication du risque
- Surveillance et réexamen du risque

7

Etablissement du contexte



7. Établissement du contexte

Action

Etablir le contexte de la gestion du risque en sécurité de l'information consiste à :

- Déterminer l'**objectif** de la gestion des risques en SI,
- Définir le **domaine d'application** et ses limites,
- Etablir une **organisation** adaptée au fonctionnement de la gestion du risque en sécurité de l'information.
- Déterminer les **critères de base** nécessaires à la gestion du risque en sécurité de l'information ;

7. Établissement du contexte

7.1. *Objectif*

Déterminer l'objectif

Il est essentiel de déterminer l'objectif de la gestion du risque en sécurité de l'information. Cet objectif peut être :

- La mise en place d'un SMSI,
- la conformité avec la loi et la preuve de la mise en œuvre du devoir de précaution,
- l'homologation d'un système d'information,
- la préparation d'un plan de continuité de l'activité, d'un plan de réponse aux incidents,
- la description des exigences en matière de sécurité de l'information pour un produit, un service ou un mécanisme,
- l'élaboration d'une politique de sécurité de l'information,
- la contribution à la gestion globale des risques de l'organisme

7. Établissement du contexte

7.3 *Domaine d'application et limites*

□ Définir le domaine d'application et ses limites

Pour rappel, la gestion des risques SI peut s'appliquer

- À un organisme dans son ensemble,
- À toute partie distincte d'un organisme : *un département, un lieu physique, un service, un processus métier,*
- À tout un système d'information existant ou prévu
- Une application
- À des mesures de sécurité particulières : *la planification de la continuité d'activité par exemple.*

D'autres éléments sont à étudier pour définir le domaine d'application et ses limites

7. Établissement du contexte

7.3 *Domaine d'application et limites*

Définir le domaine d'application et ses limites

Les éléments suivants sont à étudier pour définir le domaine d'application :

- Les caractéristiques de l'organisme
- Les contraintes affectant l'organisme
- Les exigences légales, réglementaires et contractuelles applicables à l'organisme
- Les contraintes affectant le domaine d'application

7. Établissement du contexte

7.3 *Domaine d'application et limites*

Caractéristiques de l'organisme 1/2

- Son principal objectif : raison pour laquelle il existe

  exemple : domaine d'activité, segment de marché, etc.

- Son activité : ses techniques et le savoir faire de ses employés, lui permettant de remplir ses missions .

- Ses missions qui permettent d'atteindre son objectif : identifier les services fournis et/ou les produits fabriqués par rapport aux utilisateurs finaux.

- Ses valeurs : principes majeurs ou code de conduite appliqué à la pratique de l'activité. *Exemple : qualité des produits, relation avec les clients, etc.*

7. Établissement du contexte

7.3 *Domaine d'application et limites*

Caractéristiques de l'organisme 2/2

- Sa stratégie : Principes directeurs de l'organisme, objectifs stratégiques métiers, politiques, problématiques en jeu et changement majeurs prévus
- Sa structure : Niveaux de processus décisionnel, leadership et opérationnel
- Son organigramme : Schématiser la structure de l'organisme , les axes hiérachiques, délégation de l'autorité et flux d'informations.
- Ses processus métiers :
- Les interfaces : échanges d'informations avec l'extérieur

7. Établissement du contexte

7.3 *Domaine d'application et limites*

Définir le domaine d'application et ses limites

Les éléments suivants sont à étudier pour définir le domaine d'application :

- Les caractéristiques de l'organisme
- Les contraintes affectant l'organisme
- Les exigences légales, réglementaires et contractuelles applicables à l'organisme
- Les contraintes affectant le domaine d'application

7. Établissement du contexte

7.3 *Domaine d'application et limites*

Contraintes affectant l'organisme 1/3

- Contraintes de nature politique: administrations, institutions publiques, applications des décisions gouvernementales *(Exemples : sécurisation des flux électroniques, informatisation des factures non sécurisé etc.)*

- Contraintes de nature stratégique: changement prévus ou potentiels des structures ou de l'orientation de l'organisme *(Exemples : coopération internationnale impliquant des accords pour la sécurité des échanges)*

- Contraintes territoriales: Distribution des sites sur l'ensemble du territoire national ou à l'étranger (Exemples : ambassades, banques,…)

- Contraintes liées au climat économique et politique : Continuité des services même si grèves ou crises nationales ou internationales.

7. Établissement du contexte

7.3 *Domaine d'application et limites*

Contraintes affectant l'organisme 2/3

- Contraintes structurelles : Exigences de sécurité spécifiques

  Exemple : structure internationnale, exigences spécifiques à chaque pays

- Contraintes fonctionnelles : Dépend des missions de l'organisme

  Exemple : travaille 24h/24, les ressources doivent toujours être disponibles

- Contraintes liées au personnel : Responsabilités, recrutement, qualification, formation, disponibilité, confidentialité.

- Contraintes liées au calendrier: délais imposés.

- Contraintes liées aux méthodes : gestion des projets

7. Établissement du contexte

7.3 *Domaine d'application et limites*

Contraintes affectant l'organisme 3/3

- Contraintes de nature culturelle : habitudes de travail, croyances, etc.

  Exemple : Fouille au corps interdite dans certainspays.

- Contraintes budgétaires : investissements liés à la sécurité, justifications économiques. *Exemple : coût total des mesures ne soit pas supérieur au coût des conséquences du risque.*

7. Établissement du contexte

7.3 *Domaine d'application et limites*

Définir le domaine d'application et ses limites

Les éléments suivants sont à étudier pour définir le domaine d'application :

- Les caractéristiques de l'organisme
- Les contraintes affectant l'organisme
- Les exigences légales, réglementaires et contractuelles applicables à l'organisme
- Les contraintes affectant le domaine d'application

7. Établissement du contexte

7.3 *Domaine d'application et limites*

- Exigences légales, réglementaires et contractuelles
  - Exigences légales et réglementaires: lois et actes réglementaires : décrets, arrêtés, réglements spécifiques aux domaines ou réglements internes ou externes.
  - La norme ISO 27001 insiste notamment sur :
    - Les droits de propriété intellectuelle (DPI)
    - La protection des enregistrements de l'organisme
    - La protection des données et confidentialité des informations relatives à la vie privée
    - La prévention à l'égard de l'utilisation de moyens de traitement de l'information à des fins illégales.
    - Réglementation relative aux mesures cryptographiques
  - Exigences contractuelles *:* contrats et accords convenu avec des tiers

7. Établissement du contexte

7.3 *Domaine d'application et limites*

Définir le domaine d'application et ses limites

Les éléments suivants sont à étudier pour définir le domaine d'application :

- Les caractéristiques de l'organisme
- Les contraintes affectant l'organisme
- Les exigences légales, réglementaires et contractuelles applicables à l'organisme
- Les contraintes affectant le domaine d'application

7. Établissement du contexte

7.3 *Domaine d'application et limites*

Contraintes affectant le domaine d'application 1/3

- Contraintes techniques: exigences relatives à
  - L'architecture générale (topologie, architecture physique, etc.),
  - Les logiciels d'application (conception, standard, etc.)
  - Les progiciels (standard, qualité, évaluation, conformité aux normes, à la sécurité, etc.)
  - Le matériel (standard, qualité, conformité aux normes)
  - Les réseaux de communication (couverture, standard, capacité, fiabilité)
  - L'infrastructure des bâtiments (Génie civil, construction, hautes et basses tension)

7. Établissement du contexte

7.3 *Domaine d'application et limites*

Contraintes affectant le domaine d'application 2/3

- Contraintes financières : limite de budget, négociable sur la base de l'étude de la sécurité.
- Contraintes environnementales : pays, climats, risques naturels, situation géographique, climat économique
- Contraintes de temps : mise en œuvre des mesures avant que les risques ne changent.
- Contraintes liées aux méthodes : Adaptée au savoir faire de l'organisme pour la gestion des projets

7. Établissement du contexte

7.3 *Domaine d'application et limites*

Contraintes affectant le domaine d'application 3/3

- Contraintes organisationnelles : exigences relatives :
  - Au Fonctionnement : *délais d'exécution, de fourniture des services,*
  - À la maintenance : *diagnostics d'incidents, actions rapides*
  - À la gestion des ressources humaines : *formation du personnel, qualification des postes sensibles, etc.*
  - À la gestion administrative : *responsabilités, etc*.
  - À la gestion du développement : *outils, génie logiciel, plans d'acceptation*
  - À la gestion des relations extérieurs : *tiers, contrats*

7. Établissement du contexte

7.3 *Domaine d'application et limites*

- A prendre en compte également
  - La Politique de sécurité de l'information de l'organisme
  - L'approche globale de l'organisation vis-à-vis de la gestion du risque

7. Établissement du contexte

7.3 *Domaine d'application et limites*

EXERCICE

ETABLISSEMENT DU CONTEXTE

Définition du domaine d'application et des limites du processus de gestion du risque en sécurité de l'information.

7.Établissement du contexte

7.4 L'organisation de la gestion du risque

Déterminer et de maintenir l'organisation et les responsabilités relatives au processus de gestion du risque en sécurité de l'information :

- élaboration du processus de gestion du risque en sécurité de l'information adapté à l'organisme,
- identification et analyse des parties prenantes,
- définition des rôles et des responsabilités de toutes les parties, à la fois internes et externes à l'organisme,
- établissement des relations entre l'organisme et les parties prenantes,
- détermination des processus d'escalade,
- spécification des enregistrements à conserver.

7.Établissement du contexte

7.4 L'organisation de la gestion du risque

Dans le cadre de la mise en œuvre d'un SMSI, la norme ISO 27001 exige notamment que :

« La direction doit fournir la preuve de son implication dans l'établissement, la mise en œuvre, le fonctionnement, la surveillance et le réexamen, la mise à jour et l'amélioration du SMSI, par: »

[…]

« la détermination des critères d'acceptation des risques et des niveaux de risque acceptables; »

(Cf. Chapitre 5.1.f de l'ISO 27001)

7. Établissement du contexte

7.2 Critères de base

Il convient de choisir ou d'élaborer une approche de gestion du risque adaptée qui comprenne des critères de base tels que :

- **Des critères d'impact**

  Critères utilisés pour définir le changement radical au niveau des objectifs métiers atteints que peut entrainer chaque risque.

- **Des critères d'évaluation des risques**

  Critères utilisés pour comparer les valorisations de chaque risque et décider des actions à entreprendre, en prenant en compte les critères d'acceptation et en déterminant leur priorité.

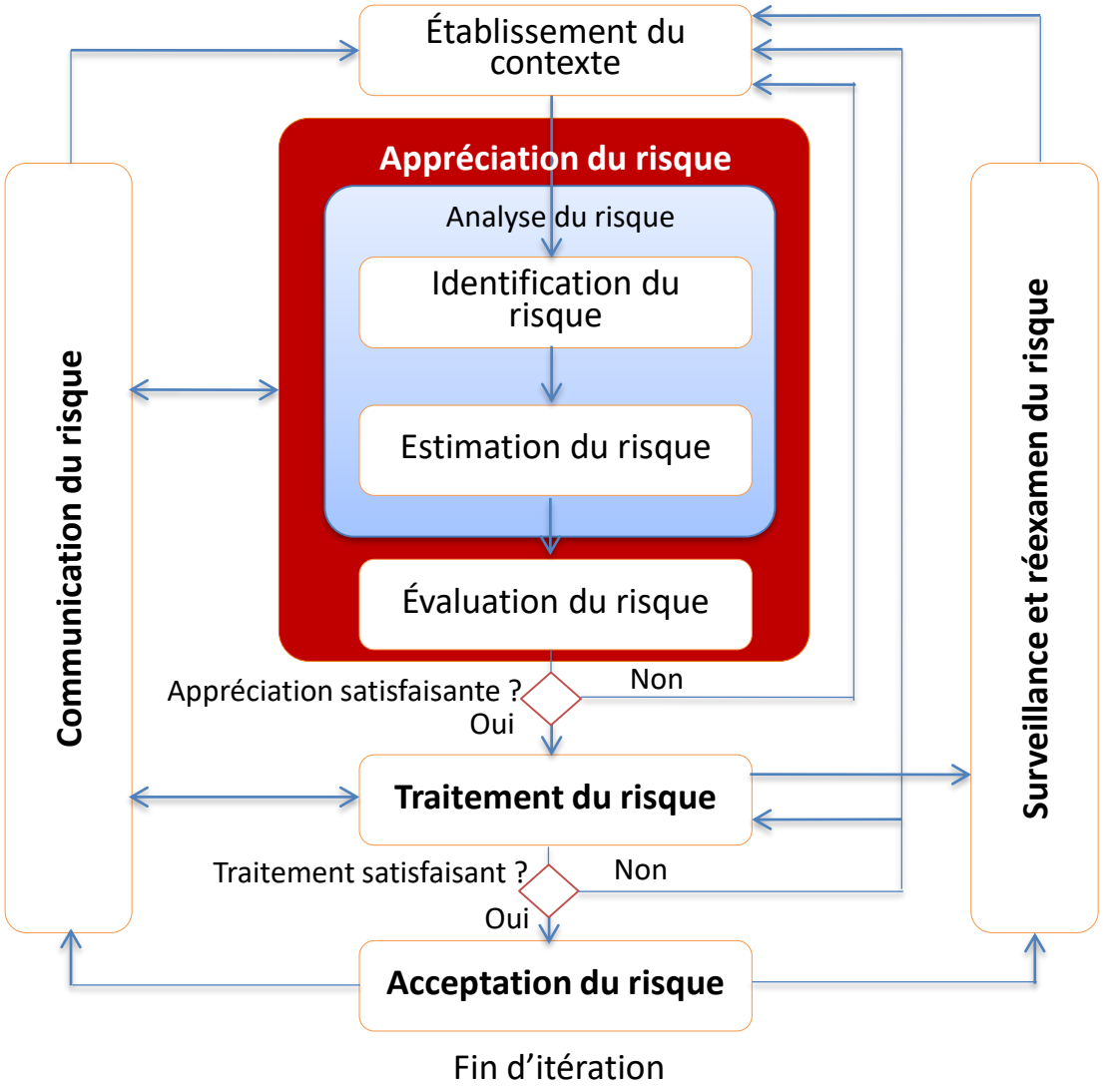
- **Des critères d'acceptation des risques**

  Critères utilisés pour déterminer si un risque est acceptable ou non.

A noter : nous reviendrons en détail sur ces critères lors de la description des activités dans lesquels ils interviennent.

8

Appréciation du risque



8. Appréciation du risque

L'appréciation du risque est souvent réalisée en deux itérations (ou plus). :

- Une appréciation de haut niveau est d'abord effectuée afin d'identifier les risques potentiels majeurs qui justifient une appréciation supplémentaire.

- L'itération suivante peut impliquer une étude détaillée des risques potentiels majeurs mis en lumière par l'itération initiale.

  Lorsque cette démarche ne fournit pas suffisamment d'informations pour apprécier le risque, d'autres analyses détaillées peuvent être réalisées, probablement sur des sous-ensembles du domaine d'application et, éventuellement, à l'aide d'une méthode différente.

8. Appréciation du risque

- 8.2: Analyse du risque (Risk Analysis)
  - 8.2.1: Identification du risque
  - 8.2.2: Estimation du risque
- 8.3: Evaluation du risque

8. Appréciation du risque

8.2. Analyse du risque

8.2.1. Identification du risque en 5 phases

- Phase 1 : Identification des actifs
- Phase 2 : Identification des menaces
- Phase 3 : Identification des mesures existantes
- Phase 4 : Identification des vulnérabilités
- Phase 5 : Identification des conséquences

8. Appréciation du risque

8.2. Analyse du risque

8.2.1.2 Identification des actifs

- Identification et évaluation des actifs du périmètre.
- Identification des propriétaires ou des responsables de ces actifs.

ISO/IEC 27005 :2008 (8.2.1.1 + Annexe B)

- Selon l'annexe B, on identifie 2 types d'actifs:
  - Actifs primordiaux :
    - Processus et activités métier
    - Informations
  - Actifs en support (exemple):
    - Matériels: PC, imprimante, climatiseur.
    - Logiciels: système d'exploitation, progiciel...
    - Réseau : LAN, WAN, VPN,…
    - Site : bâtiments, locaux,…
    - Personnel : salarié, intervenants externes, clients...
    - Structure de l'organisme…
    - Services: communications, énergie.
    - …

8. Appréciation du risque

8.2. Analyse du risque

Valorisation des actifs

La valorisation peut être effectuée à l'aide de deux mesures :

- la valeur de remplacement de l'actif : le coût de retour à une situation normale et de remplacement des informations (dans la mesure du possible),

- les conséquences sur l'activité métier d'une perte ou d'une compromission de l'actif, tels que les potentielles conséquences négatives sur l'activité et/ou les conséquences légales ou réglementaires dues à la diffusion, la modification, la non disponibilité et/ou la destruction d'informations et d'autres actifs informationnels.

Cette évaluation peut être déterminée par une analyse d'impact sur l'activité métier. La valeur, déterminée par la conséquence sur l'activité, est souvent nettement supérieure au simple coût de remplacement, en fonction de l'importance que joue l'actif dans l'accomplissement des objectifs métiers de l'organisme.

8. Appréciation du risque

8.2. Analyse du risque

8.2.1.3 Identification des menaces

- Éléments d'entrée: Informations relatives aux menaces obtenues grâce au réexamen des incidents, aux propriétaires des actifs, aux utilisateurs et à d'autres sources, y compris des catalogues de menaces externes.

- Action: Identifier les menaces et leurs sources. (ISO/IEC 27001 4.2.1.d.2)

- Élément de sortie: une liste des menaces avec l'identification de leur type et de la source.

8. Appréciation du risque

8.2. Analyse du risque

8.2.1.3 Identification des menaces

- Préconisations de mise en oeuvre:
  - Informations recueillies auprès :
    - des propriétaires ou des utilisateurs d'actifs,
    - des ressources humaines et du service juridique,
    - de spécialistes en infogérance et en sécurité de l'information,
    - d'experts en sécurité physique,
    - d'assurance, de service météorologique,
    - d'autorités nationales gouvernementales.
  - S'appuyer sur :
    - des catalogues de menaces génériques ou spécifiques aux métiers,
    - des évènements en internes : incidents de sécurité, étude des risques précédentes.

8. Appréciation du risque

8.2. Analyse du risque

8.2.1.4 Identification des mesures existantes

- Éléments d'entrée: documentation relatives aux mesures et plans d'implémentation des traitements de risques.

- Action: Identifier les mesures existantes et prévues

- Élément de sortie: Une liste des mesures existantes et prévues, l'état relatif à leur mise en œuvre et à leur utilisation.

8. Appréciation du risque

8.2. Analyse du risque

8.2.1.4 Identification des mesures existantes

- Préconisations de mise en œuvre :
  - Considérer les mesures de sécurité prévues pour déploiement de la même manière que les mesures de sécurité déjà mises en œuvre.
  - Une mesure de sécurité existante ou prévue peut être identifiée comme étant inefficace. Si elle s'avère injustifiée ou insuffisante, il convient de contrôler la mesure de sécurité afin de déterminer s'il convient de la retirer, de la remplacer par une autre mesure de sécurité plus adaptée, ou s'il convient de la laisser en place, par exemple pour des raisons de coûts.

8. Appréciation du risque

8.2. Analyse du risque

8.2.1.4 Identification des mesures existantes

- Préconisations de mise en œuvre :

  Les activités suivantes peuvent s'avérer utiles pour l'identification des mesures de sécurité existantes ou prévues :

  - Réexamen des documents contenant des informations relatives aux mesures de sécurité (ex : plan de traitement des risques),
  - Vérification avec les Responsables de la sécurité de l'information et avec les utilisateurs,
  - Revue sur site des mesures de sécurité physiques, en comparant les mesures mises en œuvre avec celles à déployer, et en vérifiant si elles sont opérationnelles et efficaces,
  - Examen des résultats des audits internes.

8. Appréciation du risque

8.2. Analyse du risque

8.2.1.4 Identification des mesures existantes

- [EBIOS] Catégories de mesures :
  - **Mesures préventives** : destinées à éviter l'apparition des incidents et des sinistres à l'aide de mesures de sécurité qui agissent sur :
    - Les sources de menaces (dissuasion, déception,…)
    - Les besoins de sécurité des actifs primordiaux (anticipation, prévention,…)
    - Les vulnérabilités des actifs supports (Réduction des failles, préparation,…)

8. Appréciation du risque

8.2. Analyse du risque

8.2.1.4 Identification des mesures existantes

- [EBIOS] Catégories de mesures :
  - **Mesures protectices** : destinées à bloquer, contenir et détecter l'apparition des incidents et des sinistres à l'aide de mesures de sécurité qui agissent sur :
    - Les besoins de sécurité des actifs primodiaux (confinement,…)
    - Les sources de menaces (lutte,…)
    - Les menaces (détection, protection, réaction offensive,…)
    - Les vulnérabilités des actifs supports (résistance, résilience,…)

8. Appréciation du risque

8.2. Analyse du risque

8.2.4 Identification des mesures existantes

- [EBIOS] Catégories de mesures :
  - **Mesures récupératrices** : destinées à minimiser les conséquences des incidents et des sinistres et revenir à l'état initial, à l'aide de mesures de sécurité qui agissent sur :
    - Les besoins de sécurité des actifs essentiels (récupération, restauration,…)
    - Les sources de menaces (réaction offensive,…)
    - Les impacts (compensation,…)
    - Les vulnérabilités des actifs supports (résistance, résilience,…)

8. Appréciation du risque

8.2. Analyse du risque

8.2.1.5 Identification des vulnérabilités

- Rappel : Qu'est ce qu'une vulnérabilité ?

Les vulnérabilités sont les éléments pouvant être exploités par les menaces pour nuire aux actifs ou à l'organisme.

[MEHARI] - deux types de vulnérabilités :

- Vulnérabilité intrinsèque : caractéristique intrinsèque d'un actif constituant un point d'application potentiel de menaces. *Exemples : Equipement ancien ou abimé, capacité de traitement ou de mémoire insuffisante, etc.*

- Vulnérabilité contextuelle : Défaut ou faille dans les dispositifs de sécurité pouvant être exploité par une menace pour atteindre un actif. *Exemples : Manque de maintenance, de surveillance, de respect des consignes de sécurité, etc.*

8. Appréciation du risque

8.2. Analyse du risque

8.2.1.5 Identification des vulnérabilités

- Éléments d'entrée: Liste des menaces connues, listes des actifs et des mesures de contrôle existantes.

- Action: Identifier les vulnérabilités susceptibles d'être exploitées par des menaces pour nuire aux actifs ou à l'organisme.

- Élément de sortie: Une liste des vulnérabilités liées aux actifs, aux menaces et aux mesures de sécurité. Une liste des vulnérabilités qui ne sont pas liées à une menace identifiée pour réexamen.

8. Appréciation du risque

8.2. Analyse du risque

8.2.1.5 Identification des vulnérabilités

- Préconisations de mise en œuvre: Les vulnérabilités peuvent être identifiées dans :
  - l'organisme,
  - les processus et procédures,
  - les activités récurrentes de gestion,
  - le personnel,
  - l'environnement physique,
  - la configuration du système d'information,
  - les matériels, logiciels ou infrastructures de communication,
  - la dépendance aux parties externes.

Des exemples de vulnérabilités sont fournis dans l'annexe D de la norme ISO 27005.

8. Appréciation du risque

8.2. Analyse du risque

8.2.1.6 Identification des conséquences

- Éléments d'entrée: Liste des actifs, liste des processus métiers et liste des menaces et des vulnérabilités , le cas échéant, liés aux actifs et leur pertinence.

- Action: Identifier les conséquences que des pertes de confidentialité, d'intégrité et de disponibilité peuvent avoir sur les actifs. *(ISO/IEC 27001 : 2005: 4.2.1.d.4)*

- Élément de sortie: Liste des scénarii d'incident et de leurs conséquences liées aux actifs et aux processus métier.

Des détails sont fournis dans l'annexe B2, notamment sur les aspects d'évaluation des actifs.

8. Appréciation du risque

8.2. Analyse du risque

8.2.1.6 Identification des conséquences

- Préconisations de mise en œuvre:

Les actifs peuvent se voir attribuer des valeurs, à la fois, selon leur coût financier et selon les conséquences sur l'activité métier s'ils sont endommagés ou compromis.

Les conséquences des scénarii d'incident doivent être déterminées en tenant compte des critères d'impact

8. Appréciation du risque

8.2. Analyse du risque

8.2.1.6 Identification des conséquences

- Préconisations de mise en œuvre:

Identifier les conséquences opérationnelles des scénarii d'incident en termes de :

- temps d'investigation et de réparation,
- temps (de travail) perdu,
- perte d'opportunités,
- santé et sûreté,
- coût financier des compétences spécifiques nécessaires pour réparer les dommages,
- image et valorisation financière de l'entreprise.

8.2.2 Estimation du risque

- 8.2.2.1 Méthodologies d'estimation du risque
- 8.2.2.2 Evaluation des conséquences
- 8.2.2.3 Evaluation des probabilités d'incident
- 8.2.2.4 Estimation du niveau de risque

8. Appréciation du risque

8.2. Analyse du risque

8.2.2.2 Appréciation des conséquences

- Éléments d'entrée: Liste de scénarii d'incident pertinents identifiés, incluant l'identification des menaces, vulnérabilités, actifs altérés, conséquences pour les actifs et les processus métier.

- Action: Apprécier l'impact sur l'activité de l'organisme pouvant résulter d'incidents de sécurité de l'information potentiels ou avérés, en tenant compte des conséquences d'une atteinte à la sécurité de l'information telle qu'une perte de confidentialité, d'intégrité ou de disponibilité des actifs

- Élément de sortie: Liste des conséquences d'un scénario d'incident appréciées et exprimées en cohérence avec les actifs et les critères d'impact.

□ Critères d'impact (Cf. 7.2)

Il convient d'élaborer une échelle afin d'évaluer les dommages ou les coûts pour l'organisme pouvant être causés par un risque, en tenant compte des points suivants :

- le niveau de classification de l'actif informationnel impacté,
- l'atteinte à la sécurité de l'information (par exemple, une perte de confidentialité, d'intégrité et de disponibilité),
- les erreurs opérationnelles (équipes internes ou tierces parties),
- la perte d'activité métier et de valeur financière,
- la perturbation des plans d'actions et des délais,
- les atteintes à la réputation,
- le non respect des exigences légales, réglementaires ou contractuelles.

Les critères d'impacts doivent être définies lors de l'établissement du contexte.

8. Appréciation du risque

8.2. Analyse du risque

Critères d'impact (Cf. 7.2)

Rappel de l'exemple d'échelle permettant d'évaluer l'impact d'un risque sur l'organisme

Critères d'impacts				
Impacts	Valeur D I C	Processus impactés	Niveaux impact sur actif	IMPACT
• Perte CA minime (< 50 K€) • Pas de perte d'image de marque • Conditions légales et réglementaires respectées	1	1	0,5	0,5
			1	1
		+2	0,5	1
			1	2
• Perte CA important (50K€ < Perte < 100K€) • Pas de perte d'image « moindre » (Clients isolés) • Conditions légales et réglementaires respectées	2	1	0,5	1
			1	2
		+2	0,5	2
			1	4
• Perte CA critique (> 100 K€) • Perte d'image critique (Tous les Clients, public) • Conditions légales et réglementaires non respectées	3	1	1	3
			0,5	1,5
		+2	1	6
			0,5	3

8. Appréciation du risque

8.2. Analyse du risque

Exemple d'échelles permettant d'apprécier la vraisemblance d'un scénario

Vraisemblance de la menace	Valeur
Susceptible de survenir chaque année ou plus de 25% de chance de survenir	3
Susceptible de survenir dans les dix prochaines années ou moins de 25% de chance de survenir	2
Peu susceptible de survenir dans les dix prochaines années ou moins de 2% de chance de survenir	1

Facilité d'exploitation	Valeur
Faisable sans expertise | Moyens facilement disponible dans les commerces |Fortes vulnérabilités	3
Faisable par une équipe | Moyens de type universitaire ou de recherche | Vulnérabilité moyenne	2
Besoin d'expertise | Gros moyens nécessaires | Vulnérabilité très faible	1

Evaluation de la couverture des Mesures de sécurité existantes	Valeur
Peu ou pas de mesures existantes ou Mesures existantes mais peu ou pas efficaces	0
Couverture partielle du niveau de la menace ou de facilité d'exploitation de la vulnérabilité	1 à 8
Mesures existantes et efficaces	9

8. Appréciation du risque

8.2. Analyse du risque

8.2.2.4 Estimation du niveau de risque

- Éléments d'entrée:

  Une liste des scénarii d'incident accompagnés de leurs conséquences liées aux actifs et aux processus métier, ainsi que leur vraisemblance.

- Action:

  Estimer le niveau de risque de tous les scénarii d'incidents pertinents.

  Il s'agit d'attribuer des valeurs à la vraisemblance et aux conséquences d'un risque.

- Élément de sortie:

  Une liste des risques avec un niveau de risque valorisé.

8. Appréciation du risque

8.2. Analyse du risque

8.2.2.4 Estimation du niveau de risque

Exemples de matrices utilisées pour l'estimation du niveau de risque

Exemple 1 :

	Vraisemblance Menace	**Faible**			**Moyenne**			**Elevée**		
	Facilité d'exploitation	F	M	E	F	M	E	F	M	E
Valeur de l'actif	0	0	1	2	1	2	3	2	3	4
	1	1	2	3	2	3	4	3	4	5
	2	2	3	4	3	4	5	4	5	6
	3	3	4	5	4	5	6	5	6	7
	4	4	5	6	5	6	7	6	7	8

8. Appréciation du risque

8.2. Analyse du risque

8.2.2.4 Estimation du niveau de risque

Exemples de matrices utilisées pour l'estimation du niveau de risque

Exemple 2 :

	Vraisemblance d'un scénario d'incident	Très faible (Très peu probable)	Faible (Peu probable)	Moyenne (Possible)	Elevée (Probable)	Très élevé (Fréquente)
Impact sur l'activité	Très faible	0	1	2	3	4
	Faible	1	2	3	4	5
	Moyen	2	3	4	5	6
	Elevé	3	4	5	6	7
	Très élevé	4	5	6	7	8

8. Appréciation du risque

8.2. Analyse du risque

8.2.2.4 Estimation du niveau de risque

Exemple : 3

Etude des Risques Disponibilité																	
Actifs				Menaces		Vulnérabilités		Mesures existantes			Conséquences			Estimation du risque			
ACTIF	Type d'actif	Valeur de l'actif	Criticité actif pour l'activité (support de processus critique ou plus de 2 processus impacté)	MENACES	Niveau de la menace	VULNÉRABILITÉS	Facilité d'exploit ou niveau vulnérabilité	Mesures préventives & Protectrices	Niveau de Couverture des mesures (1 à 9)	Vraisemblance finale	CONSÉQUENCES	Niveau Atteinte de l'actif 1 = Totale 0,5 = Partielle	IMPACT	Risque Brut	Mesures Récupératrices	Niveau de Couverture des mesures (1 à 6)	Risque Net
Disque stockage Developpement (sources)	MAT	3	2	Panne	3	Pas de surveillance du fonctionnement du disque	3	Règles d'échange des disques ts les 3 ans	3	6	Panne disque et perte des données sources	1	6	7	Disque en spare et procédure d'échange	2	4
		A	B		C		D		E	VF =C*D)-E		F	I = A*B*F	RB = (VF*I)/5,5		G	RN = ((I - G)*VF)/5,

8. Appréciation du risque

8.3. Evaluation du risque

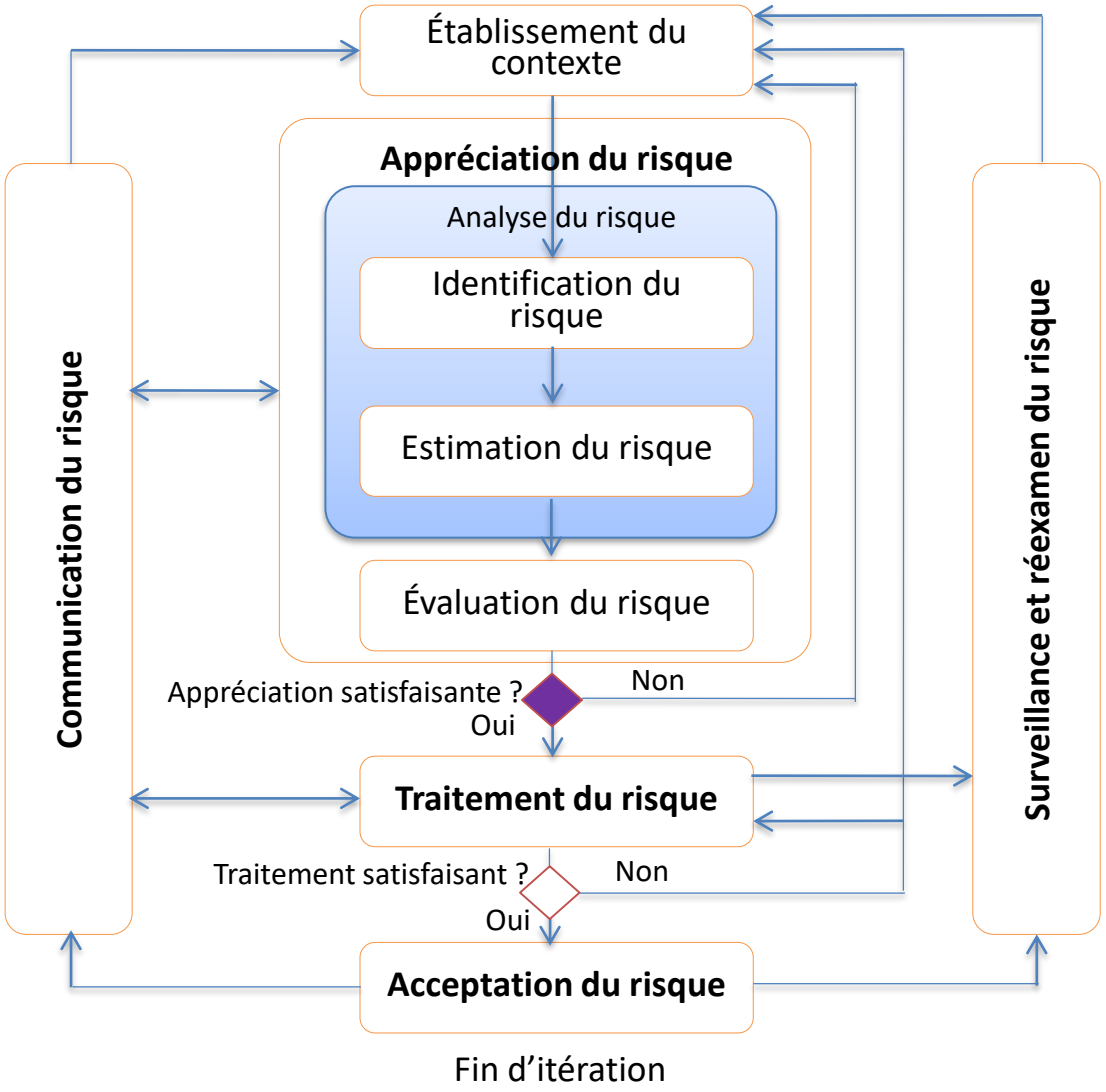
□ Critères d'évaluation

Rappel : Exemples de critères d'évaluation

Critères d'évaluation Basés sur les critères d'estimation et/ou d'autres critères si souhaités	Niveau de risque estimé	Risques évalués
- Risque avec des impacts insignifiants et une vraisemblance faible - Risque avec des impacts insignifiants et une vraisemblance moyenne - Risque avec des impacts importants et une vraisemblance faible	1 à 2	Insignifiants
- Risque avec des impacts insignifiants et une vraisemblance élevée - Risque avec des impacts importants et une vraisemblance moyenne	3 à 4	Mineurs
- Risque avec des impacts importants et une vraisemblance élevée - Risque avec des impacts vitaux et une vraisemblance faible	5 à 6	Graves
- Risque avec des impacts vitaux et une vraisemblance moyenne - Risque avec des impacts vitaux et une vraisemblance Elevée	7 à 10	Majeurs (prioritaire)

8-9

Point de Décision N°1



8. Appréciation du risque

Point de décision avant le traitement des risques

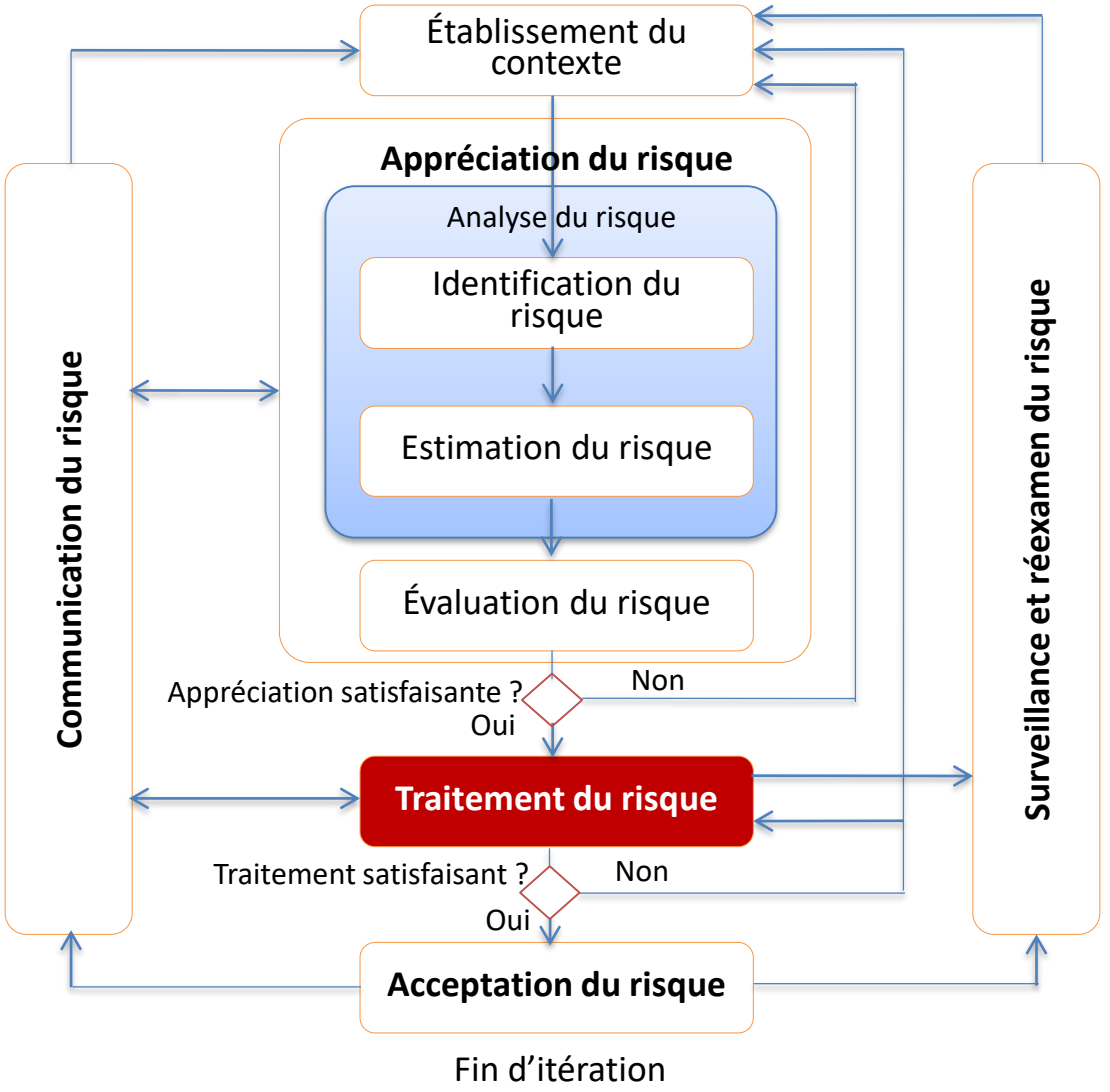
- L'appréciation des risques est elle satisfaisante ?

OUI = l'appréciation donne suffisamment d'informations pour déterminer correctement les actions nécessaires pour ramener les risques à un niveau acceptable, la tâche est alors terminée et suivie par le traitement du risque.

NON = Si les informations ne sont pas suffisantes, une autre itération de l'appréciation du risque sera réalisée avec un contexte révisé (par exemple les critères d'évaluation du risque, les critères d'acceptation du risque ou les critères d'impact) et, éventuellement, sur des parties limitées de l'ensemble du domaine d'application.

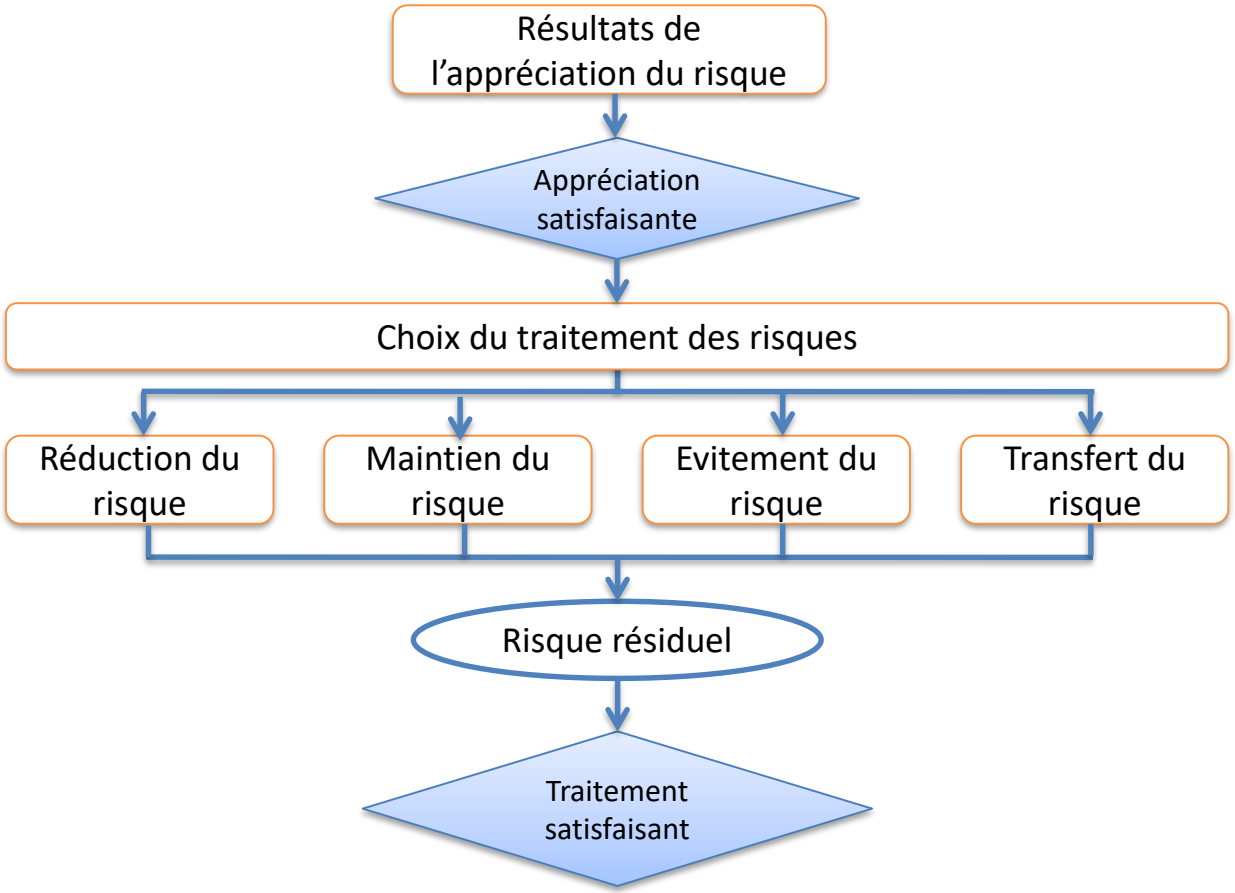
9

Traitement du risque



9. Traitement du risque

9.1. Description générale



9. Traitement du risque

9.1. Description générale

- Le plan de traitement du risque doit définir :
  - Les options de traitement du risque,
  - Les bénéfices attendus de ces options de traitement,
  - Le coût prévu de mise en œuvre des mesures,
  - Les priorités,
  - Les délais ,
  - Les risques résiduels.

9. Traitement du risque

9.1. Description générale

- Options de traitement du risque
  - Réduction du risque
  - Maintien du risque
  - Evitement du risque
  - Transfert du risque

9. Traitement du risque

Options de traitement du risque

9.2. Réduction du risque

Réduire le niveau de risque par la sélection des mesures de sécurité afin que le risque résiduel puisse être apprécié et jugé acceptable.

- Préconisation de mise en œuvre
  - Tenir compte :
    - des critères d'acceptation,
    - des exigences légales, réglementaires et contractuelles,
    - Des coûts et délais de mise en œuvre des mesures de sécurité,
    - Des aspects techniques, environnementaux et culturels.

9. Traitement du risque

Options de traitement du risque

9.2 Réduction du risque

En général, les mesures de sécurité peuvent fournir un ou plusieurs types de protection :

- *la correction,*
- *l'élimination,*
- *la prévention,*
- *l'atténuation des impacts,*
- *la dissuasion,*
- *la détection,*
- *la récupération,*
- *la surveillance,*
- *la sensibilisation.*

9. Traitement du risque

Options de traitement du risque

9.2 Réduction du risque

[EBIOS] Rappel 8.2.1.4 : Généralement, il est recommandé de mettre en place trois lignes de défense selon la gravité des risques et la capacité des sources de menaces :

- Des actions préventives ;
- Des actions protectrices ;
- Des actions récupératrices.

Chaque ligne de défense peut ensuite être renforcée en déterminant plusieurs mesures de sécurité sur un ou plusieurs bien support (un matériel, un logiciel, des locaux, une organisation…).

Un ensemble de mesures de soutien (alerte, diffusion, corrélation d'événements, protection des mesures de sécurité, réaction…) devrait compléter le dispositif de défense en profondeur.

9. Traitement du risque

Options de traitement du risque

9.2 Réduction du risque

Contraintes lors du choix des mesures de sécurité et de leur mise en œuvre :

- Contraintes de temps : ex. *Délai de mise en œuvre acceptable pour les dirigeants*
- Contraintes financières : ex. *Ne pas dépasser un budget alloué*
- Contraintes techniques : ex. *Compatibilité des programmes ou du matériel*
- Contraintes opérationnelles : ex. *Nécessité de fonctionner 24h/24, 7j/7 pour des sauvegardes*
- Contraintes culturelles : ex. *Fouilles de sacs impossible dans certaines parties du Moyen Orient*
- Contraintes éthiques : ex. *Analyse des courriers électroniques*
- Contraintes environnementales : ex. *Conditions climatiques, seisme,*
- Contraintes légales : ex. *Protection des données personnelles,*
- Facilité d'utilisation : ex. *Mauvaise interface homme machines entrainant erreur et inutilisation*
- Contraintes liées au personnel : ex. *Disponibilité et coût salarial des compétences*
- Contraintes liées à l'intégration de mesures de sécurité nouvelles et existantes : ex. *incompatibilité avec les mesures existante*
- **Détails en annexe F de la norme**

9. Traitement du risque

Options de traitement du risque

- 9.3. Maintien du risque

Action :

Prendre la décision de maintenir le risque sans autre action en fonction de l'évaluation du risque.

Préconisation de mise en œuvre

Si le niveau de risque répond aux critères d'acceptation du risque, il n'est pas nécessaire de mettre en œuvre d'autres mesures de sécurité, le risque peut alors être conservé.

9. Traitement du risque

Options de traitement du risque

9.4. Evitement du risque

Action :

Eviter l'activité ou la situation qui donne lieu à un risque particulier.

Préconisation de mise en œuvre

Lorsque les risques identifiés sont jugés trop élevés ou lorsque les coûts de mise en œuvre d'autres options de traitement du risque dépassent les bénéfices attendus, il est possible de prendre la décision d'éviter complètement le risque, en abandonnant une ou plusieurs activités prévues ou existantes, ou en modifiant les conditions dans lesquelles l'activité est effectuée

Exemples :

- *déplacer physiquement les moyens de traitement de l'information à un endroit où le risque n'existe pas ou est maitrisé.*
- *le fait de ne pas commencer ou poursuivre l'activité porteuse du risque,*
- *la séparation d'informations ayant des besoins de sécurité différents sur des bien supports isolés, etc.*

9. Traitement du risque

Options de traitement du risque

- 9.5. Transfert du risque

Action :

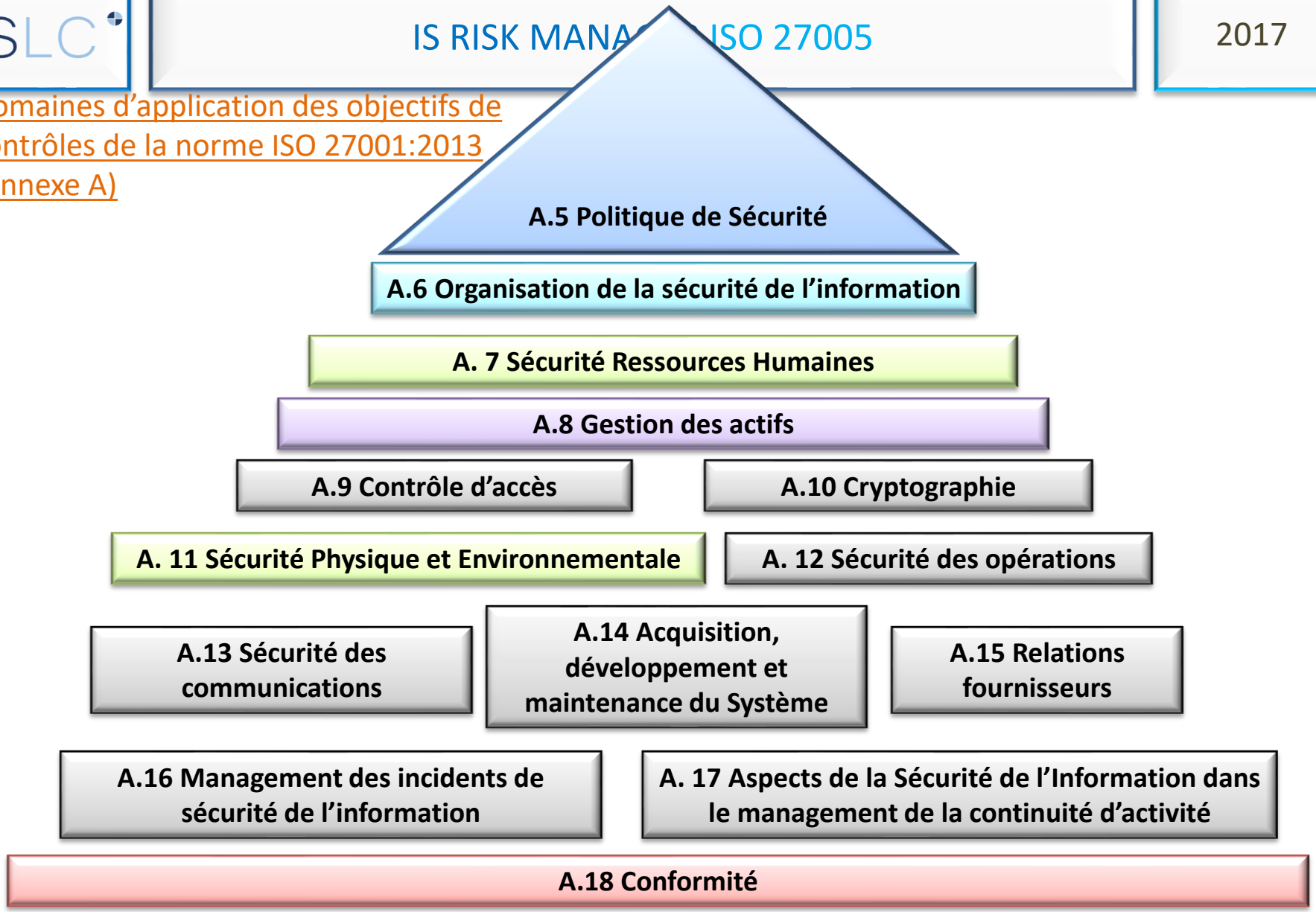
Transférer le risque à une autre partie capable de gérer de manière plus efficace le risque spécifique en fonction de l'évaluation du risque.

Préconisation de mise en œuvre

Partager certains risques avec des parties externes (partager les pertes occasionnées ou faire assumer la responsabilité à un tiers). Cela peut créer de nouveaux risques ou modifier les risques identifiés. Un autre traitement du risque peut s'avérer nécessaire.

Exemples : *Souscrire une assurance, financer le risque, utiliser des produits, des services ou des individus certifiés, contractualiser des clauses de transfert de responsabilité, etc.*

Domaines d'application des objectifs de contrôles de la norme ISO 27001:2013 (Annexe A)



9. Traitement du risque

Risques résiduels

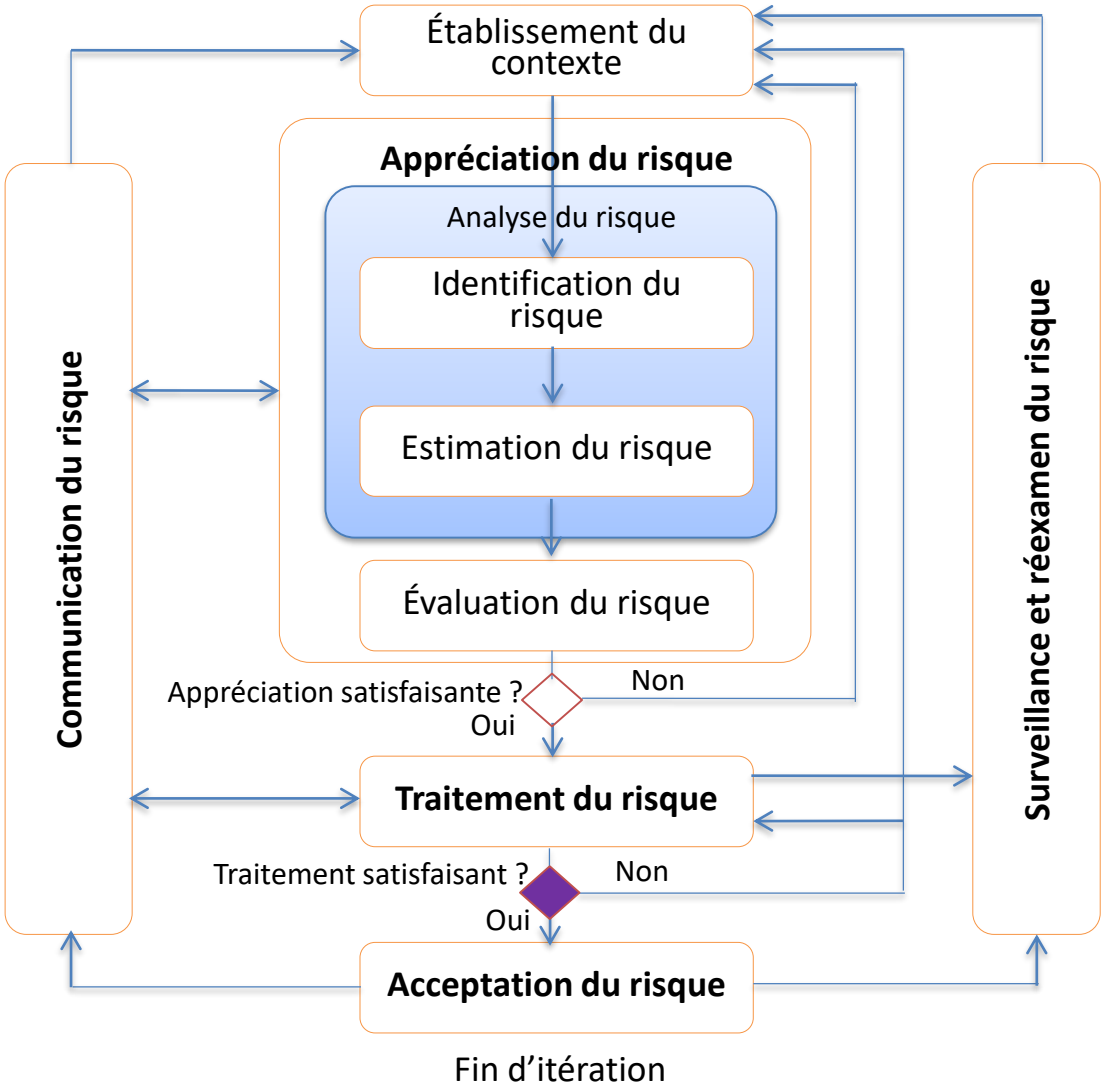
Action :

Déterminer les risques résiduels via la mise à jour ou la réitération de l'appréciation du risque, en tenant compte des effets pressentis du traitement de risque proposé.

Dans le cas où le risque résiduel ne remplirait toujours pas les critères d'acceptation du risque de l'organisme, une autre itération du traitement de risque peut s'avérer nécessaire avant de procéder à l'acceptation du risque.

9 - 10

Point de Décision N°2



9. Traitement du risque

Point de décision avant l'acceptation des risques

- Le Traitement des risques est il satisfaisant ?

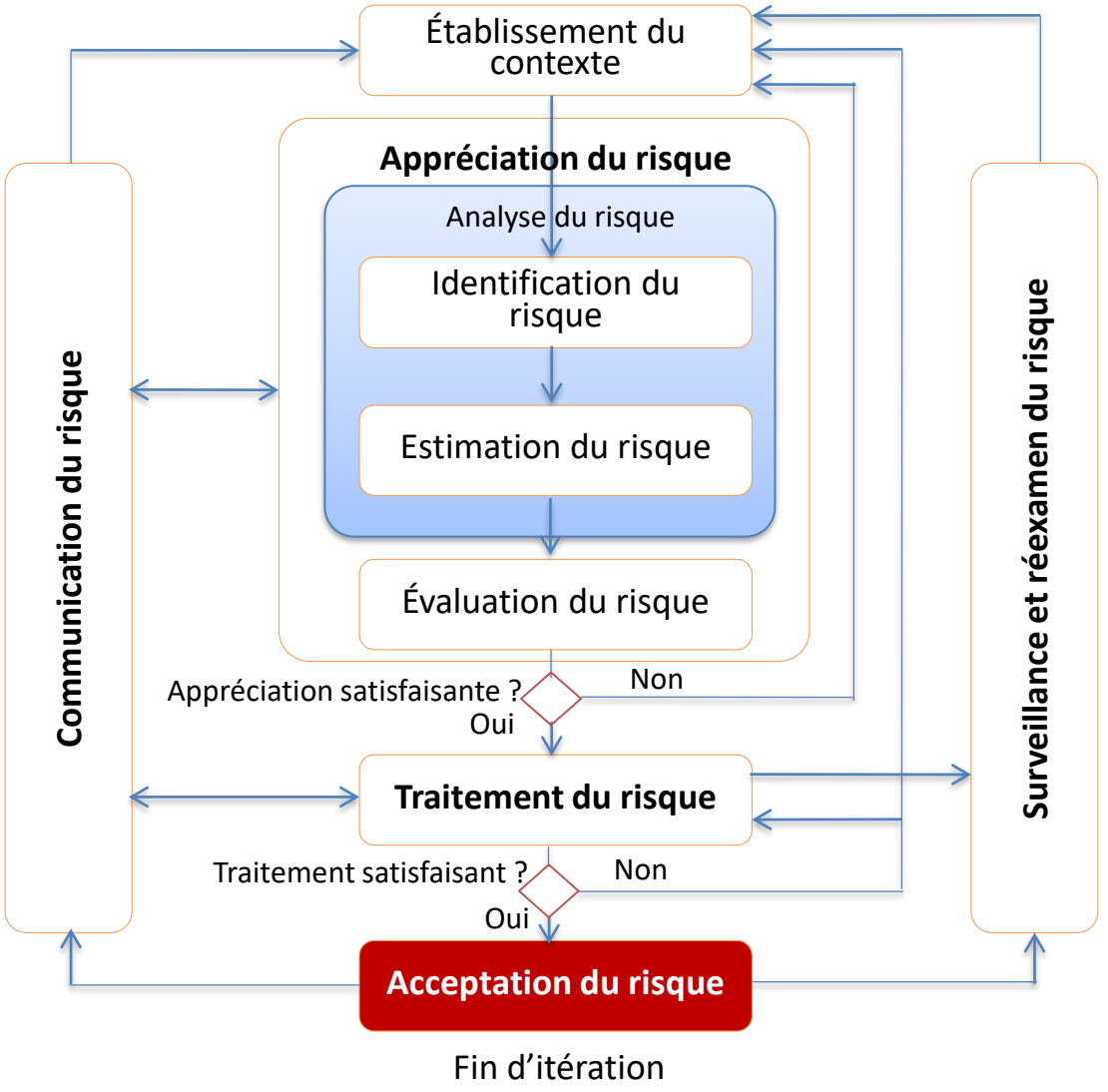
L'efficacité du traitement du risque dépend des résultats de l'appréciation du risque.

Si ne donne pas immédiatement un niveau acceptable de risque résiduel.

Dans ce cas, une nouvelle itération de l'appréciation du risque utilisant, si nécessaire, de nouveaux paramètres de contexte (à titre d'exemples : l'appréciation du risque, l'acceptation du risque ou les critères d'impact) peut être requise et suivie d'un autre traitement du risque.

10

Acceptation du risque



10. Acceptation des risques

- Éléments d'entrée:

  Plan de traitement du risque et appréciation du risque résiduel soumis à la décision d'acceptation des dirigeants de l'organisme.

- Action:

  Prendre la décision d'accepter les risques et les responsabilités de cette décision et de l'enregistrer formellement.

- Élément de sortie:

  Liste des risques acceptés et justification pour les risques ne remplissant pas les critères normaux d'acceptation du risque de l'organisme.

10. Acceptation des risques

- Préconisations de mise en œuvre :
  - Il est important que les dirigeants en charge :
    - réexaminent et approuvent les plans de traitement du risque et les risques résiduels associés
    - Enregistrent les conditions associées à l'approbation.

  - Si les décideurs ont à accepter des risques qui ne remplissent pas les critères normaux d'acceptation, il doivent commenter explicitement les risques et inclure une justification de la décision d'outrepasser ces critères.

10. Acceptation des risques

□ Critères d'acceptation

Les critères d'acceptation du risque peuvent :

- Inclure des **seuils multiples** correspondant à un niveau de risque cible souhaité, tout en réservant aux cadres décisionnaires la possibilité d'accepter des risques situés au-dessus de ce niveau dans certains cas,
- Etre exprimés comme un **rapport entre le profit estimé** (ou tout autre bénéfice métier) **et le risque estimé**,
- S'appliquer à différents types de risques, par exemple des risques susceptibles d'aboutir à une non-conformité ou à des réglementations peuvent ne pas être acceptés, tandis que l'acceptation de risques élevés peut être autorisée si cela est spécifié comme une exigence contractuelle,
- Il est possible d'accepter un risque s'il y a un engagement et une validation que des mesures destinées à le ramener à un niveau acceptable, dans un délai défini, vont être mises en œuvre.

10. Acceptation des risques

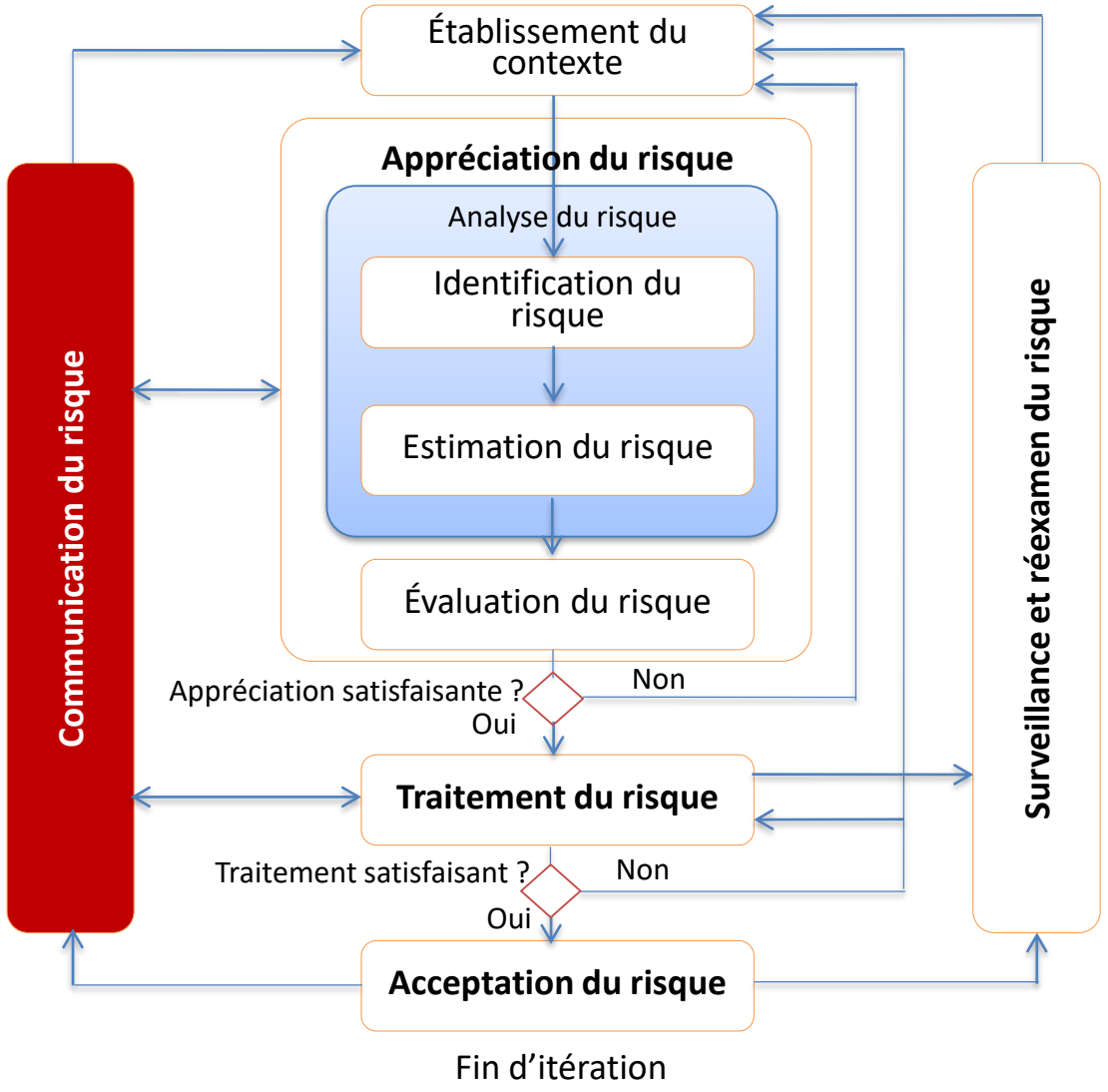
□ Critères d'acceptation

Exemple de critères d'acceptation

Niveau de Risque estimé	Risque évalué	Critères d'acceptation
1	insignifiant	**Risques jugés acceptables :** Ces risques peuvent être maintenu. *Certains risques peuvent être réduits, transférés ou évités si souhaités.*
2	Mineur	
3	Grave	**Risques jugés Non acceptables :** Ces risques doivent être réduits, transférés ou évités pour être ramenés à un niveau jugée acceptable. *Certains peuvent être acceptés sur justification.*
4	Majeur	

11

Communication du risque



11. Communication du risque en sécurité de l'information

- Éléments d'entrée:

  L'ensemble des informations, relatives au risque, obtenues grâce aux activités de gestion du risque.

- Action:

  Echanger et/ou partager les informations relatives au risque entre le décideur et les autres parties prenantes.

- Élément de sortie:

  Compréhension permanente du processus et des résultats de la gestion du risque en sécurité de l'information de l'organisme.

11. Communication du risque en sécurité de l'information

- Préconisation de mise en œuvre :
  - Garantir que les personnes responsables de la mise en œuvre de la gestion des risques et que les personnes ayant un intérêt direct comprennent les fondements sur lesquels les décisions sont prises et les raisons pour lesquelles les actions spécifiques sont nécessaires.

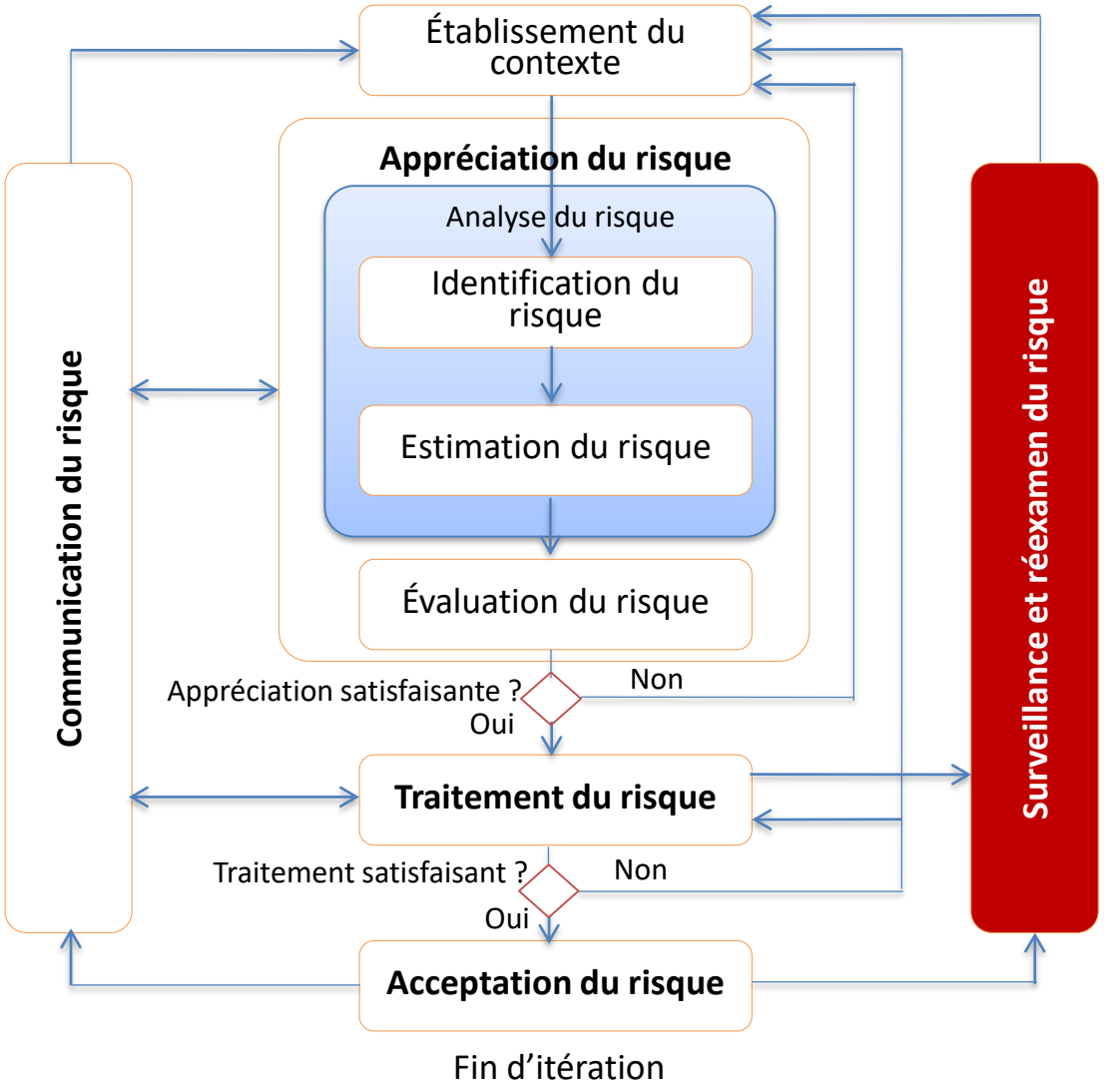
  - Les informations échangées peuvent porter sur :
    - l'existence,
    - la nature,
    - le type,
    - la vraisemblance,
    - la gravité,
    - le traitement
    - l'acceptabilité des risques.

11. Communication du risque en sécurité de l'information

- Objectifs:
  - garantir les résultats de la gestion de risque de l'organisme,
  - réunir les informations relatives au risque,
  - partager les résultats obtenus grâce à l'appréciation du risque et présenter le plan de traitement du risque,
  - éviter ou réduire à la fois l'occurrence et les conséquences des violations de sécurité de l'information dues à un manque de compréhension mutuelle entre les décideurs et les parties prenantes,
  - aider au processus de prise de décision,
  - obtenir de nouvelles connaissances en sécurité de l'information,
  - assurer une coordination avec d'autres parties et prévoir des réponses destinées à réduire les conséquences des incidents pouvant survenir,
  - responsabiliser les décideurs et les parties prenantes quant aux risques,
  - améliorer la sensibilisation à la sécurité de l'information.

12

Surveillance et réexamen



12. Surveillance et réexamen du risque

12.1 Surveillance et réexamen des facteurs de risque

- Éléments d'entrée:

  L'ensemble des informations, relatives au risque, obtenues grâce aux activités de gestion du risque.

- Action:

  Surveiller et réexaminer les risques et leurs facteurs (valeurs des actifs, impacts, menaces, vulnérabilités et vraisemblance) pour identifier au plus tôt toutes les modifications dans le contexte de l'organisme et pour maintenir une cartographie complète des risques.

- Élément de sortie:

  Alignement continu de la gestion du risque avec les objectifs métiers de l'organisme ainsi qu'avec les critères d'acceptation du risque.

12. Surveillance et réexamen du risque

12.1 Surveillance et réexamen des facteurs de risque

- Préconisations de mise en œuvre :

  Une surveillance constante pour détecter les changements pouvant être assurés par des services externes.

  Eléments à surveiller :

  - les **nouveaux actifs**,
  - les **modifications** des valeurs des actifs,
  - les **nouvelles menaces** qui n'ont pas été appréciées,
  - la possibilité que des **vulnérabilités nouvelles ou accrues** puissent permettre aux menaces de les Exploiter,
  - les **vulnérabilités** qui deviennent **exposées à des menaces nouvelles** ou qui réapparaissent,
  - l'**augmentation de l'impact** ou des **conséquences des menaces**, des vulnérabilités et des risques appréciés en agrégation entraînant un niveau de risque inacceptable,
  - les **incidents** liés à la sécurité de l'information.

12. Surveillance et réexamen du risque

12.2 Surveillance, réexamen et amélioration de la gestion du risque

- Éléments d'entrée:

  L'ensemble des informations, relatives au risque, obtenues grâce aux activités de gestion du risque.

- Action:

  Constamment surveiller, réexaminer et améliorer le processus de gestion du risque en sécurité de l'information et de manière appropriée.

- Élément de sortie:

  Pertinence permanente du processus de gestion du risque en sécurité de l'information avec les objectifs métiers de l'organisme ou mise à jour du processus.

12. Surveillance et réexamen du risque

12.2 Surveillance, réexamen et amélioration de la gestion du risque

- Préconisations de mise en œuvre :
  - Notifier aux dirigeants concernés les améliorations apportées au processus,
  - S'assurer que les ressources d'appréciation et de traitement du risque soient disponibiles,
  - Vérifier régulièrement la validité et la cohérence des critères utilisés avec les objectifs métiers, les stratégies et les politiques.

12. Surveillance et réexamen du risque

12.2 Surveillance, réexamen et amélioration de la gestion du risque

- Préconisations de mise en œuvre :

  Surveiller et réexamen les points suivants :

  - le contexte légal et environnemental,
  - le contexte concurrentiel,
  - l'approche liée à l'appréciation du risque,
  - la valeur et les catégories d'actifs,
  - les critères d'impact, d'évaluation du risque et d'acceptation du risque,
  - le coût total de maintenance,
  - les ressources nécessaires.

Méthodes connues

Présentation de méthodes de gestion des risques de sécurité de l'information

Méthode	Créé en	Auteur	Soutenu par	Pays	Outil	Site
CRAMM	1986	SIEMENS	Gouvernement	UK	Payant : CRAMM EXPERT ou CRAMM EXPRESS	www.cramm.com
EBIOS	1995	ANSSI	Gouvernement	FR	Libre mais 2005	www.ssi.gouv.fr
MEHARI	1997	CLUSIF	Association	FR	Libre	www.clusif.asso.fr
					Payant : RISICARE	www.risicare.fr
OCTAVE	1999	Université Carnegie Mellon	Universitaire	USA	Payant OCTAVE et OCTAVE-S	www.cert.org/octave

Méthodes connues - EBIOS

EBIOS : Expressions des Besoins et Identification des Objectifs de Sécurité

Description :

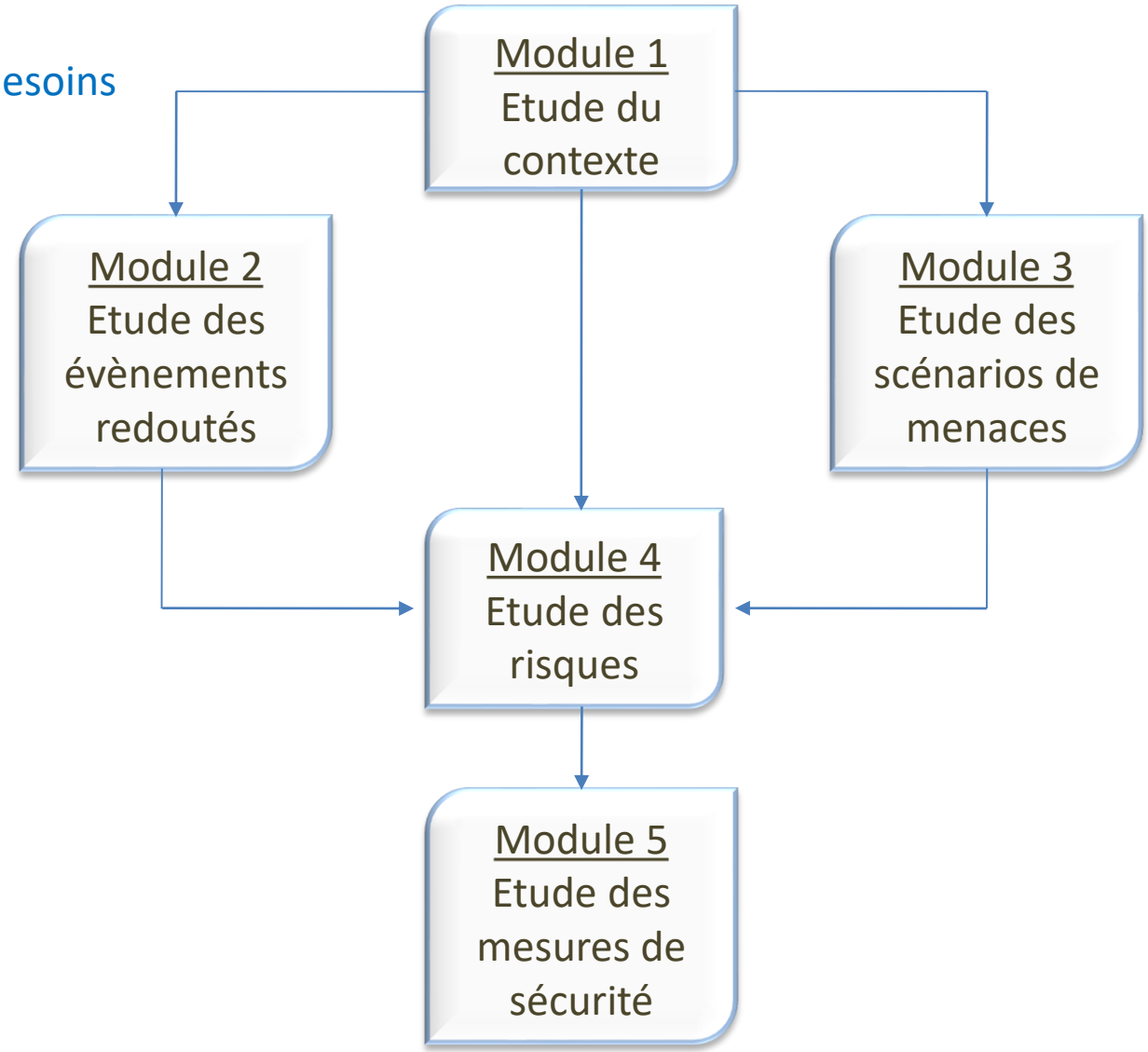
- Conçue pour permettre la rédaction de FEROS (Fiche d'Expression Rationnelle des Objectifs de Sécurité (des SI);

Méthodes connues - EBIOS

EBIOS : Expressions des Besoins

Et Identification des

Objectifs de Sécurité



Méthodes connues - EBIOS

ETUDE DU CONTEXTE	
Définition du cadre	Cadre de l'étude : but, livrables, structure de travail
	Description du contexte général (interne et externe)
	Description du périmètre de l'étude
	Identification des contraintes
	Identification des sources de menaces
Préparation des métriques	Définition des critères de sécurité et échelles de besoins (DIC)
	Elaboration d'une échelle de niveaux de gravité
	Elaboration d'une échelle de niveau de vraisemblance
	Définition des critères (estima., évalua., Ev. Redoutés + risques)
Identification des biens	Biens essentiels, leurs relations et dépositaires
	Biens supports, leurs relations et dépositaires
	Liens entre les biens essentiels et biens supports
	Identification des mesures de sécurité existantes biens supports

Méthodes connues - EBIOS

2 - ETUDE DES ÉVÉNEMENTS REDOUTÉS	
Evènement redoutés	Appréciation des évènements redoutés
3 - ETUDE DES MENACES	
Menaces	Appréciation des scénarios de menaces
	Evaluation de chaque menace
4 - ETUDE DES RISQUES	
Analyse des risques	Sélection des menaces liés aux évènements redoutés
	Identification des mesures existantes
	Estimation des niveaux de risques
	Evaluation des risques
Objectifs de sécurité	Choix des options de traitement des risques
	Analyse des risques résiduels si objectifs de sécurité atteint

Méthodes connues - EBIOS

5 - ETUDE DES MESURES DE SECURITE	
Formalisation	Détermination des mesures de sécurité
	Analyse des risques résiduels
	Etablissement de déclaration d'applicabilité (lien avec contexte)
Mise en œuvre	Elaboration des plan d'action et suivi de la réalisation
	Identification et estimation des risques résiduels
	Prononciation de l'homologation de sécurité

Méthodes connues - EBIOS

- Avantages :
  - Méthode éprouvée ;
  - Approche exhaustive : identification et combinaison des éléments constitutifs des risques
  - Méthode claire : étape bien définie avec les acteurs et actions attendues ;
  - Méthode que l'on peut adapter en fonction du périmètre (SI, application, service, processus, etc.) et de son contexte;
  - Outil et documentation (guide méthodologiques, base de connaissance,…) libres d'accès ;

- Inconvénients :
  - Ne constitue qu'un support à la réflexion et ne fournit pas de solutions immédiates aux problèmes de sécurité ;
  - Outil pour la version 2010 pas encore disponible ;

Méthodes connues - MEHARI

MEHARI : MEthode Harmonisée d'Analyse de RIsques

Phase préparatoire

- Prise en compte du contexte
- Cadrage
- Paramétrage

Phase opérationnelle D'analyse des risques

- Analyse des enjeux et classification
- Diagnostic des services de sécurité
- Analyse des risques

Phase de planification du traitement des risques

- Plan de mesures immédiates
- Plan de mesures planifiées
- Mise en place du pilotage

Méthodes connues - MEHARI

1 – PHASE PREPARATOIRE	
Prise en compte du contexte	Contexte stratégique
	Contexte technique
	Contexte organisationnel
Cadrage de la mission d'analyse et de traitement des risques	Périmètre technique
	Périmètre organisationnel
	Structure de pilotage de la mission
Fixation des principaux paramètres de l'analyse des risques	Grille d'acceptabilité des risques
	Grille des expositions naturelles
	Grille d'appréciation des risques

Méthodes connues - MEHARI

2 – PHASE OPERATIONNELLE D'ANALYSE DES RISQUES	
Analyse des enjeux et classification des actifs	Echelle de valeur des dysfonctionnements
	Classification des actifs
	Tableau d'impact intrinsèque
Diagnostic de la qualité des services de sécurité	Etablissement du schéma d'audit
	Diagnostic de la qualité des services de sécurité
Appréciation des risques	Sélection des scénarios de risques à analyser
	Estimation des scénarios de risques

Méthodes connues - MEHARI

3 – PHASE DE PLANIFICATION ET DE TRAITEMENT DES RISQUES	
La planification des actions immédiates	Sélection des risques à traiter en priorité absolue
	Choix des mesures à mettre en œuvre immédiatement
Planification des mesures à décider dans le cadre courant	Stratégie de traitement et priorités
	Choix des mesures de planification
Appréciation des risques	Sélection des scénarios de risques à analyser
	Estimation des scénarios de risques

Méthodes connues - MEHARI

- Avantages :
  - Méthode éprouvée et documentée ;
  - Approche orientée système d'information ;
  - Méthode claire et documentée ;
  - Fournit un guide d'audit du niveau de sécurité ;
  - Fournit des indicateurs de suivi et d'évolution ;
  - Documentation (guide méthodologiques, base de connaissance,…) libres d'accès ;

- Inconvénients :
  - Outil non libre d'accès ;
  - Lourdeur de la phase d'audit ;

Des questions ?

Merci pour votre attention.