-Cours-

Ingénierie et Management de la Sécurité des Système d'Information

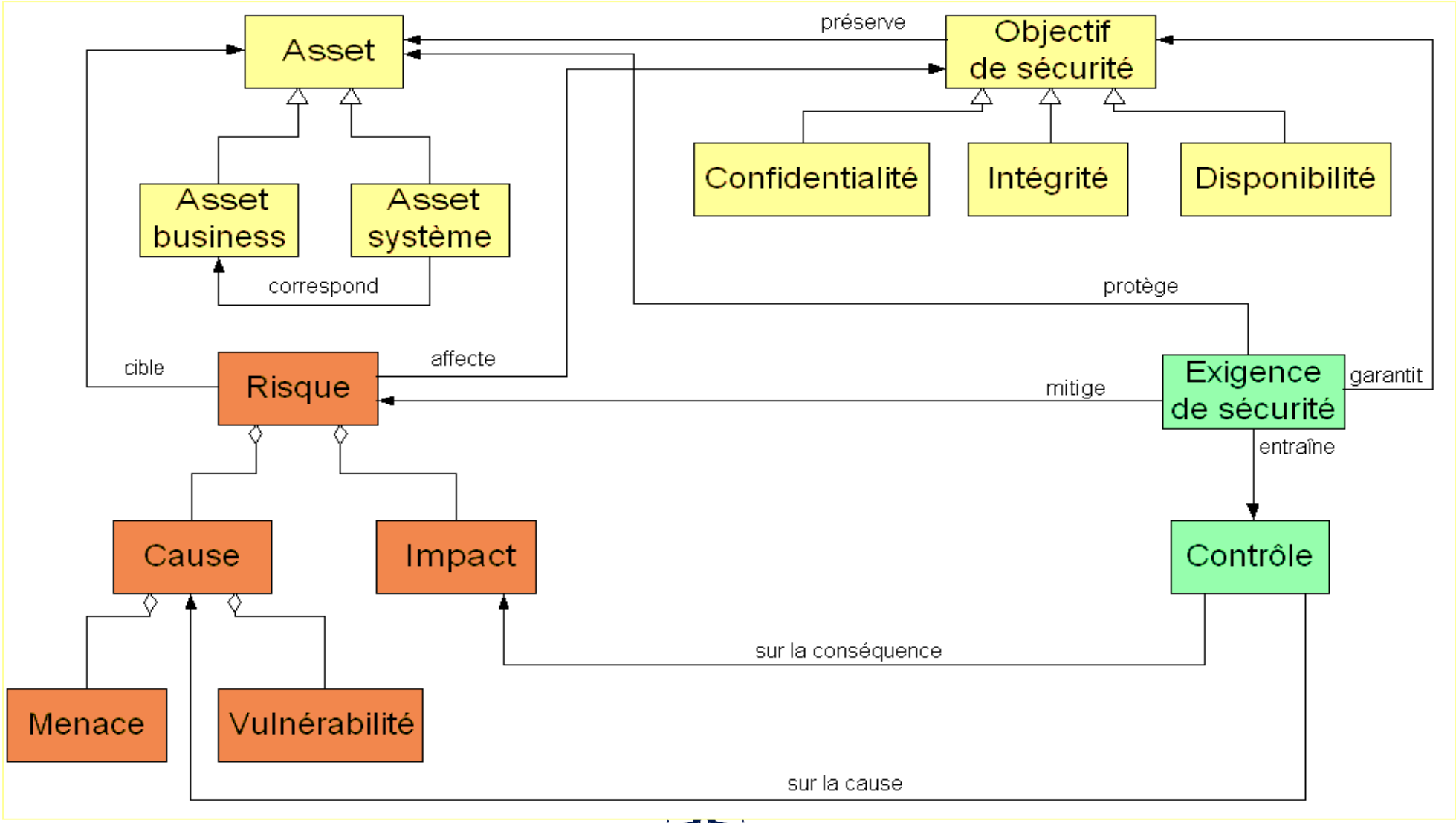
Dr. KHALDI Miloud

m.khaldi@esi-sba.dz

- Chapitre 3-

Management de la Sécurité des Systèmes d'Information

Concepts liés au management de la sécurité des SI



Concepts liés au management de la sécurité des SI

Assets

L'ensemble des **actifs**, **biens**, **ressources** ayant de la valeur pour l'organisme et nécessaires à **son bon fonctionnement**.

- **Assets business:** représentent les **informations** (données du client, numéros de cartes bancaires, …) et les **processus** (gestion des transactions, processus métier, …).
- **Assets système:** représentent les **éléments techniques** (matériels, logiciels, réseaux, …) mais aussi l'**environnement** du SI (bâtiments, locaux, …) .

Concepts liés au management de la sécurité des SI

Objectifs de sécurité

Le but du management de la sécurité des SI est d'**assurer la sécurité des assets**, exprimée la plupart du temps en termes de **confidentialité**, **intégrité** et **disponibilité**, constituant les objectifs de sécurité.

Concepts liés au management de la sécurité des SI

Risque

L'**ISO** définit un risque par la combinaison de la **probabilité** d'un événement et de ses **conséquences**.

La **potentialité** qu'une **menace** exploite la **vulnérabilités** d'un (plusieurs) **asset**(s) et cause ainsi des **désagréments** au SI.

- Se compose de 3 éléments :
  - Vulnérabilité
  - Menace
  - Impact

RISQUE = MENACE * VULNÉRABILITÉ * IMPACT

RISQUE = IMPACT (Conséquence) * VRAISEMBLENCE (Probabilité)

Concepts liés au management de la sécurité des SI

Risque

- **Menace**: la **source** du risque, est l'attaque possible d'un élément dangereux contre les **assets** (l'agent responsable du risque).
- **Vulnérabilité**: la **caractéristique** d'un **asset** constituant une faiblesse ou une faille au regard de la sécurité.
- **Impact**: représente la **conséquence** du risque sur l'**asset**.

⇨ La **menace** et la **vulnérabilité**, représentent la **cause** du risque.

Concepts liés au management de la sécurité des SI

Gestion des risques

Définie par l'**ISO** comme l'ensemble des **activités** coordonnées visant à **diriger** et **piloter** un organisme vis-à-vis du **risque**.

☞ **But:**

- Améliorer la sécurisation des SI,
- Justifier le budget alloué à la sécurisation du SI,
- Prouver la crédibilité du système d'information à l'aide des analyses effectuées.

Normes et méthodes de gestion des risques

Norme ISO/IEC 27005

Représente une **démarche générale** pour la **gestion des risques** de sécurité du SI.
Définit des lignes directrices relatives à la gestion des risques dans une organisation pour **intégrer la sécurité**.

Méthodes de gestion des risques

Plus de 200 méthodes de gestion des risques sont déclinées actuellement à travers le monde:

- **EBIOS** (Expression des Besoins et Identification des Objectifs de Sécurité) .
- **MEHARI** (Méthode Harmonisée d'Analyse de Risques).
- **OCTAVE** (Operationally Critical Threat, Asset, and Vulnerability Evaluation).
- Etc.

Processus de gestion des risques (ISO 27005)

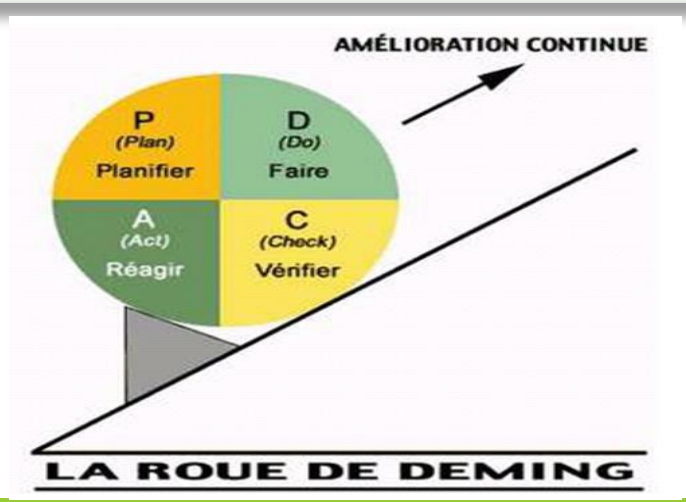
Méthode PDCA / Processus SMSI (ISO 27005)

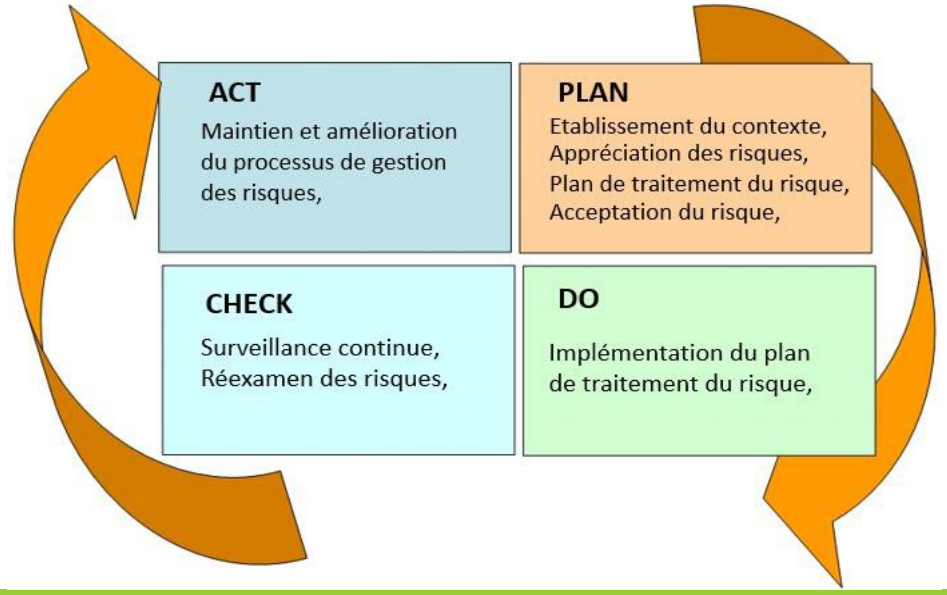
La norme **ISO 27005** utilise la logique d'amélioration continue **PDCA**:

- **P**lan ou planifier
- **D**o ou déployer
- **C**heck ou contrôler
- **A**ct ou agir

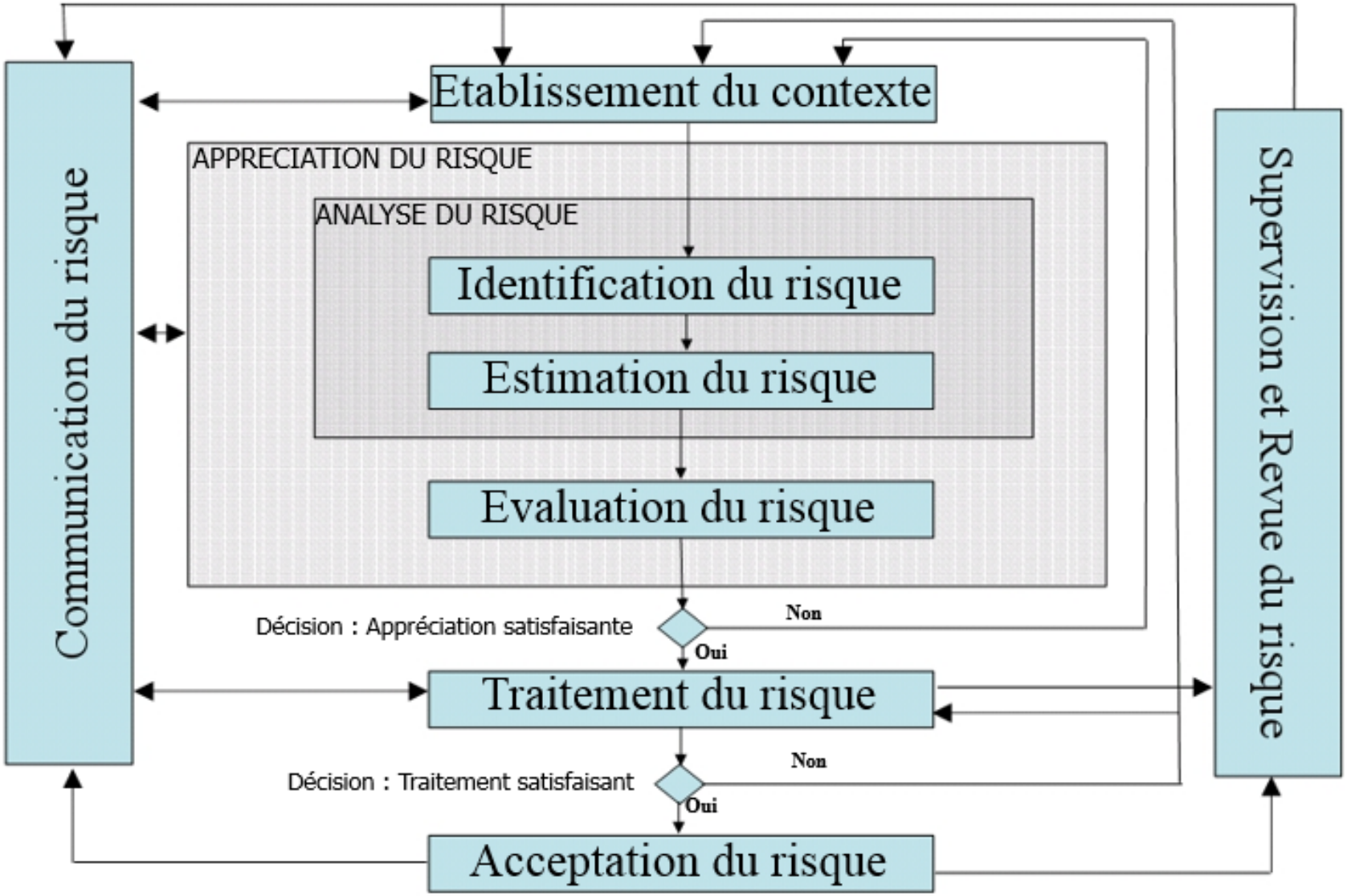
⇨ **PDCA** est utilisée pour améliorer la qualité dans une organisation (performance renforcée).

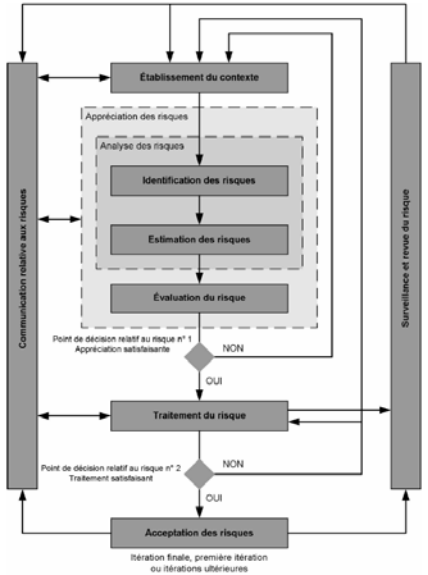
Processus SMSI	Processus de gestion des risques en sécurité de l'information
Planifier	Établissement du contexte Appréciation des risques Élaboration du plan de traitement des risques Acceptation des risques
Déployer	Mise en œuvre du plan de traitement des risques
Contrôler	Surveillance et revue continues des risques
Agir	Maintien et amélioration du processus de gestion des risques en sécurité de l'information





Processus de gestion des risques (ISO 27005)



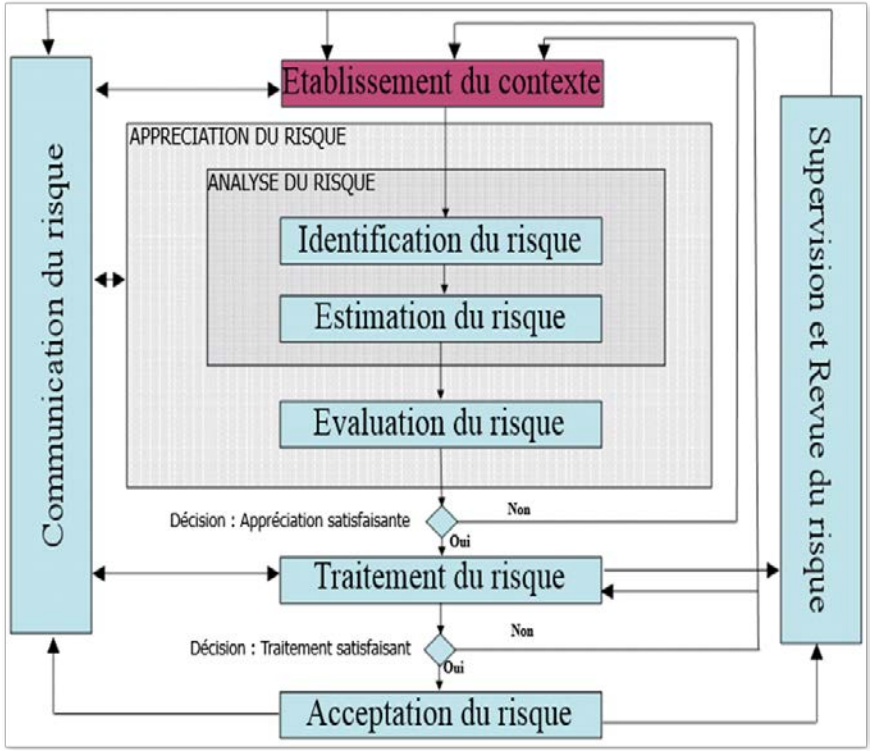


Processus de gestion des risques (ISO 27005)

1. Établissement du contexte

Liste des activités

1) Mission, valeurs et stratégies,
2) Compréhension de l'environnement externe,
3) Compréhension de l'environnement interne,
4) Identification et analyse des parties prenantes,
5) Identification et analyse des exigences,
6) Détermination des objectifs,
7) **Détermination des critères de base,**
8) Définition du périmètre.

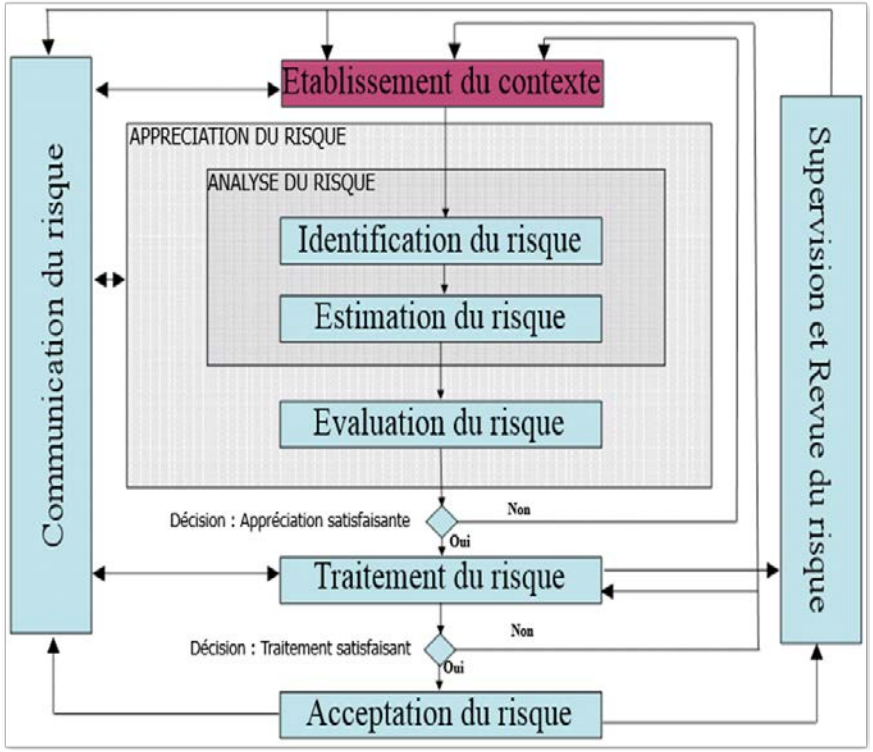


Processus de gestion des risques (ISO 27005)

1. Établissement du contexte

Détermination des critères de base:

- Critères d'évaluation du risque
- Critères d'impact
- Critères d'acceptation du risque



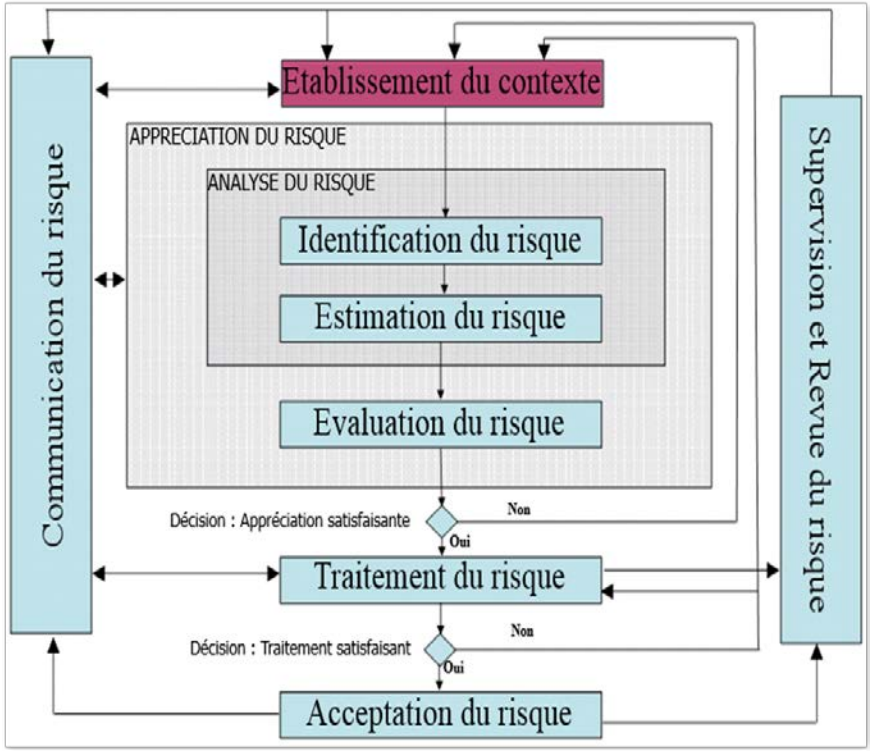
Processus de gestion des risques (ISO 27005)

1. Établissement du contexte ⇨ Détermination des critères de base

a. Critères d'évaluation du risque

1. La valeur stratégique des processus informationnels de l'entreprise,
2. La valeur des actifs informationnels,
3. Les exigences légales, réglementaire et les obligations contractuelles,
4. L'importance opérationnelle et métier de la **confidentialité**, **intégrité** et **disponibilité**,
5. Les attentes et les perceptions des parties prenantes.

↳ Définir une échelle d'évaluation



Processus de gestion des risques (ISO 27005)

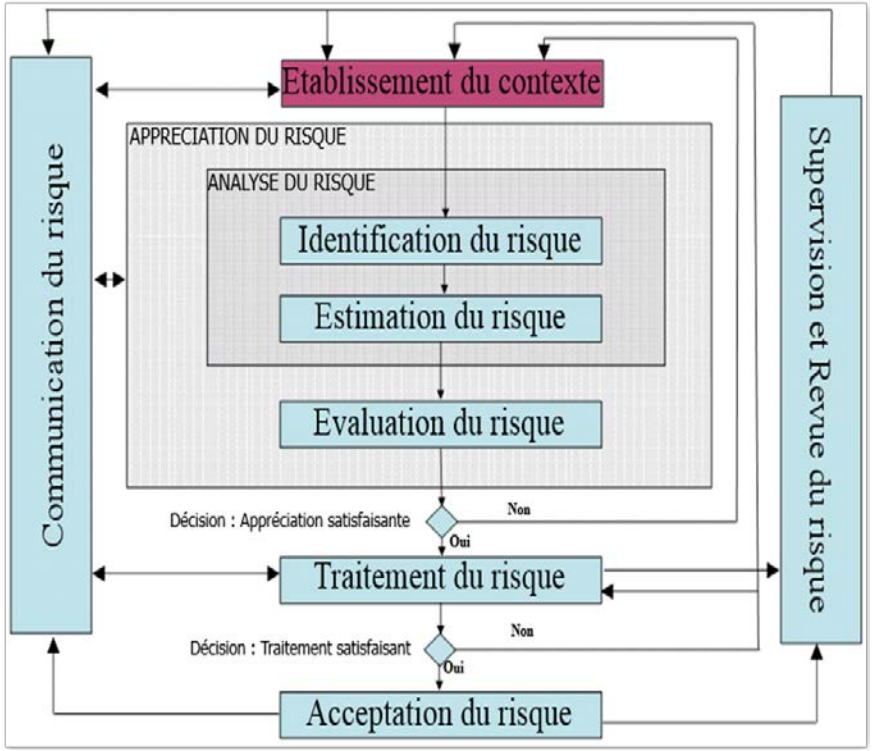
1. Établissement du contexte ⇨ Détermination des critères de base

Trois critères de base:

Confidentialité: propriété que l'information ne soit accessible qu'aux individu, entités, ou processus autorisés.

Disponibilité: propriété d'une information soit accessible et utilisable au moment voulu par une entité autorisée.

Intégrité: propriété de sauvegarder l'exactitude et la qualité des actifs.

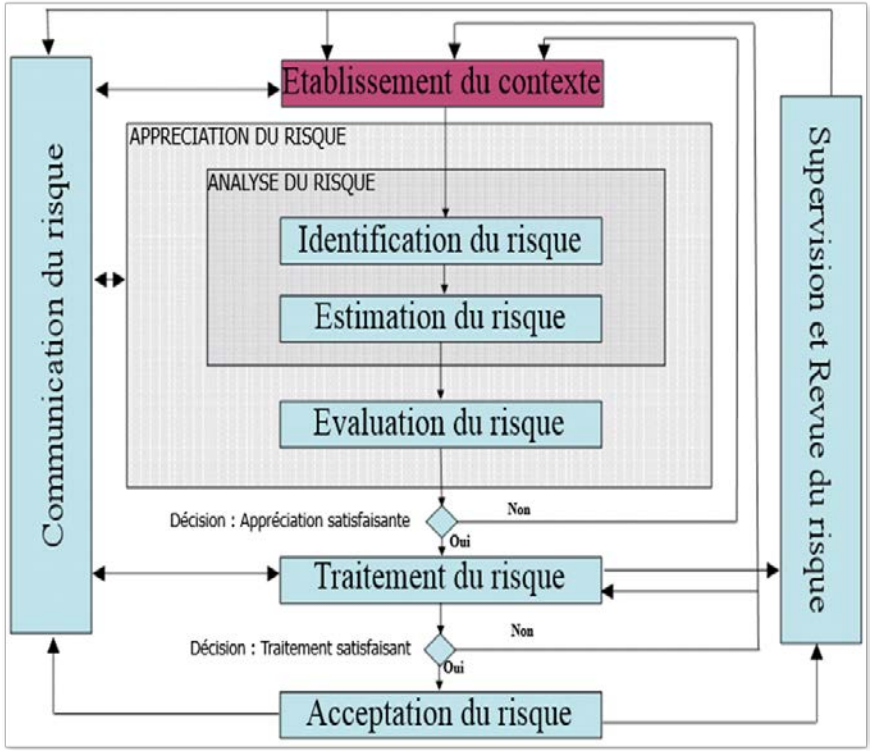


Processus de gestion des risques (ISO 27005)

1. Établissement du contexte ⇨ Détermination des critères de base

b. Critères d'impact

1. Les violations de la sécurité de l'information (impact sur la confidentialité, l'intégrité ou la disponibilité),
2. Perte de valeur financière,
3. Interruption des opérations
4. Atteinte à la réputation
5. Les violations des dispositions légales, règlementaires ou contractuelles.

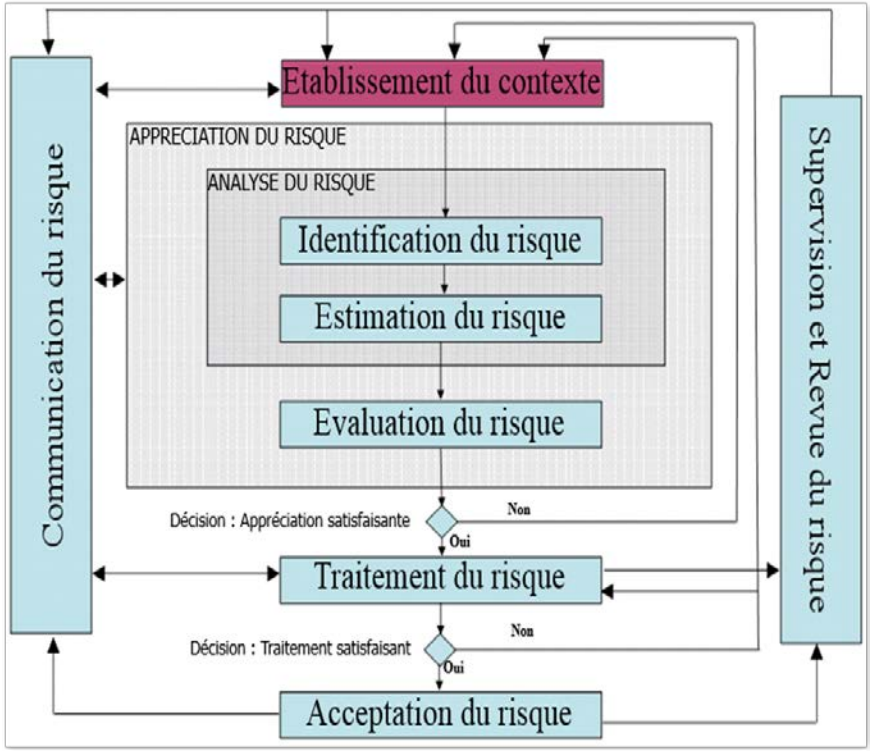


Processus de gestion des risques (ISO 27005)

1. Établissement du contexte ⇨ Détermination des critères de base

c. Critères d'acceptation du risque

1. Les considérations d'affaires,
2. Les aspects juridiques et règlementaires,
3. Les opérations de l'organisme,
4. Les technologies,
5. Les aspects financiers,
6. Les facteurs sociaux et humains.



Processus de gestion des risques (ISO 27005)

1. Établissement du contexte ⇨ Détermination des critères de base

Définition des échelles d'acceptation du risque

- Une échelle peut être:

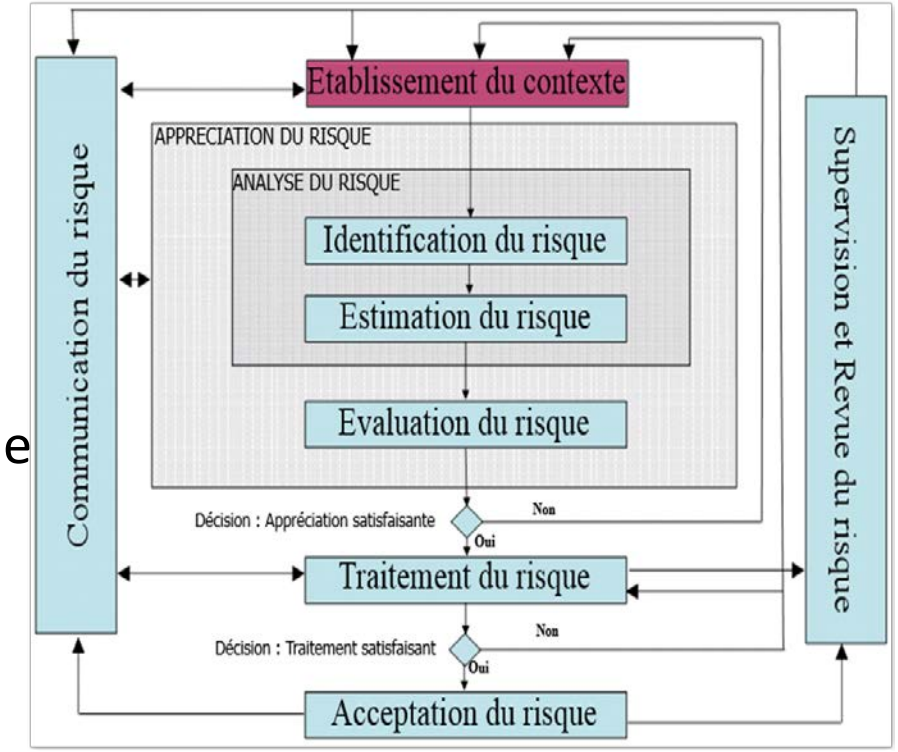
✓ **Qualitative** (échelle de valeurs: 0, 1, 2, …)

Exemple: niveau de menace/vulnérabilité:

faible: 0, moyen: 1, élevé: 2

✓ **Quantitative** (seuil financier): échelle de valeur numérique

Exemple: coût du risque/mesures de sécurité/perte CID



Processus de gestion des risques (ISO 27005)

1. Établissement du contexte ⇨ Détermination des critères de base

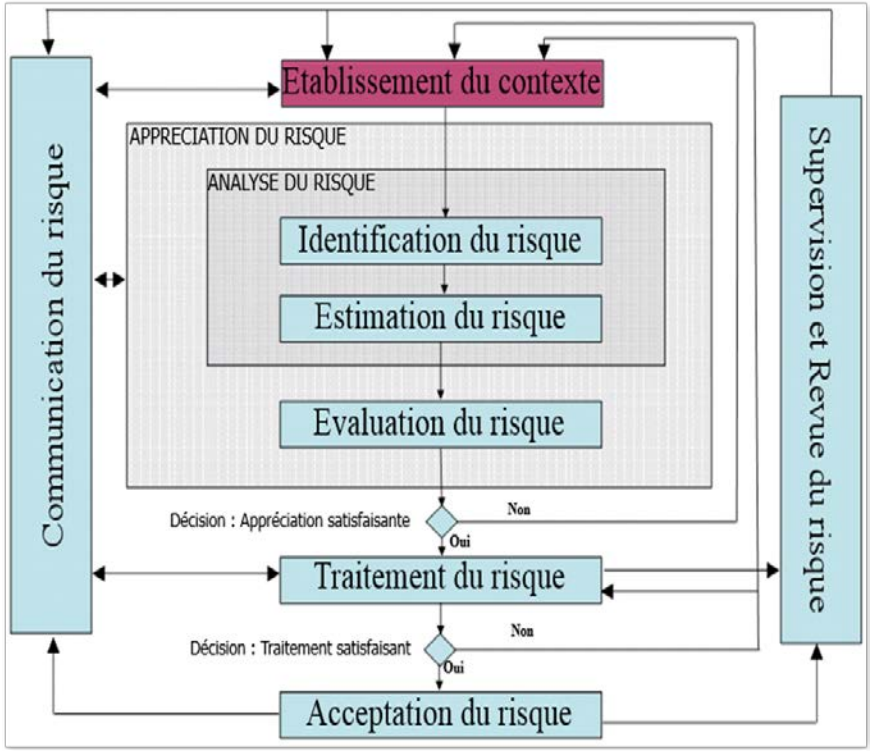
Définition des échelles d'acceptation du risque

- Une échelle peut inclure plusieurs seuils, par exemple:
  - ✓ Un premier seuil d'acceptation du risque qui correspond à celui souhaité par l'organisme
  - ✓ Un deuxième seuil d'acceptation du risque dont le risque doit être accompagné d'un plan de traitement pour être accepter.

Une plage de 0 à M ⇒ Risque non significatif

Une plage de N à **X** ⇒ Risque acceptable (X seuil d'acceptation)

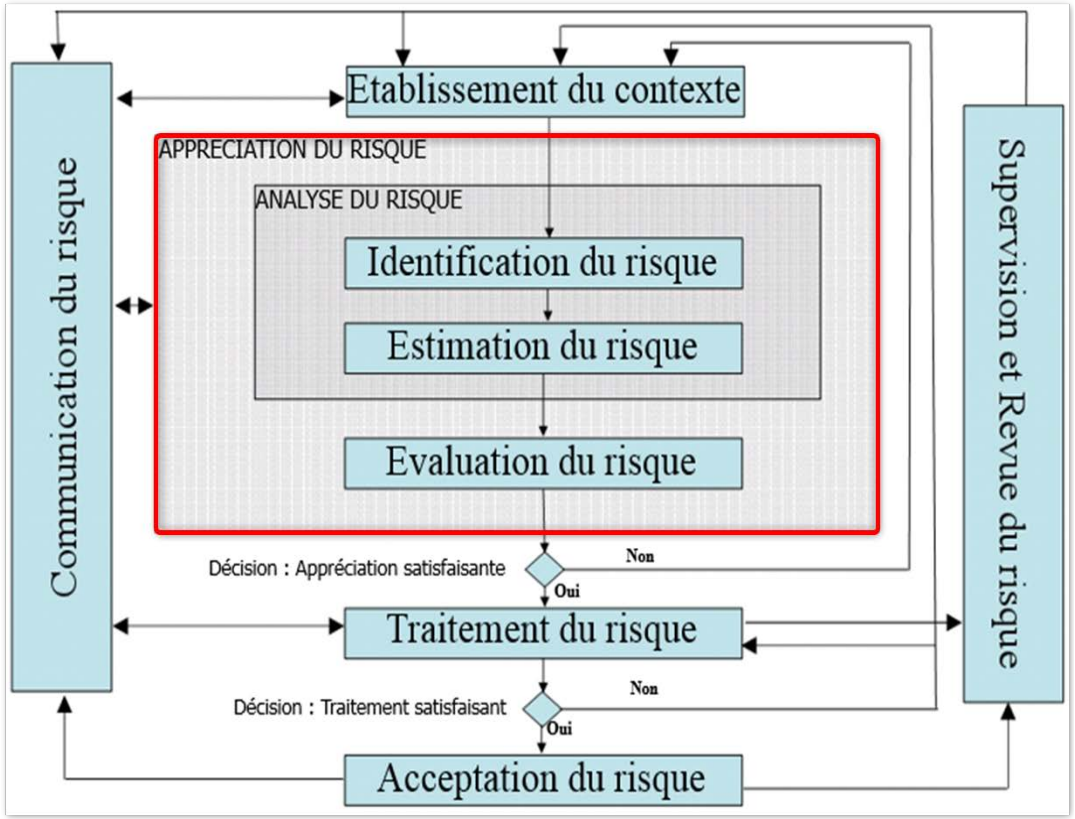
Une plage > X ⇒ Risque non acceptable



Processus de gestion des risques (ISO 27005)

2. Appréciation du risque

- Ensemble des processus d'**analyse** et d'**évaluation** du risque:
  - Identification du risque,
  - Estimation du risque,
  - Evaluation du risque.

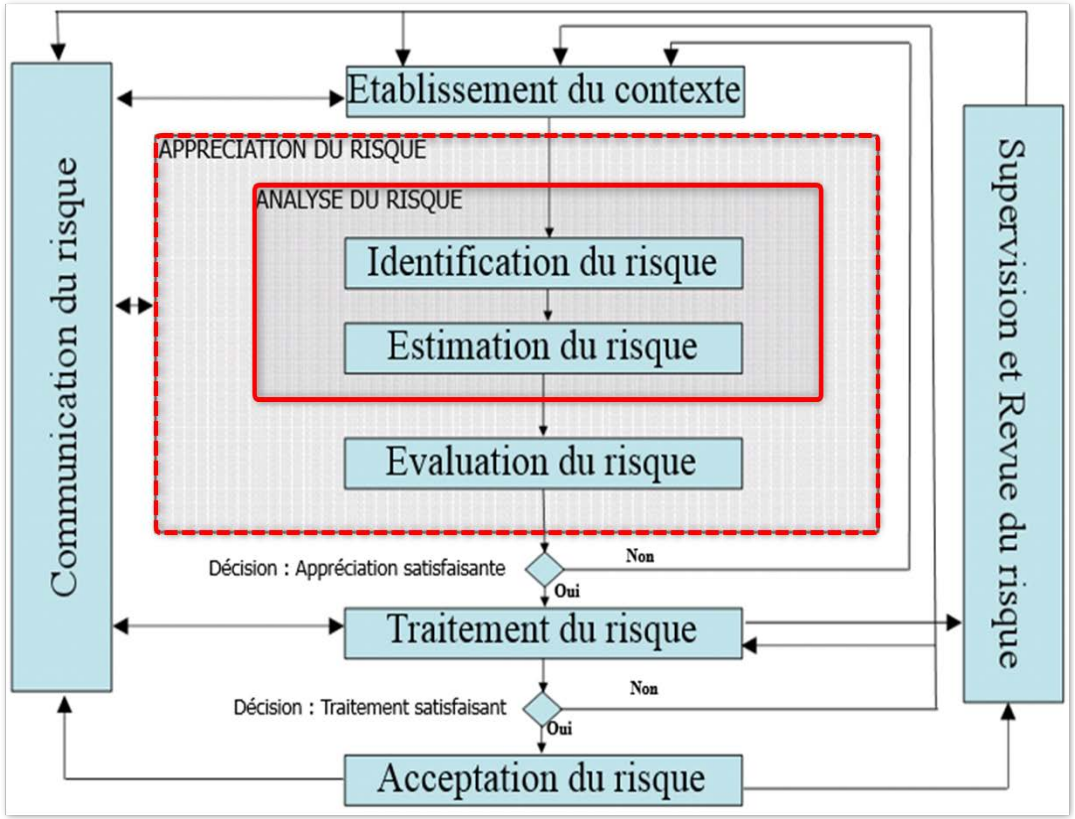


Processus de gestion des risques (ISO 27005)

2. Appréciation du risque

- **Analyse du risque**

Elle a pour finalité l'**identification** et l'**estimation** de chaque composante du risque (menace/vulnérabilité/impact), afin d'**évaluer** le risque et d'**apprécie**r son niveau, dans le but de prendre des **mesures adéquates**.



Processus de gestion des risques (ISO 27005)

2. Appréciation du risque ⇨ Analyse du risque

- **Identification du risque**

Phase de collecte d'informations (établie une liste des scénarios de risque à évaluer):

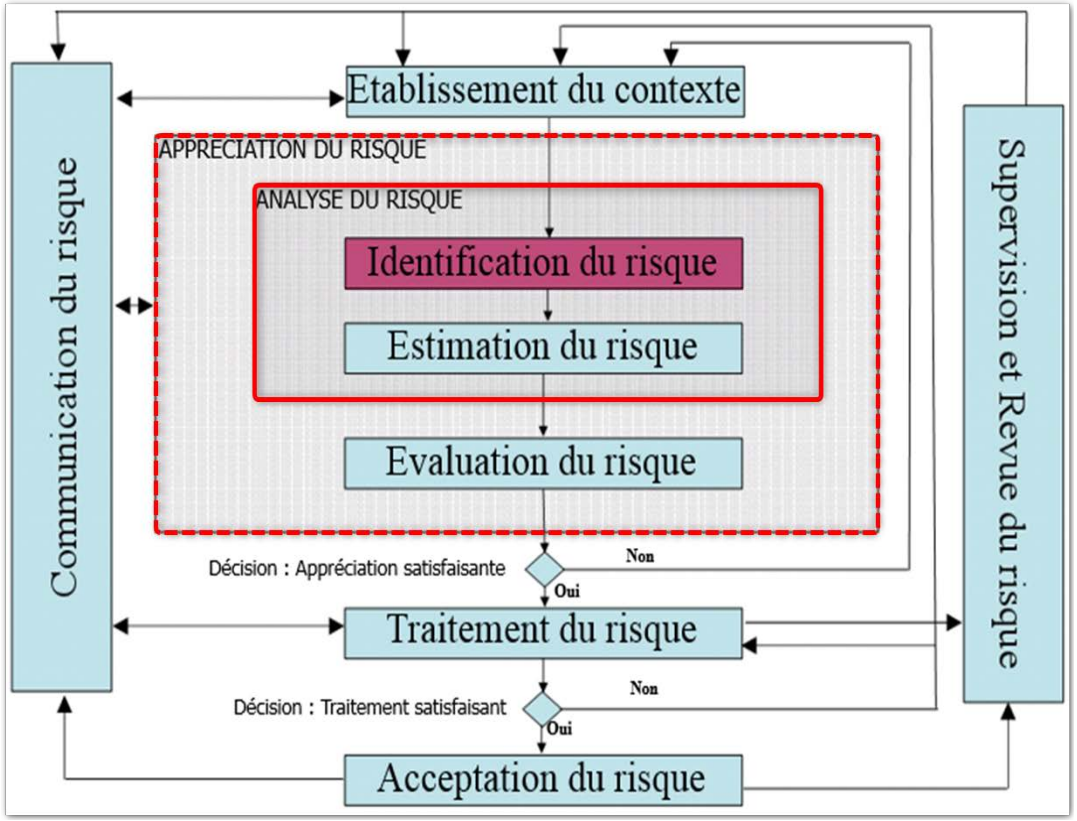
a. Identification des **actifs**,

b. Identification des **menaces**,

c. Identification des **mesures existantes**,

d. Identification des **vulnérabilités**,

e. Identification des **impacts**.



Processus de gestion des risques (ISO 27005)

2. Appréciation du risque ⇨ Analyse du risque ⇨ Identification du risque

a. Identification des actifs

Entrées

- Liste des bien avec leurs propriétaires
- Processus d'affaires
- Locaux, etc.
- Domaine d'application et les limites

Actions

- Identification des actifs inclus dans le domaine d'application

Résultats

- Liste des actifs et processus d'affaires liées

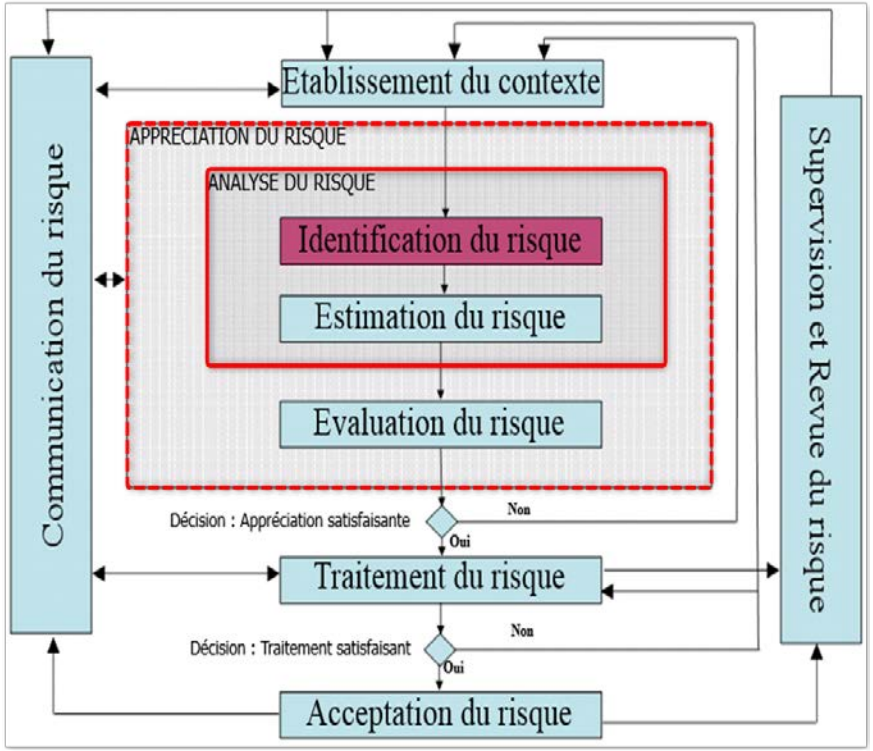
Processus de gestion des risques (ISO 27005)

2. Appréciation du risque ⇨ Analyse du risque ⇨ Identification du risque

a. Identification des actifs

- ✓ Actif avec leur **nature** et leur **propriétaire** (inventaire des actifs),
  - Actifs primaires,
  - Actifs secondaires (de support).
- ✓ Valoriser les actifs suivant l'échelle de valorisation.

☞ Livrable : liste des actifs avec leur nature, leur propriétaire et leur valeur.



Processus de gestion des risques (ISO 27005)

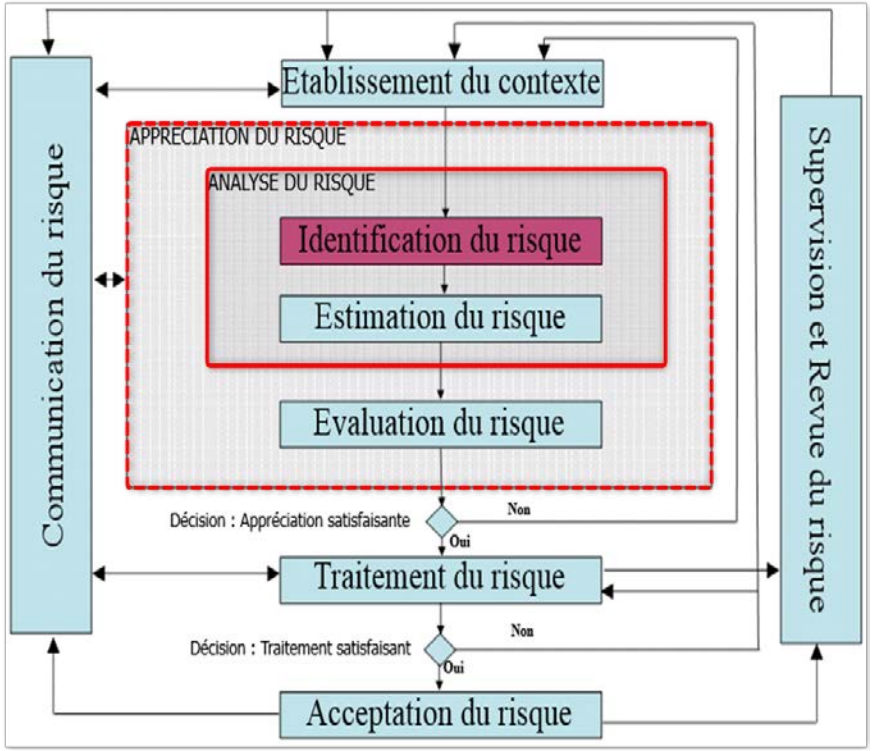
2. Appréciation du risque ⇨ Analyse du risque ⇨ Identification du risque

a. Identification des actifs

- **Actif**: Tout élément représentant une valeur pour l'organisme.

Exemples d'actifs:

- L'information : données significatives,
- Les logiciels: système d'exploitation,
- Physique: ordinateur
- Les services,
- Les personnes: qualification, aptitude, et expérience.
- Intangible: réputation, image.

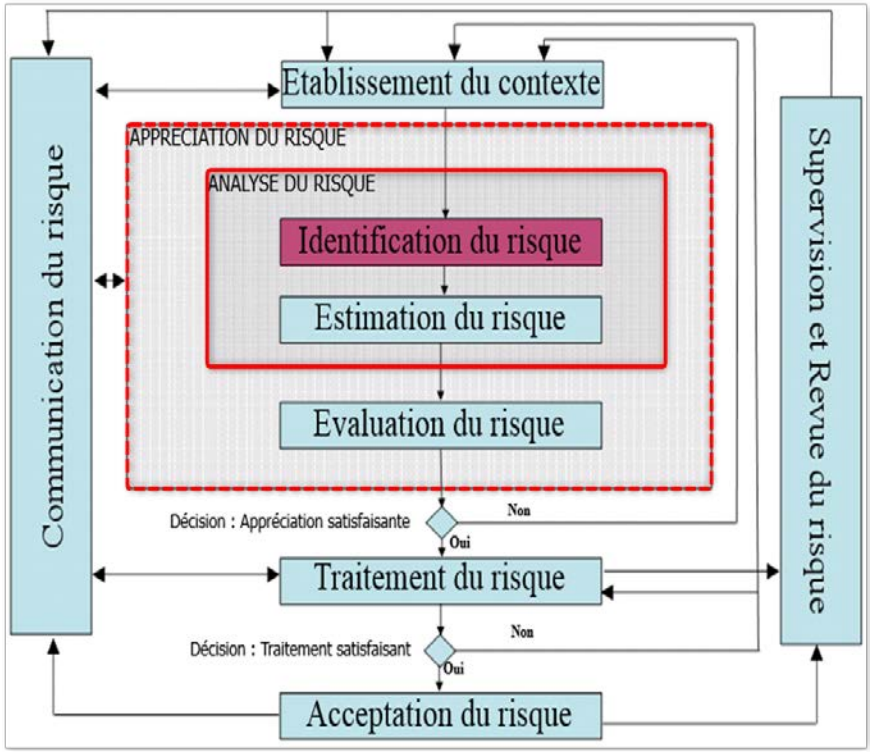


Processus de gestion des risques (ISO 27005)

2. Appréciation du risque ⇨ Analyse du risque ⇨ Identification du risque

❑ Actifs primaires/primordiaux

Toute information/processus métier ayant de la valeur pour l'organisme, **indépendamment de son support**.



✓ **Informations:**

- Données du client,
- Dossiers employés,
- États-financiers,
- Plan stratégique de l'organisme,
- Configuration de réseau, etc.

✓ **Processus métier**

- Gestion des infrastructures,
- Gestion des ressources humaines,
- Comptabilité et finance,
- Marketing, Design, production, service à la clientèle, etc.

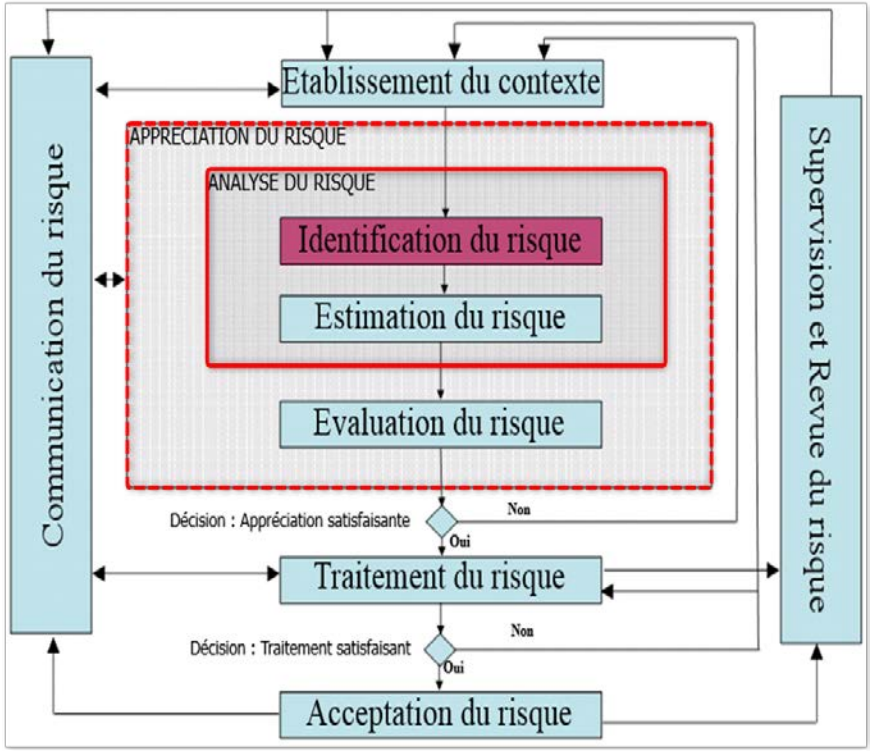
Processus de gestion des risques (ISO 27005)

2. Appréciation du risque ⇨ Analyse du risque ⇨ Identification du risque

❑ Actifs secondaires/de support

Les éléments techniques, humaines et environnementaux, **dépendamment de son support**.

- Matériels,
- Logiciels,
- Réseaux,
- Personnes,
- Sites,
- Organisation,

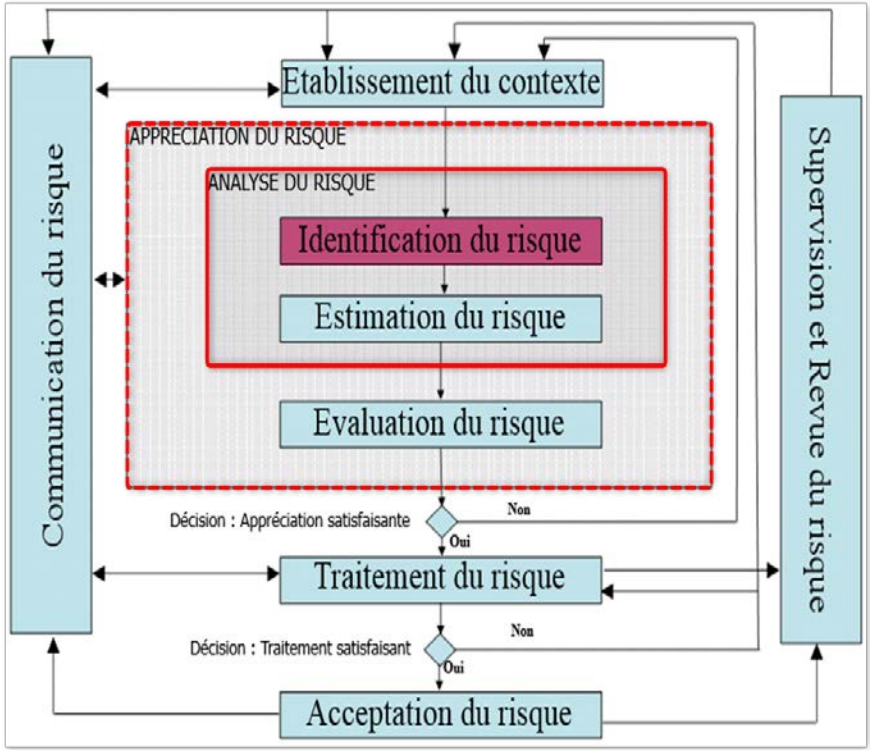


Processus de gestion des risques (ISO 27005)

2. Appréciation du risque ⇨ Analyse du risque ⇨ Identification du risque

❑ Identification des propriétaires des actifs

- Un propriétaire doit être identifié pour chaque actif, afin d'assumer la responsabilité et la traçabilité de l'actif.
- Le propriétaire d'actifs n'a pas nécessairement les droits de propriété sur l'actif, mais il a la responsabilité de sa production, son développement, son entretien, son exploitation et sa sécurité
- Le propriétaire est bien souvent la personne la plus adaptée pour déterminer la valeur de l'actif de l'organisme

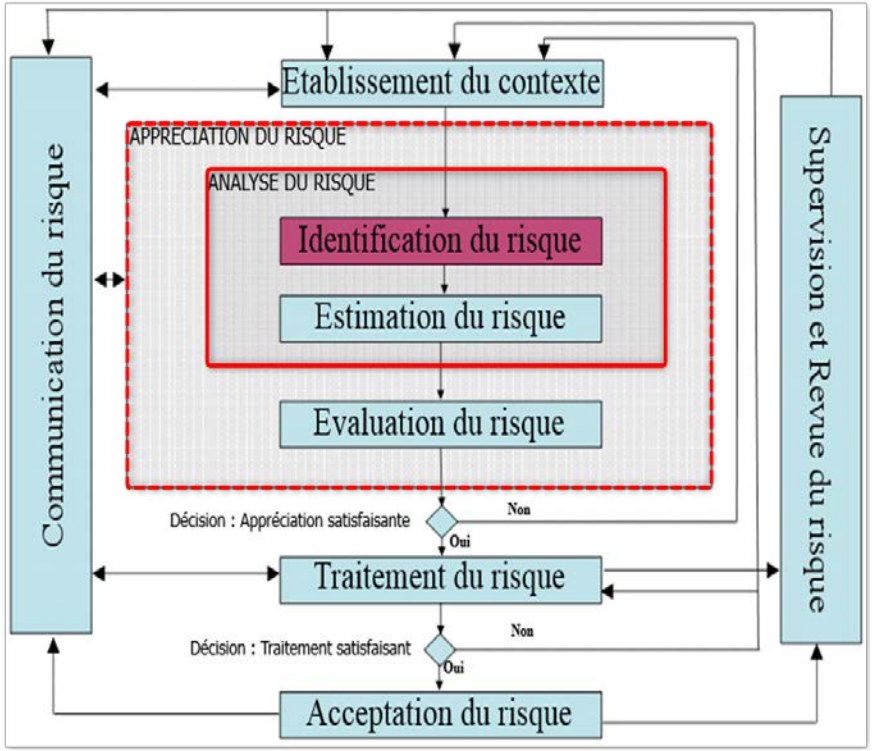


Processus de gestion des risques (ISO 27005)

2. Appréciation du risque ⇨ Analyse du risque ⇨ Identification du risque

❑ Détermination de la valeur des actifs

- L'organisme doit identifier la valeur de ses actifs en élaborant une échelle de valeur des actifs
- Les échelles de valeur des actifs doivent :
  - ✓ Intégrer la confidentialité, l'intégrité et la disponibilité, ou différentes propriétés importantes de l'actif qui pourraient être affectées
  - ✓ Tenir compte des dépendances à d'autres actifs



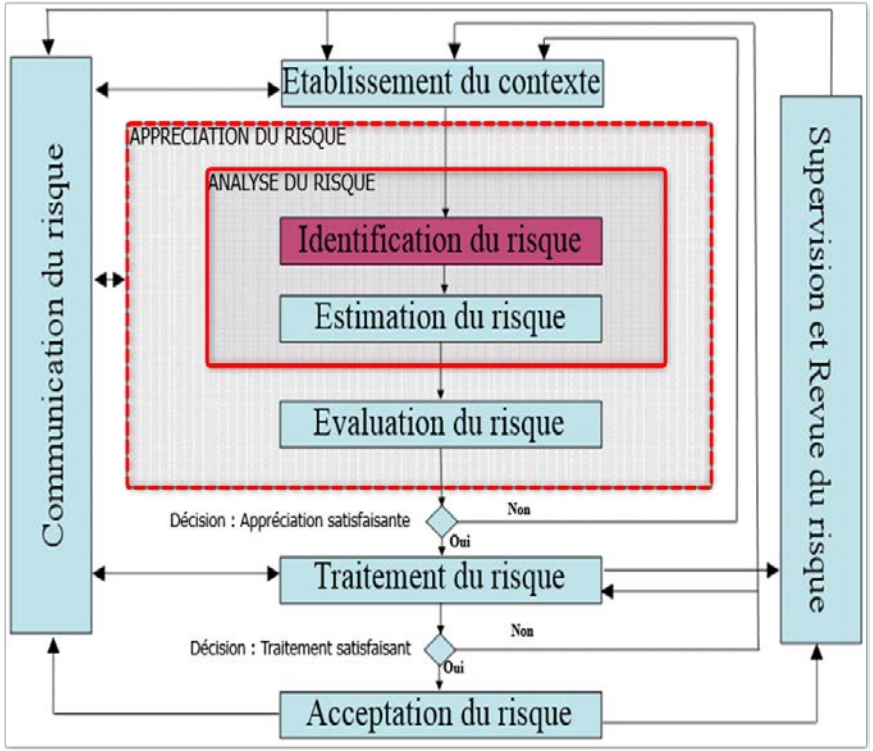
Processus de gestion des risques (ISO 27005)

2. Appréciation du risque ⇨ Analyse du risque ⇨ Identification du risque

❑ Échelle de valeur d'un actif

Exemple

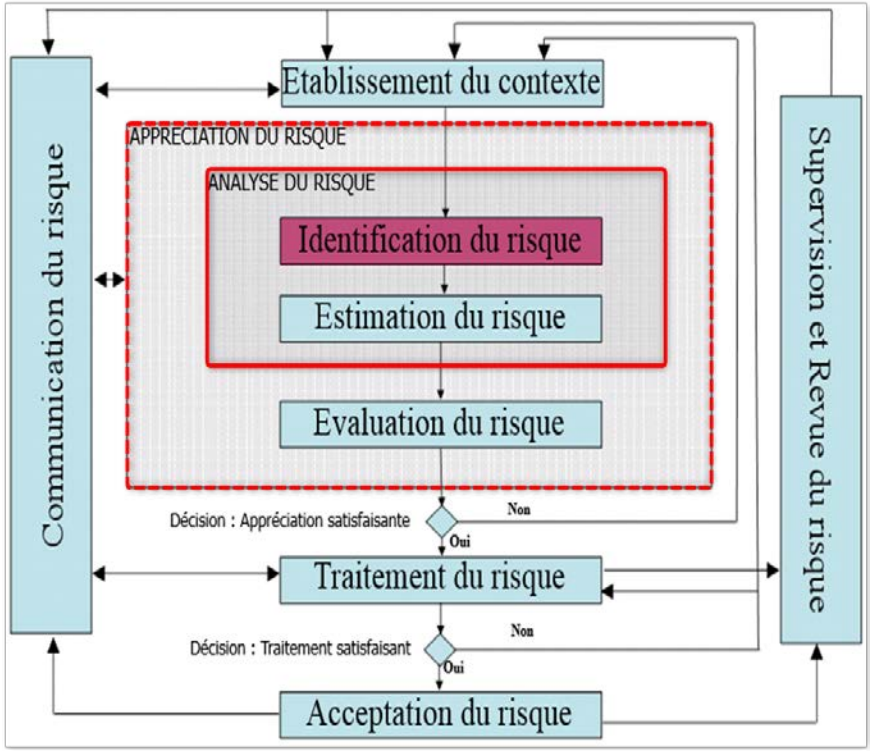
Échelle	Valeur de l'actif
Négligeable	0
Faible	1
Moyenne	2
Élevée	3
Très élevée	4



Processus de gestion des risques (ISO 27005)

2. Appréciation du risque ⇨ Analyse du risque ⇨ Identification du risque

- **Exemple** (École de formation)
  - Une école de formation ayant pour activité:
    - ✓ Créer les supports de cours
    - ✓ Donner les formations
  - 2 salariés : le formateur et un assistant
  - Formation sur la norme ISO 27005



Processus de gestion des risques (ISO 27005)

2. Appréciation du risque ⇨ Analyse du risque ⇨ Identification du risque

Inventaire des actifs

Liste des actifs			
	Description	**Nature**	**Propriétaire**
Actifs Primaires			
AP - 1	Processus de formation	Processus	Formateur
AP - 2	Processus de création du contenu	Processus	Formateur
AP - 3	Cours - contenu	Information	Assistant
Actifs Secondaires (Support)			
AS - 1	Salle de formation	Site	Assistant
AS - 2	Vidéo projecteur	Matériel	Assistant
AS - 3	Ordinateur	Matériel	Assistant
AS - 4	Formateur	Personnel	Formateur
AS - 5	Assistant	Personnel	Assistant
AS - 6	Microsoft PowerPoint	Logiciel	Assistant
AS - 7	Cours - format numérique	Document	Assistant

Processus de gestion des risques (ISO 27005)

2. Appréciation du risque ⇨ Analyse du risque ⇨ Identification du risque

Échelle de valorisation des actifs

Valeur	Signification	Coût achat			délai remplacement			Compétence		
		Faible	moyen	élevé	jour	semaine	> semaine	aucune	faible	forte
1	Faible	X			X			X		
2	Moyen		X			X			X	
3	Elevé			X			X			
4	Très élevé	-	-	-	-	-	-			X

Processus de gestion des risques (ISO 27005)

2. Appréciation du risque ⇨ Analyse du risque ⇨ Identification du risque

Liste des actifs				
	Description	**Nature**	**Propriétaire**	**Valeur**
Actifs Primaires				
AP - 1	Processus de formation	Processus	Formateur	4
AP - 2	Processus de création du contenu	Processus	Formateur	3
AP - 3	Cours - contenu	Information	Assistant	4
Actifs Secondaires (Support)				
AS - 1	Salle de formation	Site	Assistant	3
AS - 2	Vidéo projecteur	Matériel	Assistant	2
AS - 3	Ordinateur	Matériel	Assistant	2
AS - 4	Formateur	Personnel	Formateur	4
AS - 5	Assistant	Personnel	Assistant	3
AS - 6	Microsoft PowerPoint	Logiciel	Assistant	1
AS - 7	Cours - format numérique	Document	Assistant	3

Processus de gestion des risques (ISO 27005)

2. Appréciation du risque ⇨ Analyse du risque ⇨ Identification du risque

b. Identification des menaces

Entrées

- Informations générale sur les menaces obtenues à partir de sources diverses (interne et externe)

Actions

- Recensement des menaces et leurs sources concernant le domaine d'application

Résultats

- Une liste des menaces avec l'identification du type et de la source

Processus de gestion des risques (ISO 27005)

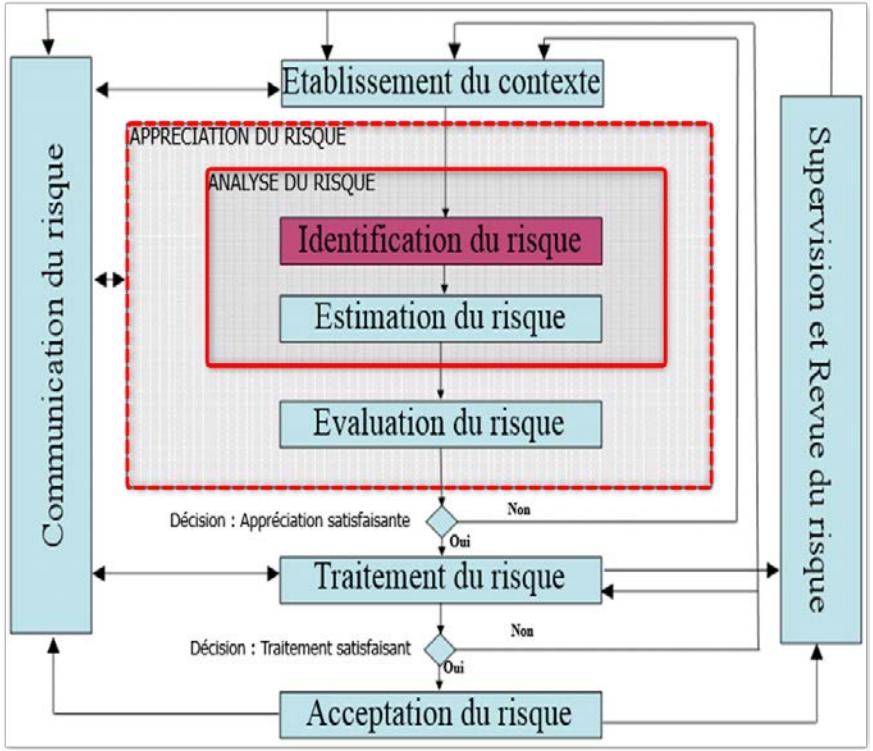
2. Appréciation du risque ⇨ Analyse du risque ⇨ Identification du risque

b. Identification des menaces

✓ Menaces avec leur **type**, leur **source** et leur **cible** :

- **Type**: Compromission de l'information, pannes techniques, actions non autorisées, etc.
- **Source**: Qui et quoi cause la menace?,
- **Cible:** Quels éléments du système peuvent être affectés par la menace ?.

☞ Livrable : liste des menaces avec l'identification du type, la source et la cible

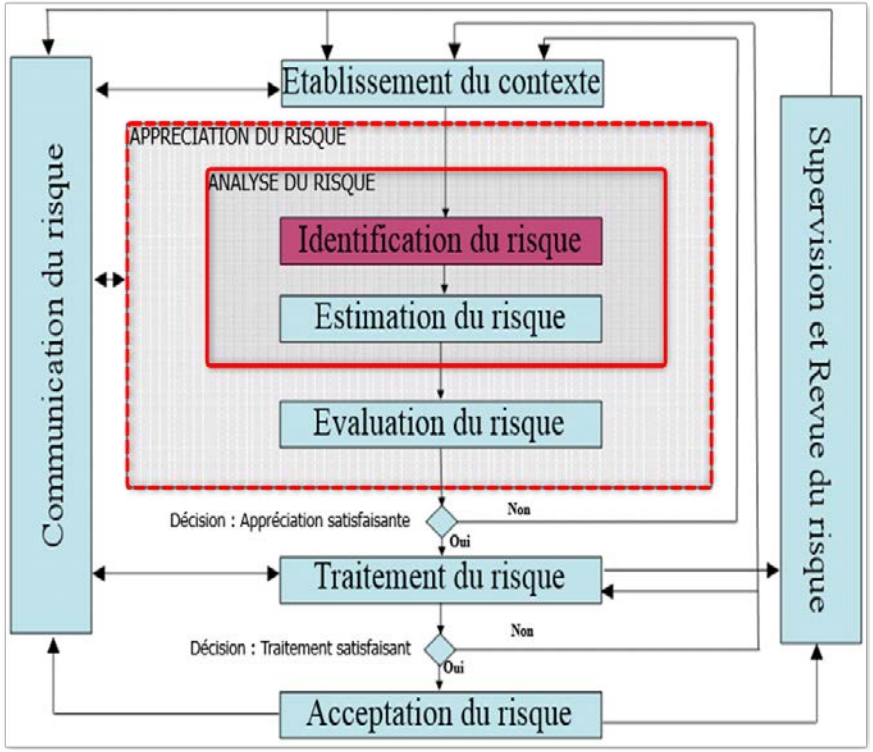


Processus de gestion des risques (ISO 27005)

2. Appréciation du risque ⇨ Analyse du risque ⇨ Identification du risque

b. Identification des menaces

- **Menace**: Cause potentielle d'un accident indésirable pouvant affecter une organisation



Processus de gestion des risques (ISO 27005)

2. Appréciation du risque ⇨ Analyse du risque ⇨ Identification du risque

❑ Type de menaces

Type de menaces	Exemple
1. Dommage physique	Feu
	Dégât d'eau
2. Désastre naturel	Tremblement de terre
	Inondation
3. Perte de service essentiel	Panne de climatisation
	Panne électrique
4. Perturbation causée par radiation	Radiation électromagnétique
	Radiation thermique
5. Information compromise	Écoute électronique
	Vol de documents
6. Panne technique	Bris d'équipement
	Saturation de réseau
7. Action non autorisée	Accès non autorisé Utilisation d'un logiciel piraté

Processus de gestion des risques (ISO 27005)

2. Appréciation du risque ⇨ Analyse du risque ⇨ Identification du risque

- **Origine des menaces**

Exemple

	Naturelle	Délibérée	Accidentelle
Incendie	x	x	x
Abus de privilèges	-	x	x
Vol d'équipements	-	x	-
Tremblement de terre	x	-	-

Processus de gestion des risques (ISO 27005)

2. Appréciation du risque ⇨ Analyse du risque ⇨ Identification du risque

- **Menace de nature intentionnelle**

  Exemple

	Motivation	Impact potentiel
Hacker	Argent, défi, statut, etc.	Ingénierie sociale, accès non autorisé
Criminel	Gain financier	Fraude, extorsion
Ancien employé	Vengeance	Sabotage de système
Compétiteur	Espionnage	Vol d'informations

Processus de gestion des risques (ISO 27005)

2. Appréciation du risque ⇨ Analyse du risque ⇨ Identification du risque

- **Exemple** (École de formation)

Liste des actifs					
	Description	**Nature**	**Propriétaire**	**Valeur**	**Menace**
Actifs Primaires					
AP - 1	Processus de formation	Processus	Formateur	4	
AP - 2	Processus de création du contenu	Processus	Formateur	3	
AP - 3	Cours - contenu	Information	Assistant	4	
Actifs Secondaires (Support)					
AS - 1	Salle de formation	Site	Assistant	3	
AS - 2	Vidéo projecteur	Matériel	Assistant	2	
AS - 3	Ordinateur	Matériel	Assistant	2	Vol Panne
AS - 4	Formateur	Personnel	Formateur	4	Maladie Démission
AS - 5	Assistant	Personnel	Assistant	3	
AS - 6	Microsoft PowerPoint	Logiciel	Assistant	1	
AS - 7	Cours - format numérique	Document	Assistant	3	Destruction

Processus de gestion des risques (ISO 27005)

2. Appréciation du risque ⇨ Analyse du risque ⇨ Identification du risque

c. Identification des mesures existantes

Entrées

- Documentation des mesures de sécurité
- Plan de traitement de risque

Actions

- Identification des mesures de sécurité existantes et prévues

Résultats

- Liste des mesures de sécurité existantes et prévues avec leur statut

Processus de gestion des risques (ISO 27005)

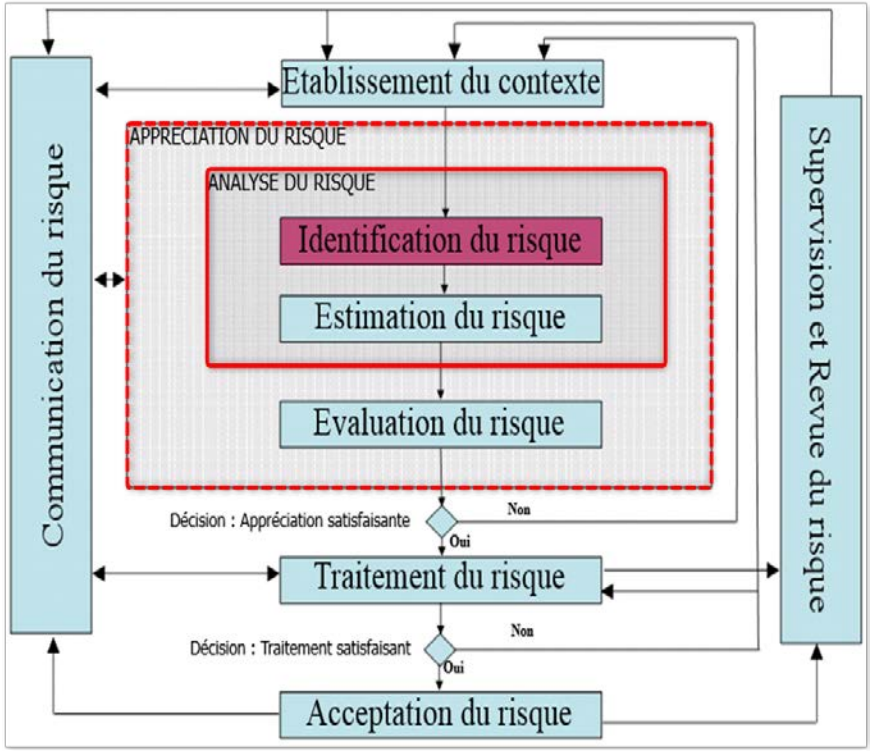
2. Appréciation du risque ⇨ Analyse du risque ⇨ Identification du risque

c. Identification des mesures existantes

✓ Vérification de l'efficacité des mesures de sécurité:

- Audit et contrôle du SI,
- Vérification sur le terrain,
- Interview avec RSSI (Responsable SSI),
- Revue sur site des mesures de sécurité physique,
- Etc.

☞ Livrable : liste des mesures de sécurité existante et prévues avec leur statut



Processus de gestion des risques (ISO 27005)

2. Appréciation du risque ⇨ Analyse du risque ⇨ Identification du risque

❑ Modèle d'identification des mesures existantes

Exemple

Mesure de sécurité	Description de la mesure de sécurité	Description actuelle	Responsable
Document de politique de sécurité de l'information	Un document de politique de sécurité de l'information doit être approuvé par la direction, puis publié et diffusé auprès de l'ensemble des salariés et des tiers concernés	Une politique de sécurité de l'information a été publiée et a été signée par la direction générale, mais le document est difficilement accessible à tous les employés	Ahmed, RSSI
Réexamen de la politique de sécurité de l'information	Pour garantir la pertinence, l'adéquation et l'efficacité de la politique de sécurité de l'information, la politique doit être examinée à intervalles fixés probablement ou en cas de changements majeurs	La politique est en vigueur depuis 6 ans et n'a jamais fait le réexamen formel	Ahmed, RSSI

№	Scénario d'incident	Actif impacté		C	I	D	Somme	MAX	Mes. Sec.
1	Vol de l'ordinateur du à sa portabilité	AP-1	Processus de formation	3	1	2	6	8	
		AP-2	Processus de création du contenu	1	1	2	4		
		AP-3	Cours-contenu	3	3	2	8		
		AS-3	Ordinateur	3	3	2	8		
		AS-8	Cours-Format numérique	3	3	2	8		
2	Destruction de l'ordinateur du à sa portabilité	AP-1	Processus de formation	1	2	2	5	6	
		AP-2	Processus de création du contenu	1	2	2	5		
		AP-3	Cours-contenu	1	2	2	5		
		AS-3	Ordinateur	1	3	2	6		
		AS-8	Cours-Format numérique	1	3	2	6		
3	L'ordinateur ne s'allume (décharge totale des batteries)	AP-1	Processus de formation	1	1	3	5	5	
		AP-2	Processus de création du contenu	1	1	2	4		
		AS-3	Ordinateur	1	1	2	4		
4	Connexion frauduleuse et altération du support de cours	AP-1	Processus de formation	2	3	2	7	7	Identifiant/mot de passe
		AP-3	Cours-contenu	1	3	2	6		
		AS-8	Cours-Format numérique	1	3	2	6		
5	Connection frauduleuse et vol du support par la concurrence	AP-1	Processus de formation	3	2	1	6	6	Identifiant/mot de passe
		AP-3	Cours-contenu	3	1	2	6		
		AS-8	Cours-Format numérique	3	1	1	5		
6	Le formateur est approché par la concurrence et démissionne	AP-1	Processus de formation	3	1	3	7	7	
		AS-4	Formateur	1	1	3	5		

Processus de gestion des risques (ISO 27005)

2. Appréciation du risque ⇨ Analyse du risque ⇨ Identification du risque

d. Identification des vulnérabilités

Entrées

- La liste des menaces et vulnérabilité connues
- La liste des actifs
- La liste des mesures de sécurité existantes

Actions

- Identification des vulnérabilités

Résultats

- Liste des vulnérabilité en fonction des actifs, des menaces et des mesures de sécurité

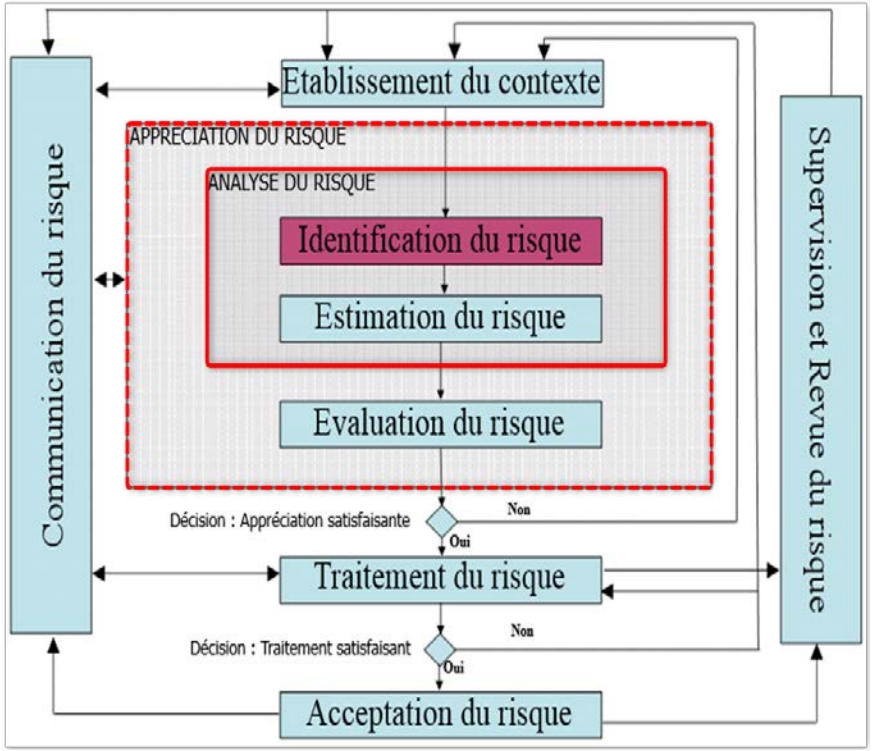
Processus de gestion des risques (ISO 27005)

2. Appréciation du risque ⇨ Analyse du risque ⇨ Identification du risque

d. Identification des vulnérabilités

- ✓ Vulnérabilités spécifiques aux actifs inclus dans le domaine d'application:
  - Audit,
  - Expérience,
  - Autres méthodes.

☞ **Livrable** : liste de vulnérabilités en fonction des actifs, des menaces et des mesures de sécurité

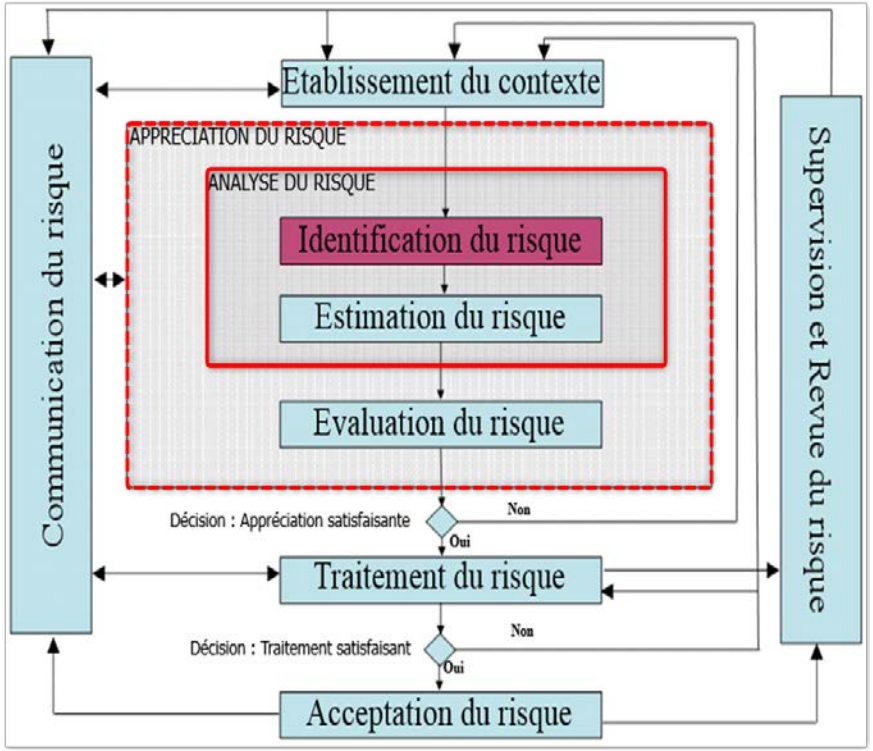


Processus de gestion des risques (ISO 27005)

2. Appréciation du risque ⇨ Analyse du risque ⇨ Identification du risque

d. Identification des vulnérabilités

- **Vulnérabilité**: Faille d'un actif ou d'une mesure de sécurité qui pourrait être exploitée par une menace



Processus de gestion des risques (ISO 27005)

2. Appréciation du risque ⇨ Analyse du risque ⇨ Identification du risque

❑ Type de vulnérabilité

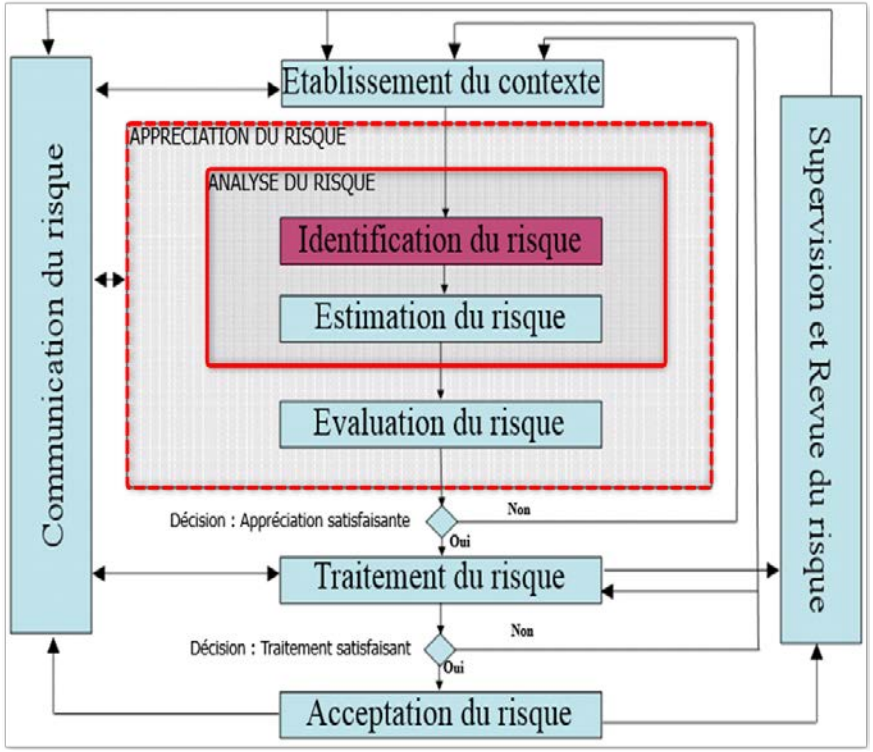
Type de vulnérabilité	Exemple
1. Matériel informatique	Manque d'entretien
	Portabilité
2. Logiciel	Absence d'enregistrement des logs
	Interfaces de saisie compliquées
3. Réseau	Absence de chiffrement des transferts
	Point unique d'accès
4. Personnel	Formation insuffisante
	Manque d'encadrement
5. Localisation (lieu)	Système électrique instable
	Site en zone inondable
6. Structure organisationnelle	Absence de séparation des tâches
	Absence de description de tâches

Processus de gestion des risques (ISO 27005)

2. Appréciation du risque ⇨ Analyse du risque ⇨ Identification du risque

❑ Identification des vulnérabilités techniques

- Il est possible d'utiliser des méthodes proactives comme des tests du système d'information afin d'identifier les vulnérabilités par rapport à la criticité du système de technologie de l'information, des communication (TIC) et des ressources disponibles
- Les méthodes de tests comprennent:
  - Outil automatisé d'analyse de vulnérabilités,
  - Test et évaluation de sécurité,
  - Tests d'intrusion,
  - Revue de code.



Processus de gestion des risques (ISO 27005)

2. Appréciation du risque ⇨ Analyse du risque ⇨ Identification du risque

❑ Lien entre actif, vulnérabilité et menace

Exemples

Actif	Vulnérabilité	Menace
1. Matériel	Entrepôt non surveillé	Vol d'équipement
	Sensibilité à l'humidité	Corrosion
2. Logiciel	Absence de piste d'audit	Abus de droit non détecté
	Interface usager compliqué	Erreur de saisie
3. Réseau	Ligne de communication non protégée	Écoute électronique
	Transfert des mots de passe en claire	Hacker
4. Personnel	Insuffisance de formation	Erreur
	Manque de supervision	Vol d'équipement
5. Site	Site dans un endroit inondable	Inondation
	Réseau électrique non stable	Perte de courant
6. Organisation	Absence de processus d'autorisation de droits d'accès	Abus de privilèges
	Absence de gestion documentaire	Corruption de données

Processus de gestion des risques (ISO 27005)

2. Appréciation du risque ⇨ Analyse du risque ⇨ Identification du risque

- **Exemple** (École de formation)

Liste des actifs						
	Description	**Nature**	**Propriétaire**	**Valeur**	**Menace**	**Vulnérabilité**
Actifs Primaires						
AP - 1	Processus de formation	Processus	Formateur	4		
AP - 2	Processus de création du contenu	Processus	Formateur	3		
AP - 3	Cours - contenu	Information	Assistant	4		
Actifs Secondaires (Support)						
AS - 1	Salle de formation	Site	Assistant	3		
AS - 2	Vidéo projecteur	Matériel	Assistant	2		
AS - 3	Ordinateur	Matériel	Assistant	2	Vol Panne	Portabilité Alimentation élec
AS - 4	Formateur	Personnel	Formateur	4	Maladie Démission	Manque de prévention Manque d'ambition
AS – 5	Assistant	Personnel	Assistant	3		
AS - 6	Microsoft PowerPoint	Logiciel	Assistant	1		
AS - 7	Cours - format numérique	Document	Assistant	3	Destruction	Support numérique

Processus de gestion des risques (ISO 27005)

2. Appréciation du risque ⇨ Analyse du risque ⇨ Identification du risque

e. Identification des impacts (conséquences)

Entrées

- Une liste des actifs, des processus métier, des menaces et des vulnérabilités

Actions

- Identification des conséquences en terme de confidentialité, d'intégrité et de disponibilité sur les actifs

Résultats

- Liste des scénarios d'incidents avec leurs conséquences liées aux actifs et aux processus métier

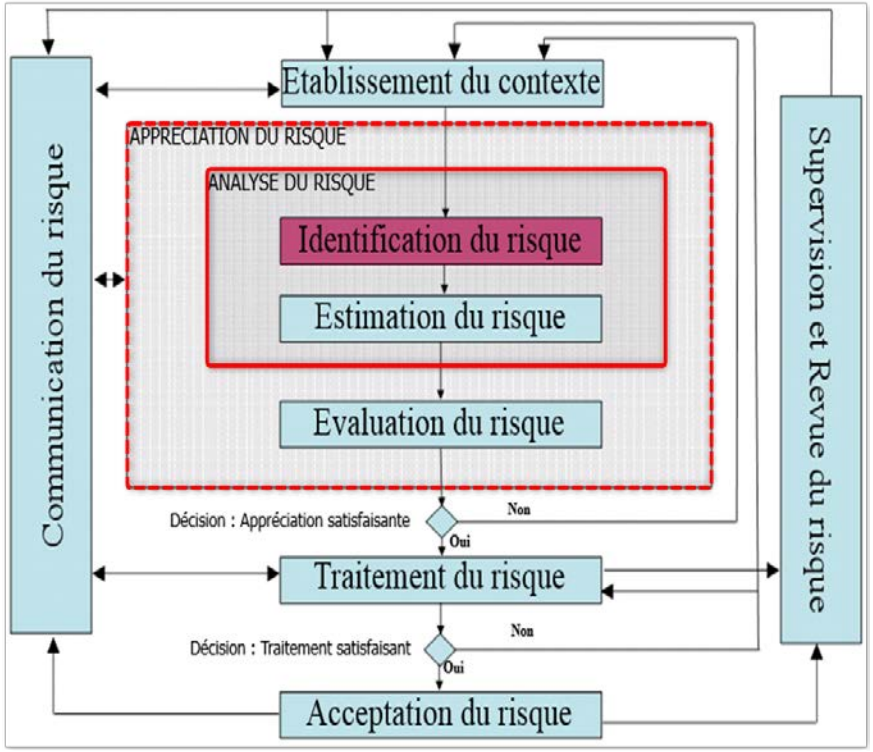
Processus de gestion des risques (ISO 27005)

2. Appréciation du risque ⇨ Analyse du risque ⇨ Identification du risque

e. Identification des impacts (conséquences)

- ✓ **Dommages** ou **impacts** sur l'organisme lors d'un **incident** de sécurité.

☞ <u>Livrable</u> : Liste des scénarios d'incidents avec leurs conséquences liées aux actifs et aux processus métier



Processus de gestion des risques (ISO 27005)

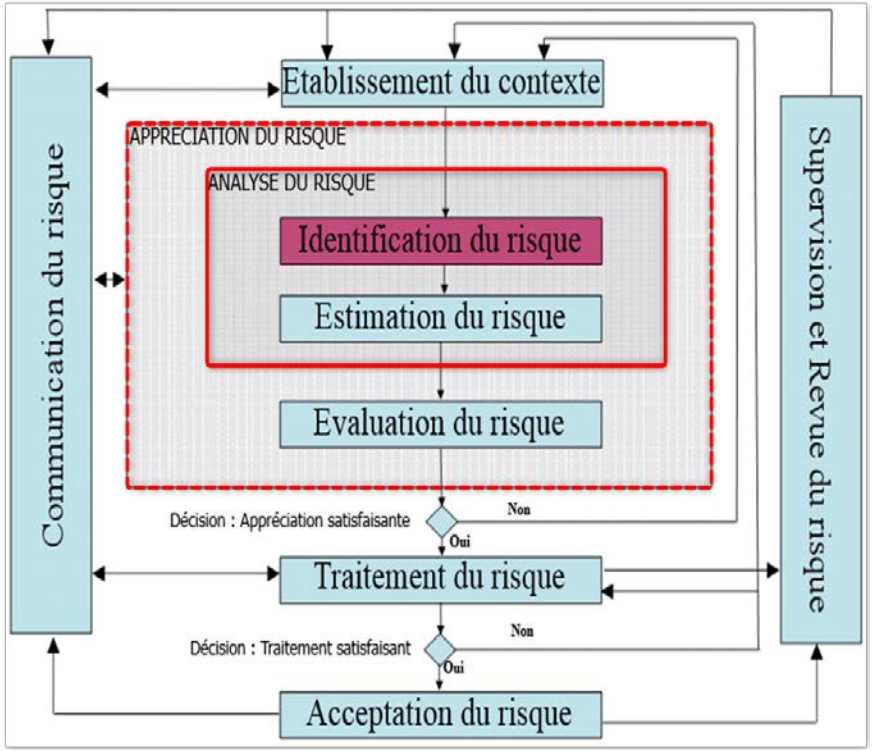
2. Appréciation du risque ⇨ Analyse du risque ⇨ Identification du risque

e. Identification des impacts (conséquences)

- **Conséquence**: Effet d'un événement affectant les objectifs

Remarques:

- Un événement peut engendrer une série de conséquences
- Une conséquence peut être certaine ou incertaine
- Les conséquences peuvent être exprimées de façon qualitative ou quantitative
- Des conséquences initiales peuvent déclencher des réactions en chaîne

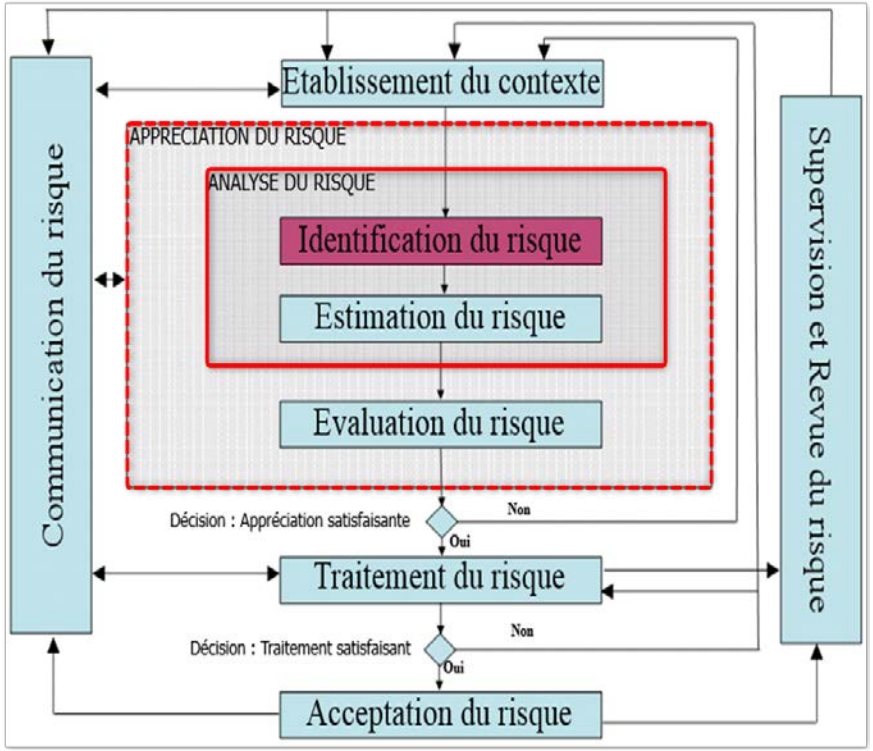


Processus de gestion des risques (ISO 27005)

2. Appréciation du risque ⇨ Analyse du risque ⇨ Identification du risque

❑ Critères d'identification des impacts

- Les organisations devraient identifier les impacts des scénarios d'incident en termes de:
  1. Délais d'investigation et de réparation
  2. Du temps (de travail) perdu
  3. Des opportunités perdues
  4. La santé et la sécurité au travail
  5. Dépenses de formation, d'honoraire, d'achat de matériel, etc.
  6. Impact sur la réputation



Processus de gestion des risques (ISO 27005)

2. Appréciation du risque ⇨ Analyse du risque ⇨ Identification du risque

❑ Identification des impacts

Exemple

Disponibilité	Intégrité	Confidentialité
▪ Dégradation des performances ▪ Interruption d'un service ▪ Inaccessibilité d'un service ▪ Perturbation des opérations	▪ Modification accidentelle ▪ Modification délibérée ▪ Résultats incorrects ▪ Résultats incomplets ▪ Perte de données	▪ Atteinte à la vie privée des usagers ou des clients ▪ Atteinte à la vie privée du personnel de l'organisme ▪ Fuite d'information confidentielle

Processus de gestion des risques (ISO 27005)

2. Appréciation du risque ⇨ Analyse du risque ⇨ Identification du risque

❑ Menace, vulnérabilité et impact

Exemples de liens

Menace	Vulnérabilité	Impact
Vol d'équipements	Entrepôt non surveillé	Pertes monétaires
Corrosion	Sensibilité à l'humidité	Bris d'équipement
Erreur de saisie	Interface utilisateur compliquée	Base de donnée corrompue
Écoute électronique	Ligne de communication non protégée	Interception de communication
Hacker	Transfert des mots de passe en clair	Vol d'information
Corruption de données	Absence de processus de gestion documentaire	Documentation pas à jour

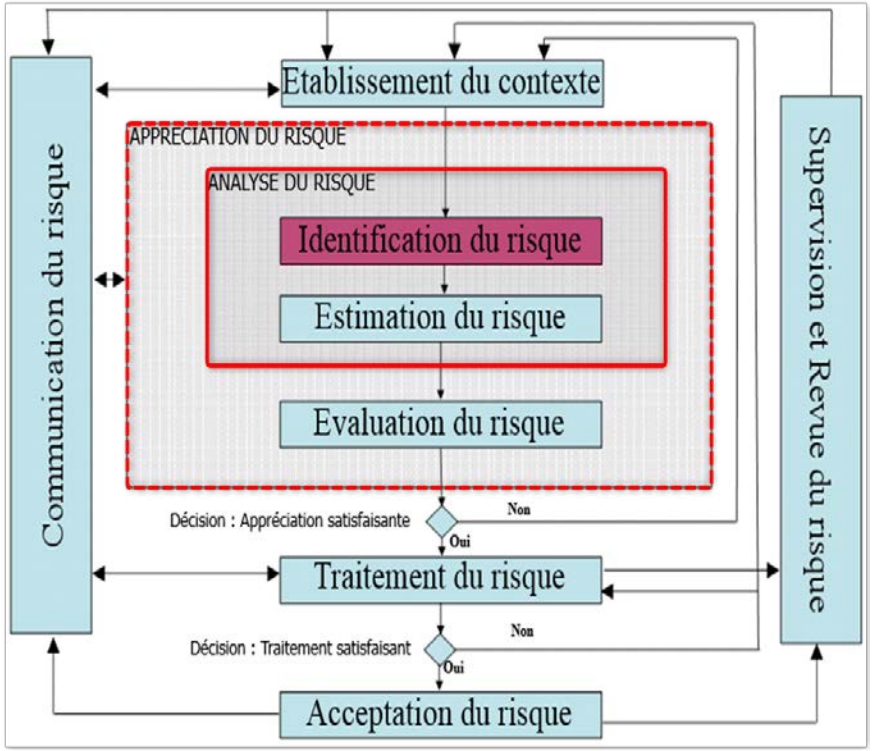
Processus de gestion des risques (ISO 27005)

2. Appréciation du risque ⇨ Analyse du risque ⇨ Identification du risque

❑ Événement - Définition

- Occurrence ou changement d'un ensemble particulier de circonstances
- <u>Remarques</u>
  - ➢ Un évènement peut être unique ou se reproduire et peut avoir plusieurs causes
  - ➢ Un évènement peut consister en quelque chose qui ne se reproduit pas
  - ➢ Un évènement peut parfois être qualifié « d'incident » ou « d'accident »

<u>Note:</u> Un événement dans le contexte de la gestion des risques peut être appelé aussi : scénario d'incident ou scénario de risque



Processus de gestion des risques (ISO 27005)

2. Appréciation du risque ⇨ Analyse du risque ⇨ Identification du risque

❑ Événement – Exemple d'un scénario d'incident

ROYAUME-UNI

Défiguration de plusieurs site web du parti conservateur

(Vital Security du 01/03/2010)

Le texte de défiguration encourage les visiteurs des sites Web de voter pour la partie travailliste. Les messages laissée par les attaquants comporte des critiques sur la sécurité des sites et slogan à caractère politique

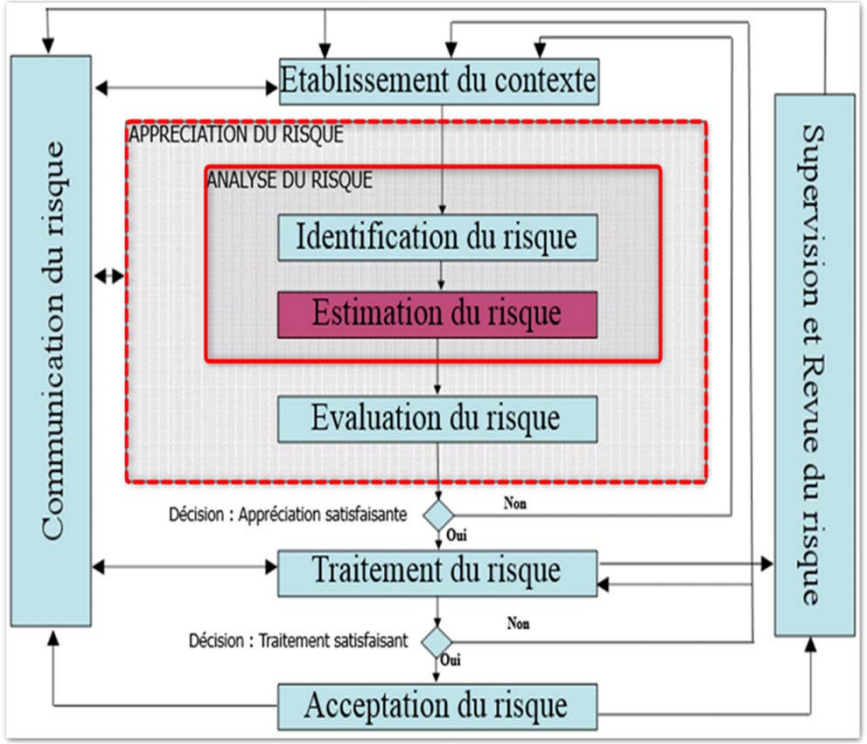
Actif primaire	Contenu du site du parti conservateur
Actif de support	Serveur hébergeant le site du parti conservateur
Critère de sécurité	Intégrité
Vulnérabilité	Failles de sécurité liées au serveur web
Menace	Hackers
Conséquence	Site web défiguré

N	Soénario d'incident		Actif impacté	C	I	A	Somme	Max	Conséquence
1	Vol de l'ordinateur du à sa portabilité	AP - 1	Processus de formation	3	1	2	6	8	Perte financière modérée
		AP -2	Processus de création du contenu	1	1	2	4		Perte d'image très importante
		AP -3	Cours - Contenu	3	3	2	8		Perte de productivité modérée
		AS - 3	Ordinateur	3	3	2	8		
		AS - 8	Cours - Format numérique	3	3	2	8		
2	Destruction de l'ordinateur du à sa portabilité	AP - 1	Processus de formation	1	2	2	5	6	Perte financière modérée
		AP -2	Processus de création du contenu	1	2	2	5		Perte d'image nulle
		AP -3	Cours - Contenu	1	2	2	5		Perte de productivité modérée
		AS - 3	Ordinateur	1	3	2	6		
		AS - 8	Cours - Format numérique	1	3	2	6		
3	L'ordinateur ne s'allume - décharge totale des batteries	AP -1	Processus de formation	1	1	3	5	5	Perte financière modérée
		AP -2	Processus de création du contenu	1	1	2	4		Perte d'image nulle
		AS - 3	Ordinateur	1	1	2	4		Perte de productivité nulle
4	Connexion frauduleuse altération du support de cours	AP - 1	Processus de formation	2	3	2	7	7	Perte financière nulle
		AP - 3	Cours - Contenu	1	3	2	6		Perte d'image très importante
		AS - 8	Cours - Format numérique	1	3	2	6		Perte de productivité modérée
5	Connexion frauduleuse vol du support par la concurrence	AP -1	Processus de formation	3	1	2	6	6	Perte financière modérée
		AP -3	Cours - Contenu	3	1	2	6		Perte d'image très importante
		AS - 8	Cours - Format numérique	3	1	1	5		Perte de productivité modérée
6	Formateur contracte la grippe	AP - 1	Processus de formation	1	1	3	5	5	Perte financière modérée
		AS - 4	Formateur	1	1	3	5		Perte d'image nulle
									Perte de productivité modérée
7	Le formateur est approché par la concurrence et démissionne	AP - 1	Processus de formation	3	1	3	7	7	Perte financière importante
		AS - 4	Formateur	1	1	3	5		Perte d'image très importante
									Perte de productivité modérée

Processus de gestion des risques (ISO 27005)

2. Appréciation du risque ⇨ Analyse du risque

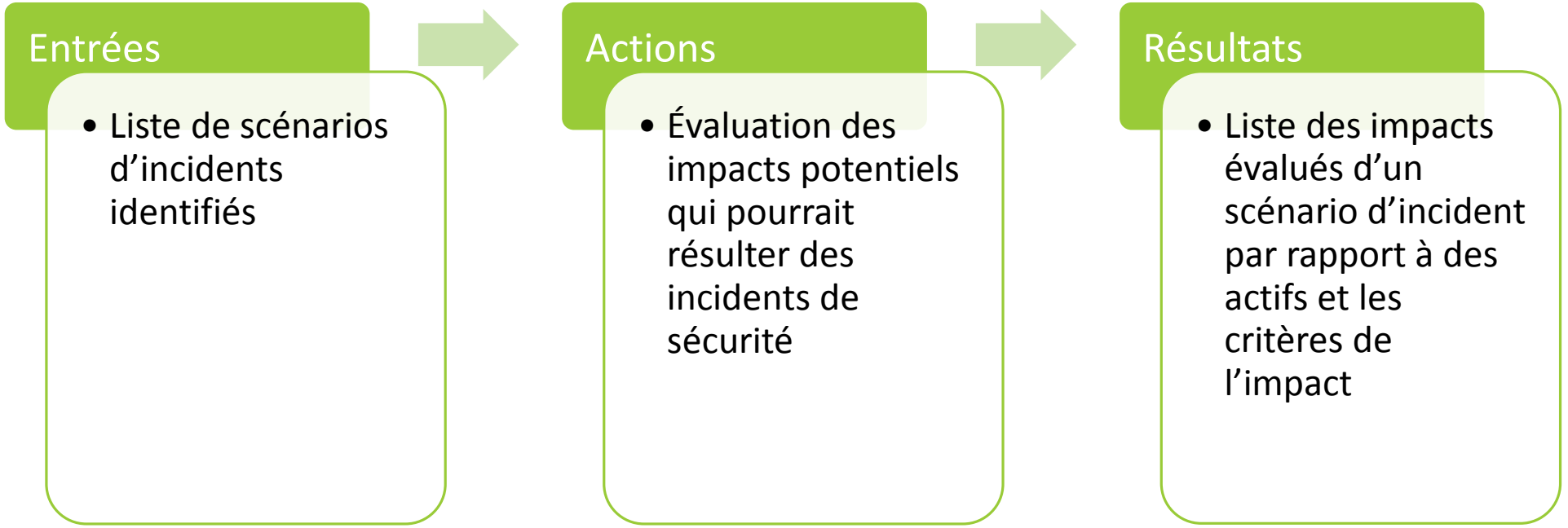
- **Estimation du risque**
  a. Estimation des impacts (conséquences)
  b. Estimation de la probabilité (vraisemblance)
  c. Estimation du niveau de risque



Processus de gestion des risques (ISO 27005)

2. Appréciation du risque ⇨ Analyse du risque ⇨ Estimation du risque

a. Estimation des impacts (conséquences)

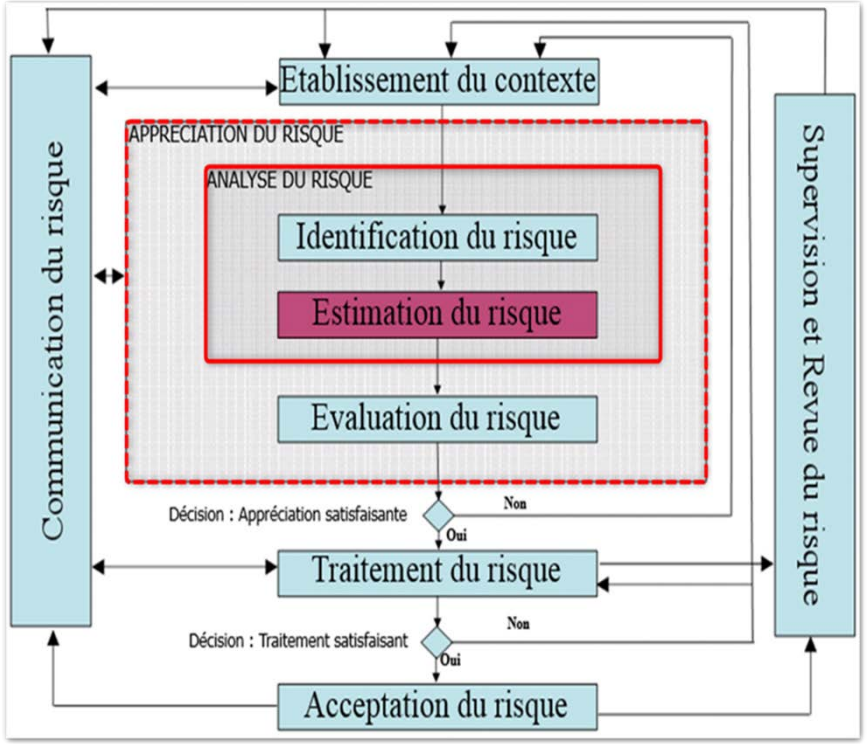


Processus de gestion des risques (ISO 27005)

2. Appréciation du risque ⇨ Analyse du risque ⇨ Estimation du risque

a. Estimation des impacts (conséquences)

- L'estimation des impacts peut être exprimé en termes qualitatifs ou quantitatifs
- La valeur d'un impact dépend généralement de la valeur et de la criticité de l'actif affecté par le scénario d'incident
- Cette estimation peut être obtenue par une analyse d'impacts des activités (« business impact analysis »)



Processus de gestion des risques (ISO 27005)

2. Appréciation du risque ⇨ Analyse du risque ⇨ Estimation du risque

❑ Facteurs à considérer pour l'estimation des impacts

Impacts directs	Impacts indirects
▪ Valeur financière de remplacement de la perte de l'actif ▪ Coût de remplacement, d'installation et/ou de configuration de remplacement de l'actif ▪ Coût d'interruption des opérations durant l'incident ▪ Résultats de l'impact de l'incident de sécurité	▪ Coût des opportunités perdues ▪ Coût d'interruption des opérations causée par l'incident ▪ Perte de revenus causée par une utilisation frauduleuse d'information volées lors d'un incident de sécurité ▪ Violation d'obligations légales ou contractuelles ▪ Violation du code éthique

Processus de gestion des risques (ISO 27005)

2. Appréciation du risque ⇨ Analyse du risque ⇨ Estimation du risque

❑ Estimation des impacts (conséquences)

Exemple d'échelle

Valeur	Description
0	Négligeable
1	Faible
2	Moyen
3	Important

Valeur	Confidentialité	Intégrité	Disponibilité
1	Perte faible	Perte faible	Perte faible
2	Perte moyenne	Perte moyenne	Perte moyenne
3	Perte élevée	Perte élevée	Perte élevée

N.	Soénario d'incident		Actif impacté	C	I	A	Somme	Max	Conséquence	Mesure sécurité	Valeur Conséquence
1	Vol de l'ordinateur du à sa portabilité	AP - 1	Processus de formation	3	1	2	6	8	Perte financière modérée		2
		AP -2	Processus de création du contenu	1	1	2	4		Perte d'image très importante		3
		AP -3	Cours - Contenu	3	3	2	8		Perte de productivité modérée		2
		AS - 3	Ordinateur	3	3	2	8				
		AS - 8	Cours - Format numérique	3	3	2	8				
2	Destruction de l'ordinateur du à sa portabilité	AP - 1	Processus de formation	1	2	2	5	6	Perte financière modérée		2
		AP -2	Processus de création du contenu	1	2	2	5		Perte d'image nulle		1
		AP -3	Cours - Contenu	1	2	2	5		Perte de productivité modérée		2
		AS - 3	Ordinateur	1	3	2	6				
		AS - 8	Cours - Format numérique	1	3	2	6				
3	L'ordinateur ne s'allume - décharge totale des batteries	AP - 1	Processus de formation	1	1	3	5	5	Perte financière modérée		
		AP - 2	Processus de création du contenu	1	1	2	4		Perte d'image nulle		1
		AS - 3	Ordinateur	1	1	2	4		Perte de productivité nulle		1
4	Connexion frauduleuse altération du support de cours	AP -1	Processus de formation	2	3	2	7		Perte financière nulle	identifiant / mot de passe	1
		AP -3	Cours - Contenu	1	3	2	6		Perte d'image très importante		3
		AS -8	Cours - Format numérique	1	3	2	6		Perte de productivité modérée		2
5	Connexion frauduleuse vol du support par la concurrence	AP -1	Processus de formation	3	1	2	6	6	Perte financière modérée	identifiant / mot de passe	2
		AP -3	Cours - Contenu	3	1	2	6		Perte d'image très importante		3
		AS -8	Cours - Format numérique	3	1	1	5		Perte de productivité modérée		2
6	Formateur contracte la grippe	AP - 1	Processus de formation	1	1	3	5	5	Perte financière modérée		2
		AS - 4	Formateur	1	1	3	5		Perte d'image nulle		1
									Perte de productivité modérée		2
7	Le formateur est approché par la concurrence et démissionne	AP - 1	Processus de formation	3	1	3	7	7	Perte financière importante		3
		AS - 4	Formateur	1	1	3	5		Perte d'image très importante		3
									Perte de productivité modérée		2

Processus de gestion des risques (ISO 27005)

2. Appréciation du risque ⇨ Analyse du risque ⇨ Estimation du risque

b. Estimation de la probabilité (vraisemblance)

Entrées

- Liste de scénarios d'incident identifiés avec conséquences sur l'actif et le processus métier

Actions

- Évaluation de la probabilité des scénarios d'incidents identifiés

Résultats

- Probabilité des scénarios d'incidents (Qualitatif ou quantitatifs)

Processus de gestion des risques (ISO 27005)

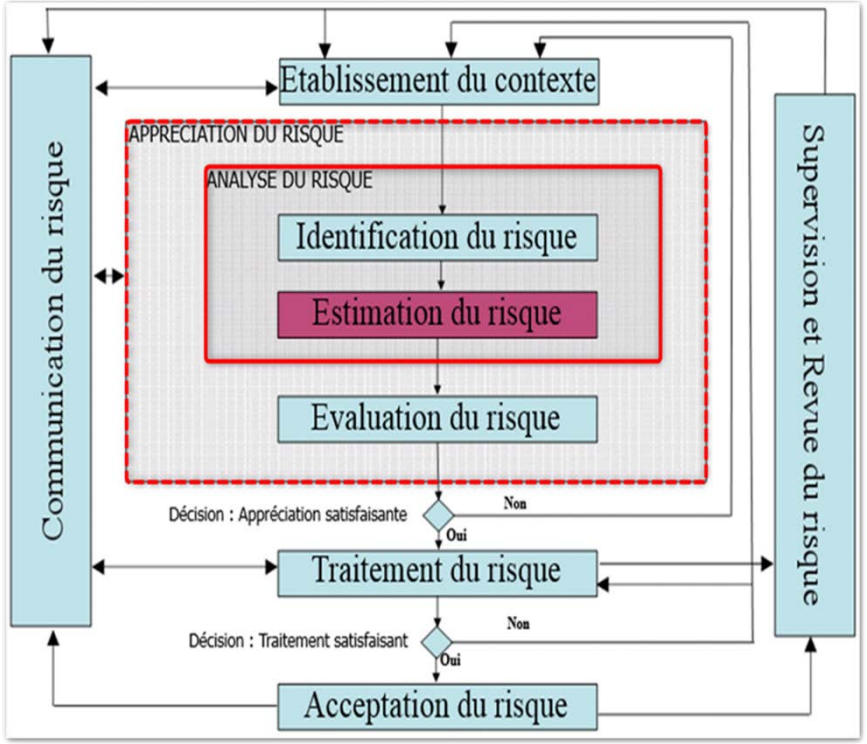
2. Appréciation du risque ⇨ Analyse du risque ⇨ Estimation du risque

b. Estimation de la probabilité (vraisemblance)

- **Vraisemblance**: Possibilité que quelque chose se produise

Remarques:

- Dans la terminologie du management du risque, le mot « vraisemblance » est utiliser pour indiquer la possibilité que quelque chose se produise, que cette possibilité soit définie, mesurée ou déterminer de façon objective ou subjective, qualitative ou quantitative



Processus de gestion des risques (ISO 27005)

2. Appréciation du risque ⇨ Analyse du risque ⇨ Estimation du risque

❑ Probabilité d'incident

Exemple d'échelle

Niveau	Description	Probabilité
0	Très rare	Moins d'une fois par 100 ans
1	Rare	Une fois tous les 10 ans en moyenne
2	Peu plausible	Une fois tous les 3 ans en moyenne
3	Plausible	Une fois par année en moyenne
4	Très plausible	Plusieurs fois par année
5	Peu courant	Plusieurs fois par mois
6	Courant	Plusieurs fois par semaine
7	Très courant	Plusieurs fois par jour

Processus de gestion des risques (ISO 27005)

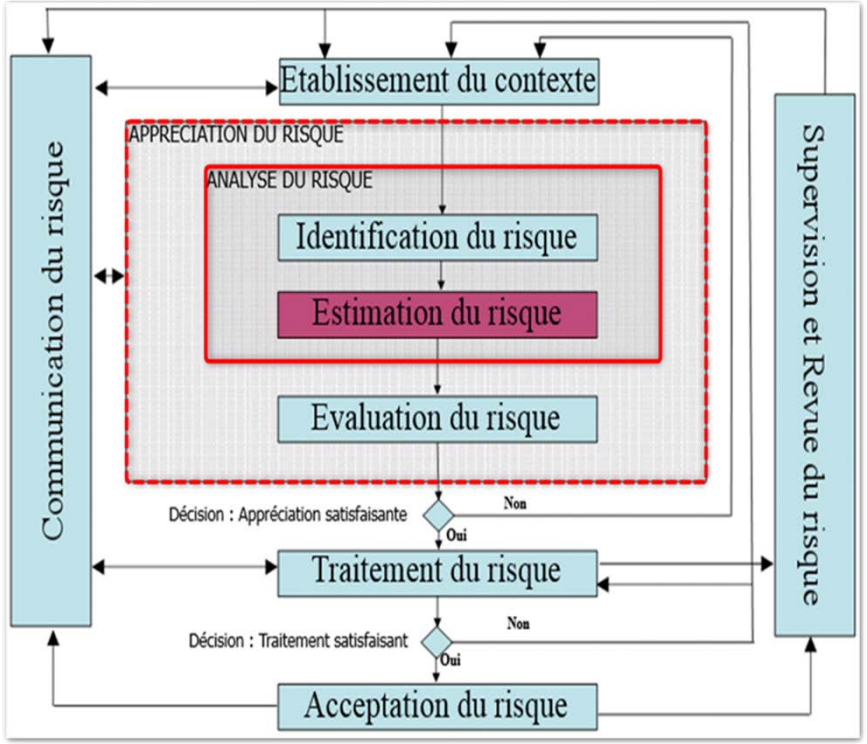
2. Appréciation du risque ⇨ Analyse du risque ⇨ Estimation du risque

b. Estimation de la probabilité (vraisemblance)

Exemple de calcul

- L'année dernière, une organisation a enregistrée 730 incidents liée à l'oubli d'un mot de passe
- 730 incidents / 365 jours = 2
- La probabilité de ce scénario d'incident pour l'organisation est d'une:

moyenne de 2 par jour



N.	Scénario d'incident		Actif impacté	C	I	A	Somme	Max	Conséquence	Mes. Séc.	Valeur Conséquence	Vrais.
1	Vol de l'ordinateur du à sa portabilité	AP - 1	Processus de formation	3	1	2	6	Perte d'image très importante 8	Perte financière modérée		2	2
		AP - 2	Processus de création du contenu	1	1	2	4				3	
		AP - 3	Cours - Contenu	3	3	2	8		Perte de productivité modérée		2	
		AS - 3	Ordinateur	3	3	2	8					
		AS - 8	Cours - Format numérique	3	3	2	8					
2	Destruction de l'ordinateur du à sa portabilité	AP - 1	Processus de formation	1	2	2	5	Perte d'image nulle 6	Perte financière modérée		2	2
		AP - 2	Processus de création du contenu	1	2	2	5				1	
		AP - 3	Cours - Contenu	1	2	2	5		Perte de productivité modérée		2	
		AS - 3	Ordinateur	1	3	2	6					
		AS - 8	Cours - Format numérique	1	3	2	6					
3	L'ordinateur ne s'allume - décharge totale des batteries	AP - 1	Processus de formation	1	1	3	5	5	Perte financière modérée			3
		AP - 2	Processus de création du contenu	1	1	2	4		Perte d'image nulle		1	
		AS - 3	Ordinateur	1	1	2	4		Perte de productivité nulle		1	
4	Connexion frauduleuse altération du support de cours	AP - 1	Processus de formation	2	3	2	7		Perte financière nulle	identifiant mot de passe	1	3
		AP - 3	Cours - Contenu	1	3	2	6		Perte d'image très importante		3	
		AS - 8	Cours - Format numérique	1	3	2	6		Perte de productivité modérée		2	
5	Connexion frauduleuse vol du support par la concurrence	AP - 1	Processus de formation	3	1	2	6	6	Perte financière modérée	identifiant mot de passe	2	1
		AP - 3	Cours - Contenu	3	1	2	6		Perte d'image très importante		3	
		AS - 8	Cours - Format numérique	3	1	1	5		Perte de productivité modérée		2	
6	Formateur contracte la grippe	AP - 1	Processus de formation	1	1	3	5	5	Perte financière modérée		2	1
		AS - 4	Formateur	1	1	3	5		Perte d'image nulle		1	
									Perte de productivité modérée		2	
7	Le formateur est approché par la concurrence et démissionne	AP - 1	Processus de formation	3	1	3	7	7	Perte financière importante		3	1
		AS - 4	Formateur	1	1	3	5		Perte d'image très importante		3	
									Perte de productivité modérée		2	

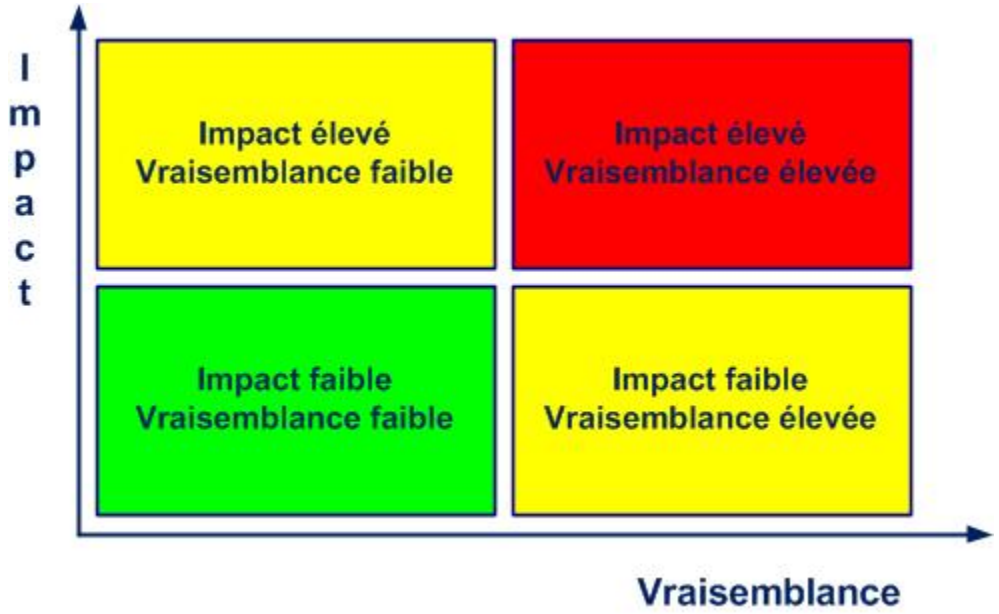
Processus de gestion des risques (ISO 27005)

2. Appréciation du risque ⇨ Analyse du risque ⇨ Estimation du risque

❑ Niveau de risque - Définition

- Importance d'un risque ou combinaison de risques, exprimée en terme de combinaison des conséquences et de leur vraisemblance:

RISQUE = IMPACT (Conséquence) * VRAISEMBLENCE (Probabilité)



Processus de gestion des risques (ISO 27005)

2. Appréciation du risque ⇨ Analyse du risque ⇨ Estimation du risque

c. Estimation du niveau (valeur) du risque

Entrées

- Liste de scénarios d'incident avec leurs conséquences liées aux l'actif et aux processus métier et de leur probabilité

Actions

- Évaluation du niveau de risque pour tous les scénarios d'incident

Résultats

- Liste de risques avec les niveaux de valeur attribués

Processus de gestion des risques (ISO 27005)

2. Appréciation du risque ⇨ Analyse du risque ⇨ Estimation du risque

- Exemple de matrice d'estimation du risque

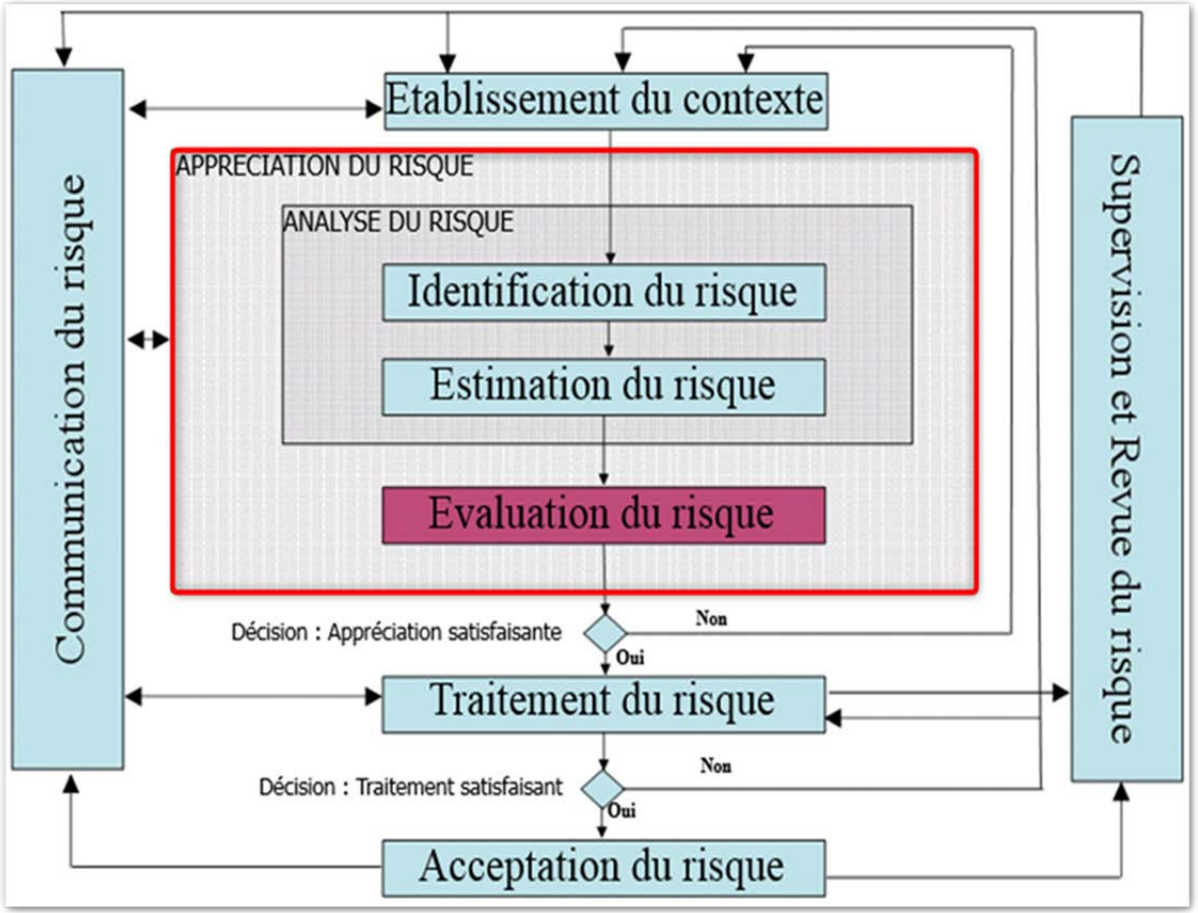
Vraisemblance

Impact	Très faible occurrence	Faible occurrence	Occurrence moyenne	Forte occurrence	Très forte occurrence
Conséquence très faible	0	1	2	3	4
Conséquence faible	1	1	2	3	4
Conséquence moyenne	2	2	4	6	8
Conséquence forte	3	3	6	9	12
Conséquence très forte	4	4	8	12	16

Processus de gestion des risques (ISO 27005)

2. Appréciation du risque

- **Évaluation du risque**



Processus de gestion des risques (ISO 27005)

2. Appréciation du risque

❑ Évaluation du risque

Entrées

- Liste de risques avec leur valeur attribuée de niveau de risque et des critères d'évaluation

Actions

- Évaluation du niveau de risque en fonction des critères d'évaluation et d'acceptation des risques

Résultats

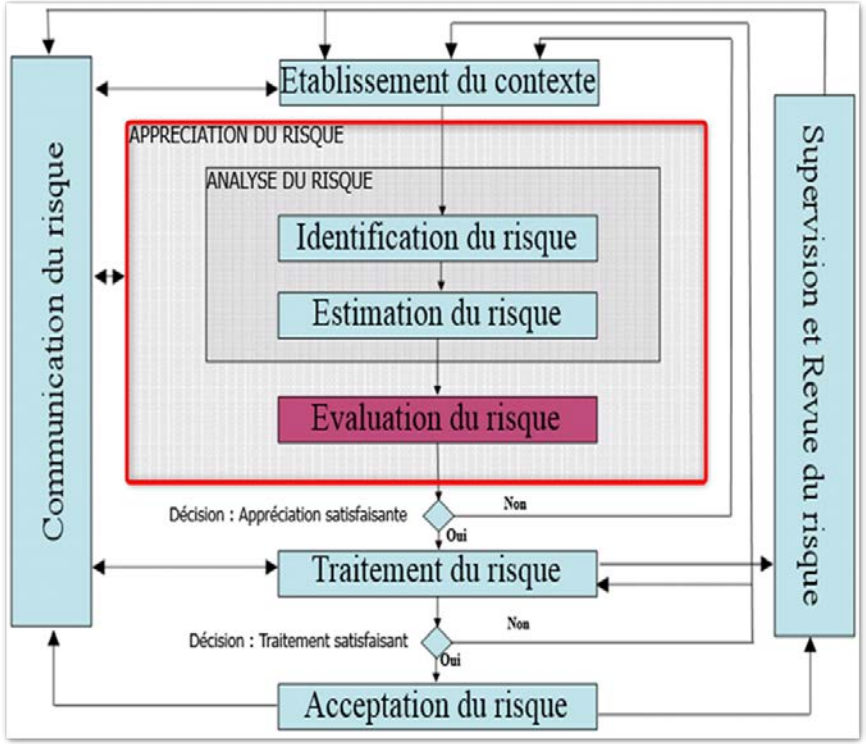
- Liste de risques classés par ordre de priorité en fonction de critères d'évaluation des risques

Processus de gestion des risques (ISO 27005)

2. Appréciation du risque ⇨ Évaluation du risque

❑ Lignes directrices pour l'évaluation du risque

- La nature des décisions relatives à l'évaluation des risques et les critères d'évaluation des risques qui seront utilisés pour prendre ces décisions ont été définis lors de l'établissement de contexte
- A cette étape, ces décisions et le contexte doivent être revus en détail au regard des risques identifiés
- Afin d'évaluer les risques, il convient que les organisation comparent les risques estimés aux critères d'évaluation des risques définis lors de l'établissement de contexte



Processus de gestion des risques (ISO 27005)

2. Appréciation du risque ⇨ Évaluation du risque

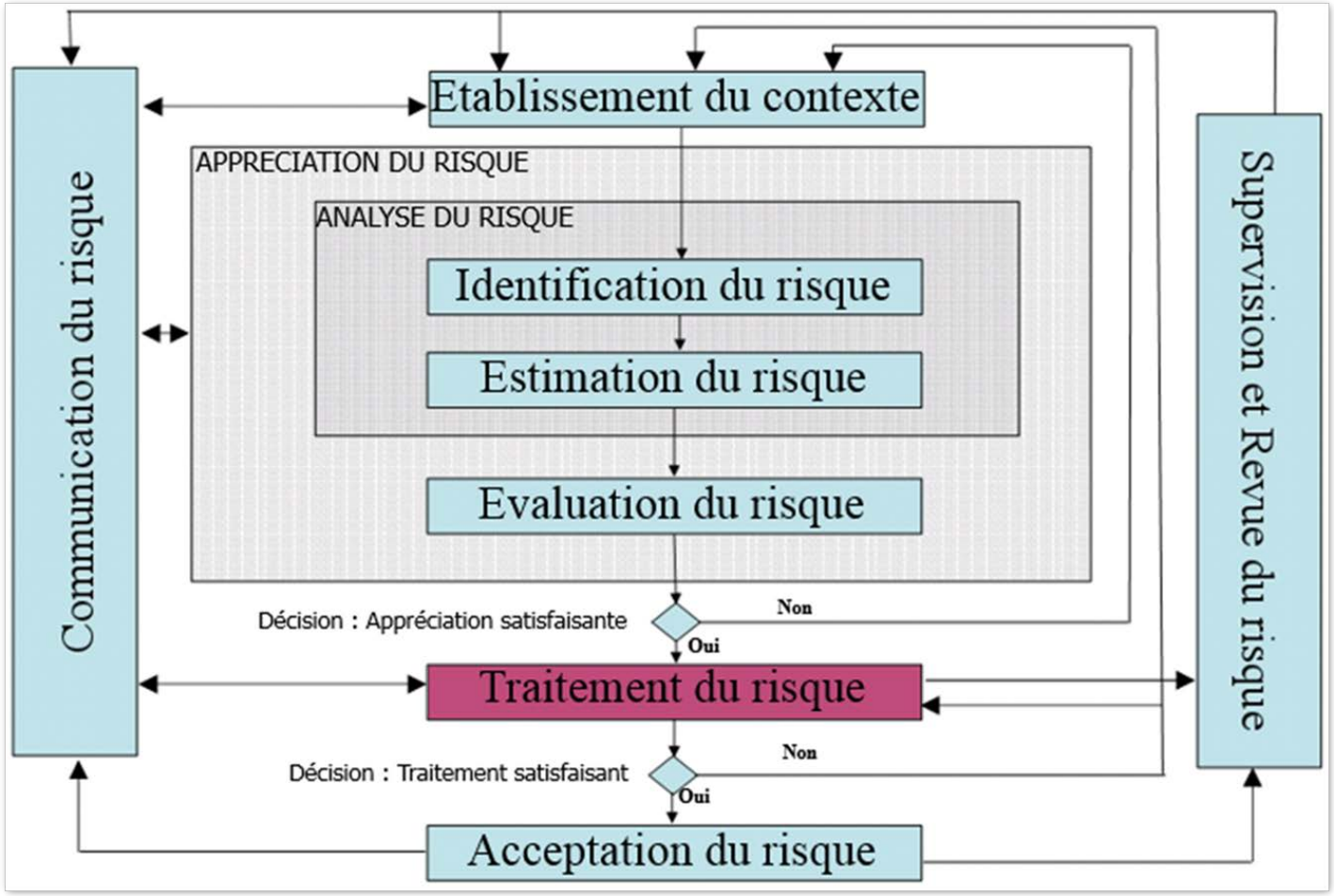
❑ Exemple d'évaluation du risque

Menace	Valeur conséquences sur l'actif	Probabilité d'occurrence de la menace	Mesure du risque	Ordre de priorité
Scénario A	5	2	10	2
Scénario B	2	4	8	3 ou 4
Scénario C	3	5	15	1
Scénario D	1	3	3	6
Scénario E	4	1	4	5
Scénario F	2	4	8	3 ou 4

N	Scénario d'incident		Actif impacté	C	I	A	Somme	Max	Conséquence	Mes. Séc.	Valeur Conséquence	Vrais.	Niv Risq.
1	Vol de l'ordinateur du à sa portabilité	AP - 1	Processus de formation	3	1	2	6	8	Perte financière modérée		2	2	16
		AP - 2	Processus de création du contenu	1	1	2	4		Perte d'image très importante		3		
		AP - 3	Cours - Contenu	3	3	2	8		Perte de productivité modérée		2		
		AS - 3	Ordinateur	3	3	2	8						
		AS - 8	Cours - Format numérique	3	3	2	8						
2	Destruction de l'ordinateur du à sa portabilité	AP - 1	Processus de formation	1	2	2	5	6	Perte financière modérée		2	2	12
		AP - 2	Processus de création du contenu	1	2	2	5		Perte d'image nulle		1		
		AP - 3	Cours - Contenu	1	2	2	5		Perte de productivité modérée		2		
		AS - 3	Ordinateur	1	3	2	6						
		AS - 8	Cours - Format numérique	1	3	2	6						
3	L'ordinateur ne s'allume - décharge totale des batteries	AP - 1	Processus de formation	1	1	3	5	5	Perte financière modérée			3	15
		AP - 2	Processus de création du contenu	1	1	2	4		Perte d'image nulle		1		
		AS - 3	Ordinateur	1	1	2	4		Perte de productivité nulle		1		
4	Connexion frauduleuse altération du support de cours	AP - 1	Processus de formation	2	3	2	7		Perte financière nulle	identifiant mot de passe	1	3	18
		AP - 3	Cours - Contenu	1	3	2	6		Perte d'image très importante		3		
		AS - 8	Cours - Format numérique	1	3	2	6		Perte de productivité modérée		2		
5	Connexion frauduleuse vol du support par la concurrence	AP - 1	Processus de formation	3	1	2	6	6	Perte financière modérée	identifiant mot de passe	2	1	6
		AP - 3	Cours - Contenu	3	1	2	6		Perte d'image très importante		3		
		AS - 8	Cours - Format numérique	3	1	1	5		Perte de productivité modérée		2		
6	Formateur contracte la grippe	AP - 1	Processus de formation	1	1	3	5	5	Perte financière modérée		2	1	5
		AS - 4	Formateur	1	1	3	5		Perte d'image nulle		1		
									Perte de productivité modérée		2		
7	Le formateur est approché par la concurrence et démissionne	AP - 1	Processus de formation	3	1	3	7	7	Perte financière importante		3	1	7
		AS - 4	Formateur	1	1	3	5		Perte d'image très importante		3		
									Perte de productivité modérée		2		

Processus de gestion des risques (ISO 27005)

3. Traitement du risque



Processus de gestion des risques (ISO 27005)

3. Traitement du risque

❑ Différentes zones de risque

- Risque (occurrence **faible** - impact **faible**)

⇒ **Négligeable**,

- Risque (occurrence **forte** - impact **faible**)

⇒ **Acceptable**,

- Risque (occurrence **faible** - impact **important**)

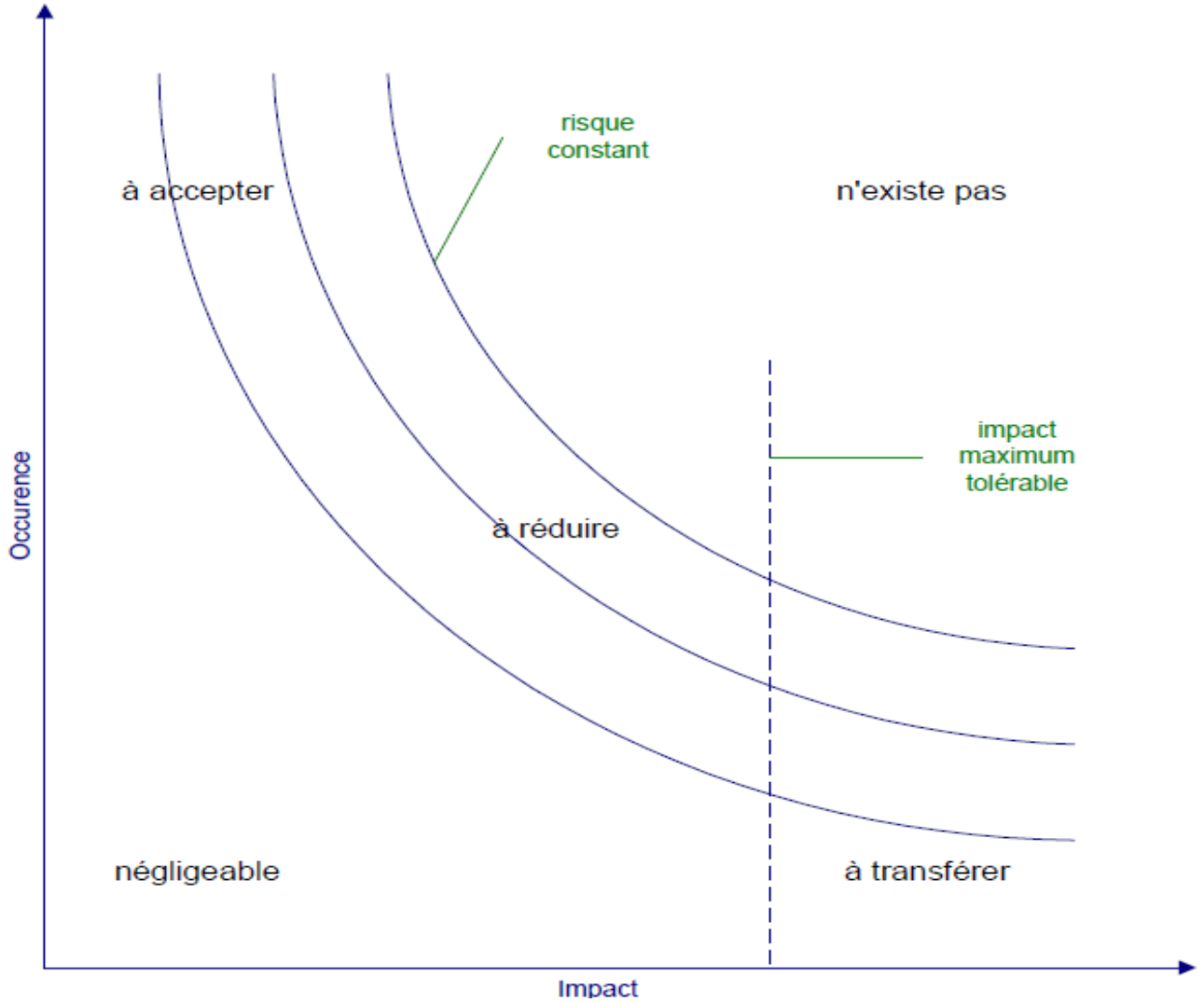
⇒ **A transférer**,

- Risque (occurrence **forte** - impact **important**)

⇒ **A éviter** (ne doit pas exister),

- Autres risques

⇒ **A réduire**.



Processus de gestion des risques (ISO 27005)

3. Traitement du risque

3.1 Sélection des options de traitement du risque

Entrées

- Liste de risques classés par ordre de priorité en fonction des critères d'évaluation du risque

Actions

- Choisir les mesures pour réduire, conserver, éviter, ou pour transférer le risque

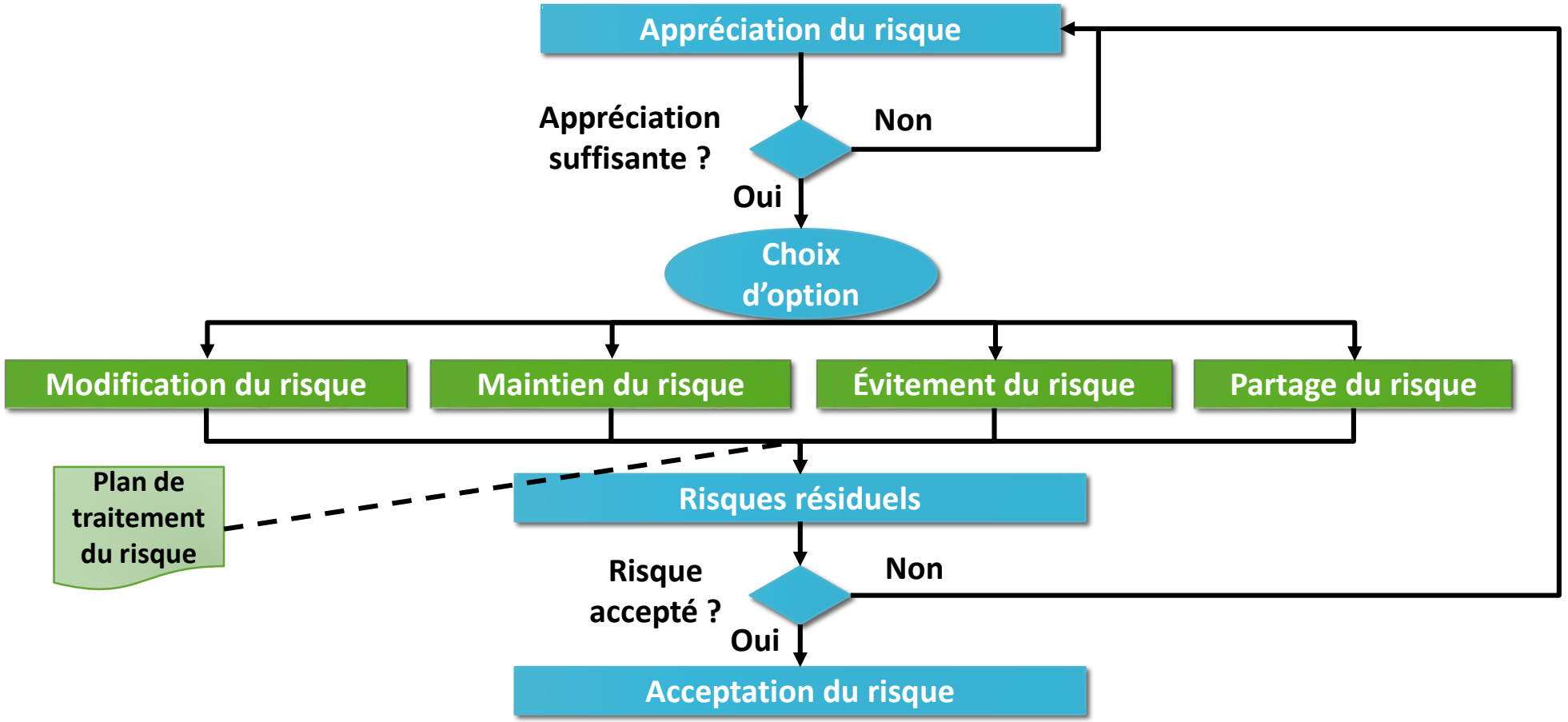
Résultats

- Plan de traitement des risques
- Liste des risques résiduels

Processus de gestion des risques (ISO 27005)

3. Traitement du risque

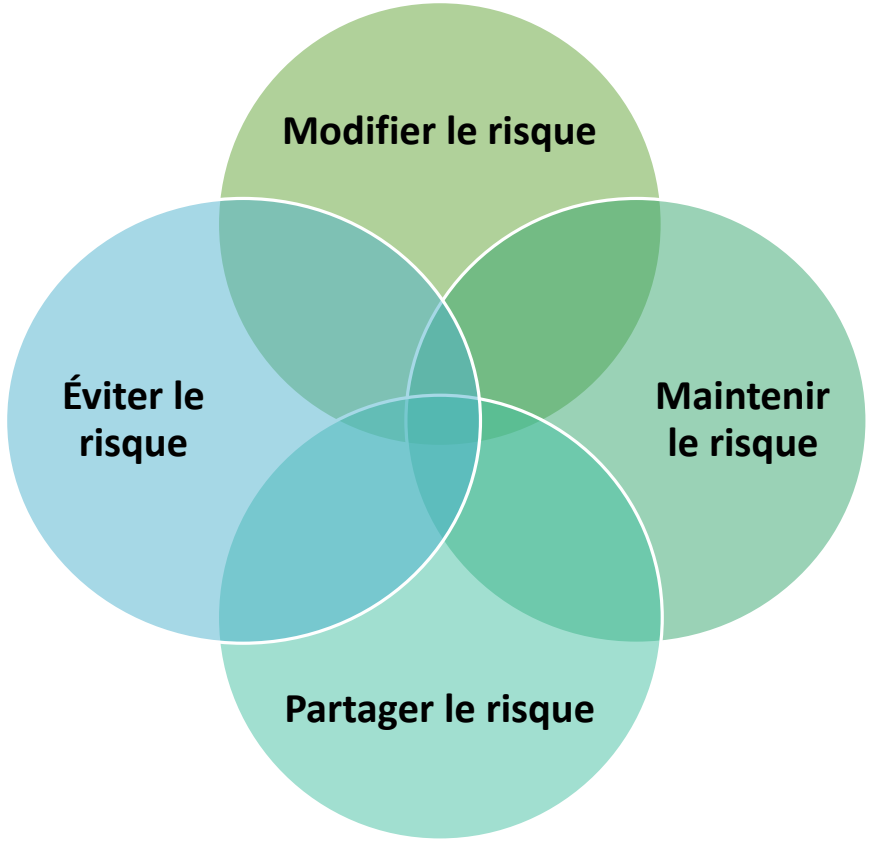
❑ Processus de traitement et d'acceptation du risque



Processus de gestion des risques (ISO 27005)

3. Traitement du risque

❑ Évaluation des options de traitement



Modifier le risque

- Mesurer la sécurité sélectionnées pour diminuer le risque

Maintenir le risque

- La direction décide d'assumer le risque

Partager le risque

- Décision de partager certains risques avec des parties externes: assurance ou infogérance

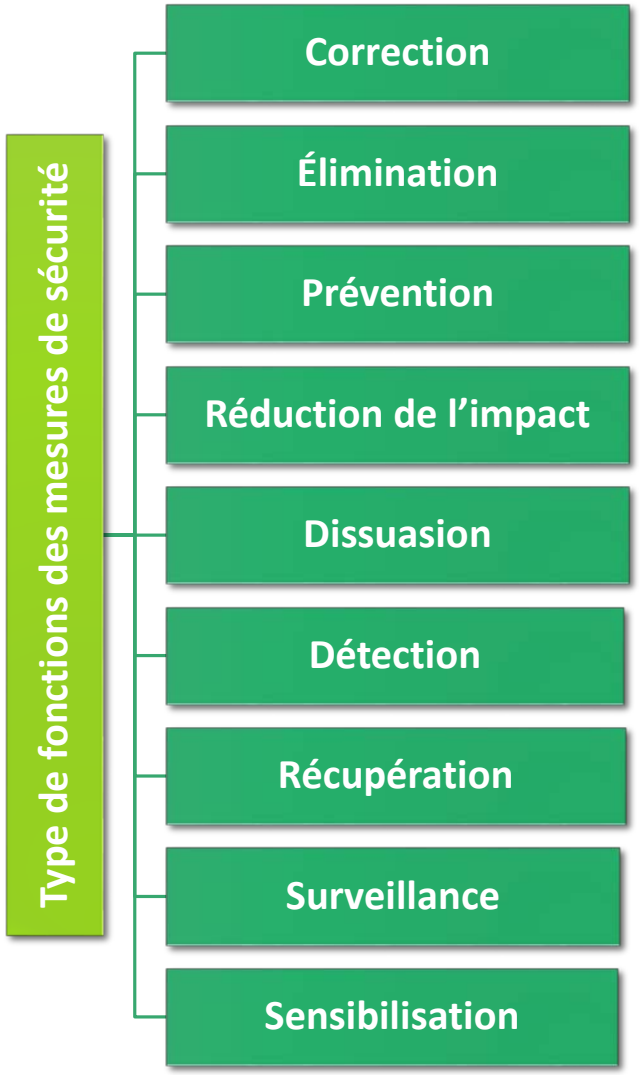
Éviter le risque

- Annulation ou modification d'une activité ou d'un ensemble d'activités liés au risque

Processus de gestion des risques (ISO 27005)

3. Traitement du risque

- **La modification du risque**
  - Le niveau de risque devrait être réduit par la sélection des mesures de sécurité afin que le risque résiduel puisse être réévalué comme étant acceptable

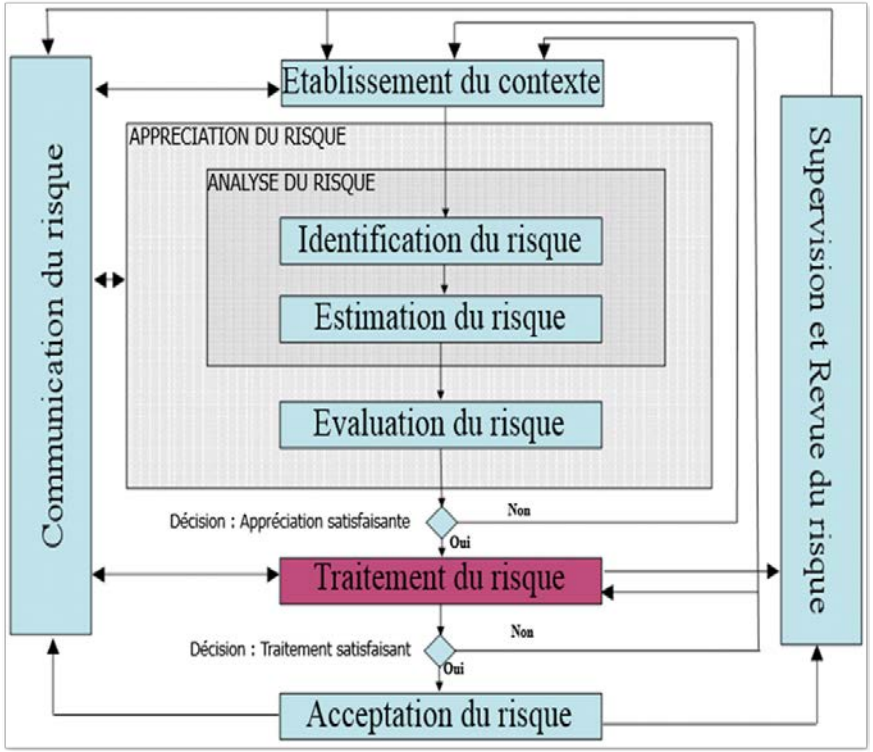


Processus de gestion des risques (ISO 27005)

3. Traitement du risque

❑ Le maintien du risque

- Si niveau de risque répond aux critères d'acceptation des risques, il n'est pas nécessairement de mettre en œuvre des mesures de sécurité supplémentaires et le risque peut être accepté de *facto*
- Le maintien du risque actuel doit cependant être documenté



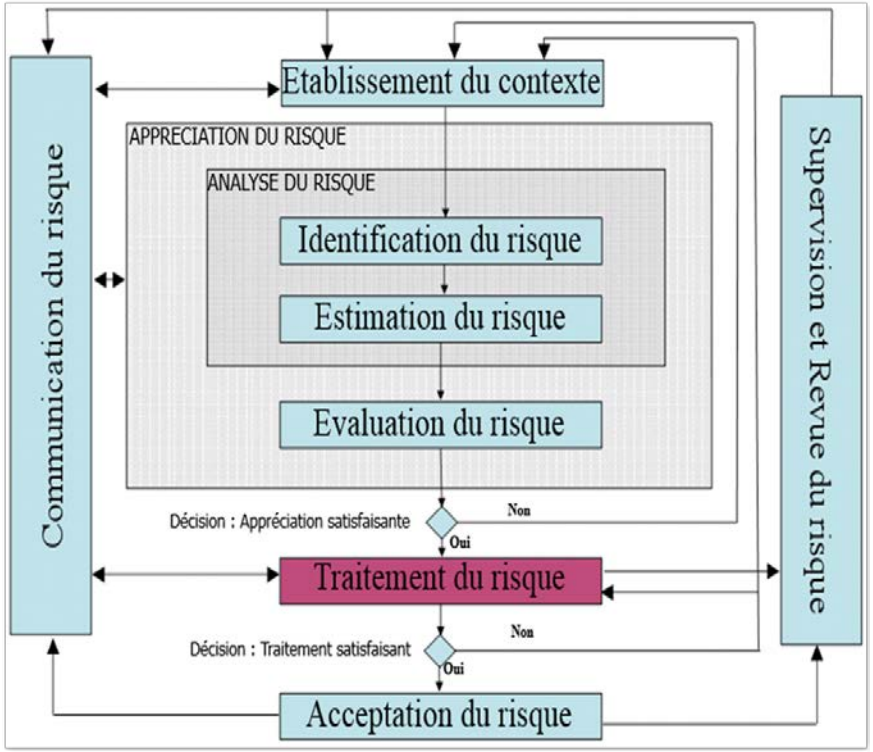
Processus de gestion des risques (ISO 27005)

3. Traitement du risque

❑ L'évitement du risque

- Lorsque les scénarios de risque identifiés sont considérés trop élevés, une décision peut être prise pour éviter le risque entièrement:
  - Par l'annulation d'une activité ou d'un ensemble d'activités
  - Ou par la modification des conditions en vertu desquelles l'activité est exploitée

Exemple: On évite les risques d'accidents lors d'une tempête en travaillant à domicile



Processus de gestion des risques (ISO 27005)

3. Traitement du risque

- **L'évitement du risque**

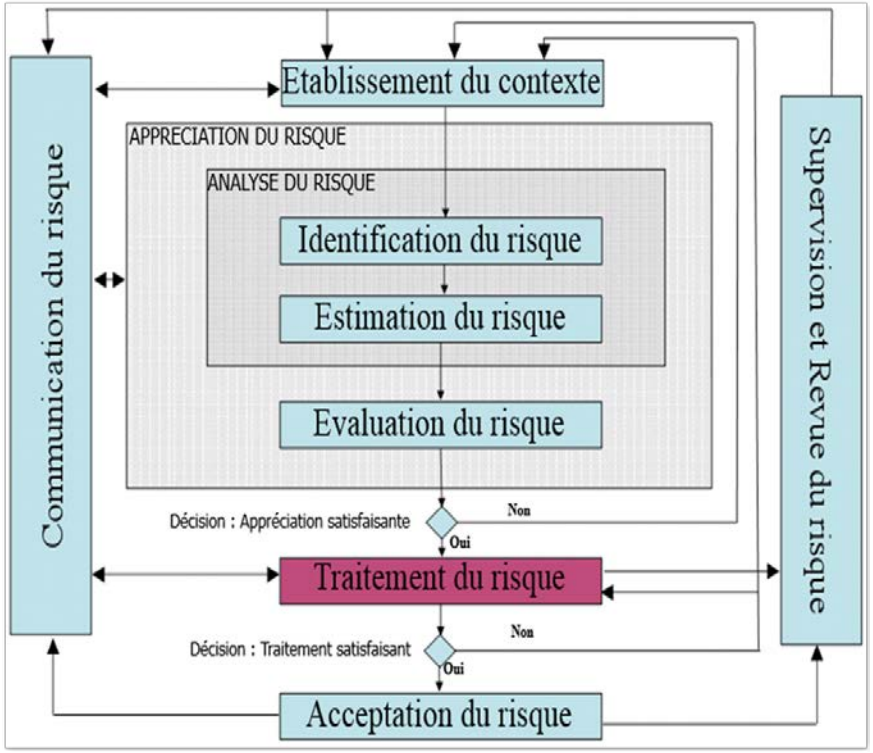
Exemples

1. En arrêtant certaines activités (arrêter d'utiliser internet dans un centre de recherche)
2. En enlevant les actifs d'une zone à risque (déménager les serveurs au 4e étage afin d'éviter un risque d'inondation)
3. En décidant de ne pas échanger des information sensible (avec des tiers parties) si une protection suffisante n'est pas garantie

Processus de gestion des risques (ISO 27005)

3. Traitement du risque

- **Le partage du risque**
  - Le risque peut être transféré à une autre partie qui peut le gérer très efficacement
  - C'est la meilleur option quand:
  - Il est difficile pour une organisation de réduire le risque à un niveau acceptable
  - L'organisme n'a pas l'expertise pour le gérer
  - Il est plus économique de le transférer à une tierce partie



Processus de gestion des risques (ISO 27005)

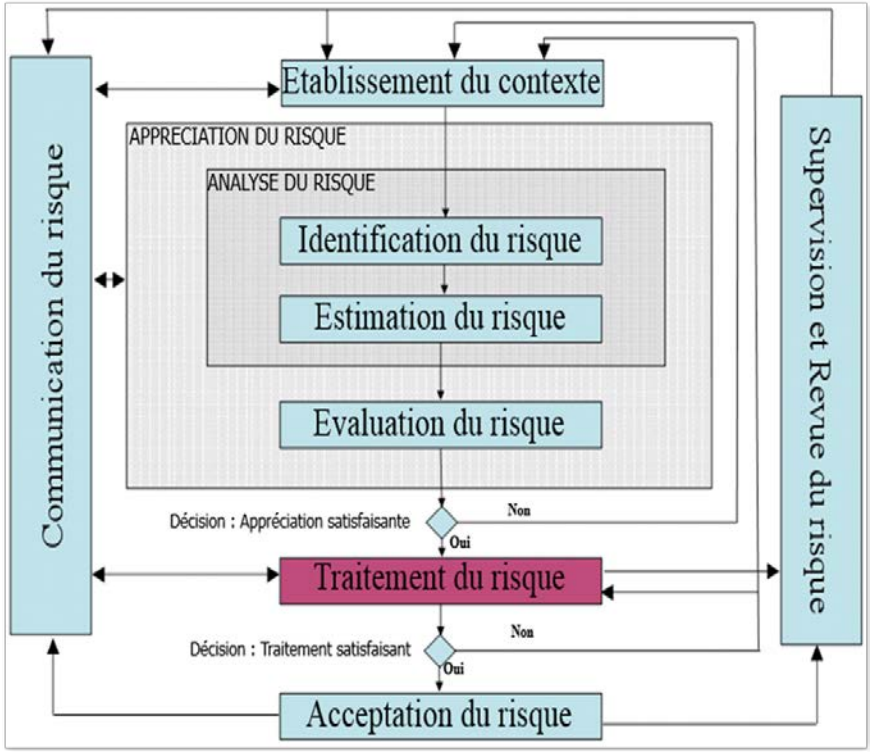
3. Traitement du risque

- **Le partage du risque**

Méthodes possibles

- Il existe deux grandes méthodes de transfert de risque:

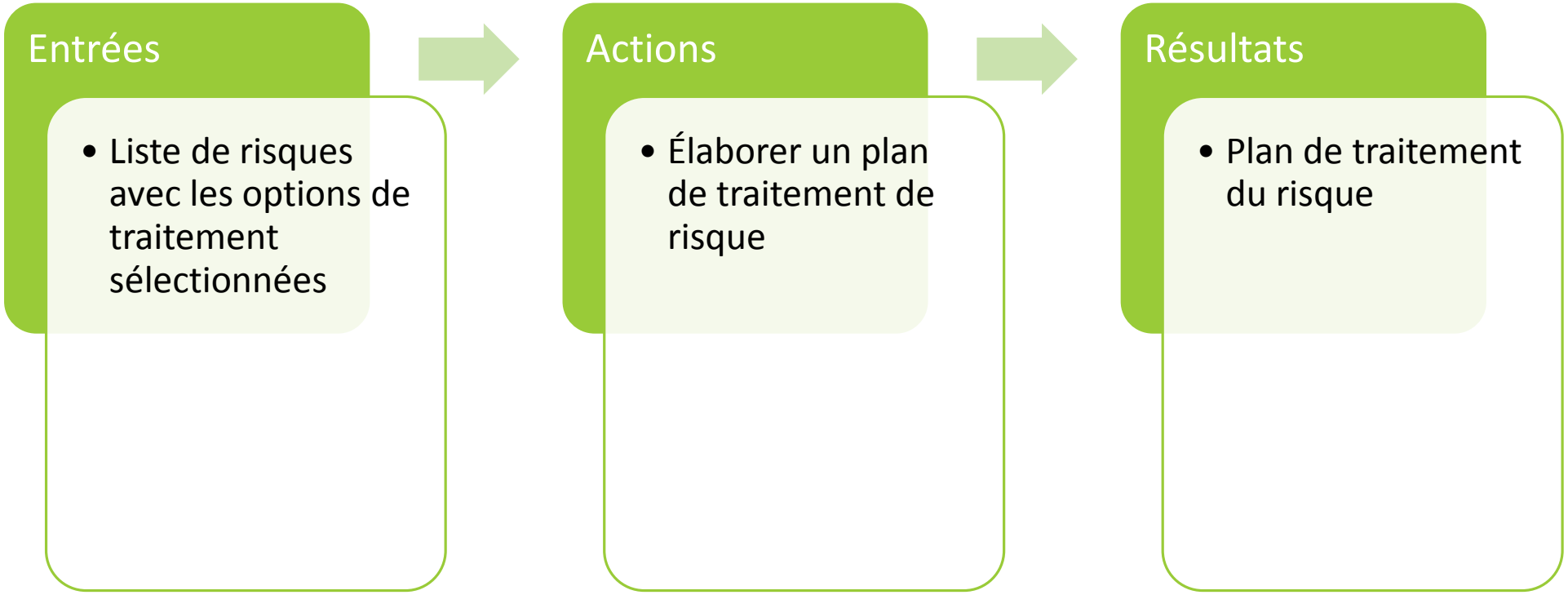
1. **L'assurance**: Toute autre forme de couverture de risque contractée par une organisation en échange du paiement d'une prime
2. **L'externalisation (outsourcing)**: Transfert de tout ou partie d'une fonction d'une entreprise vers un partenaire externe



Processus de gestion des risques (ISO 27005)

3. Traitement du risque

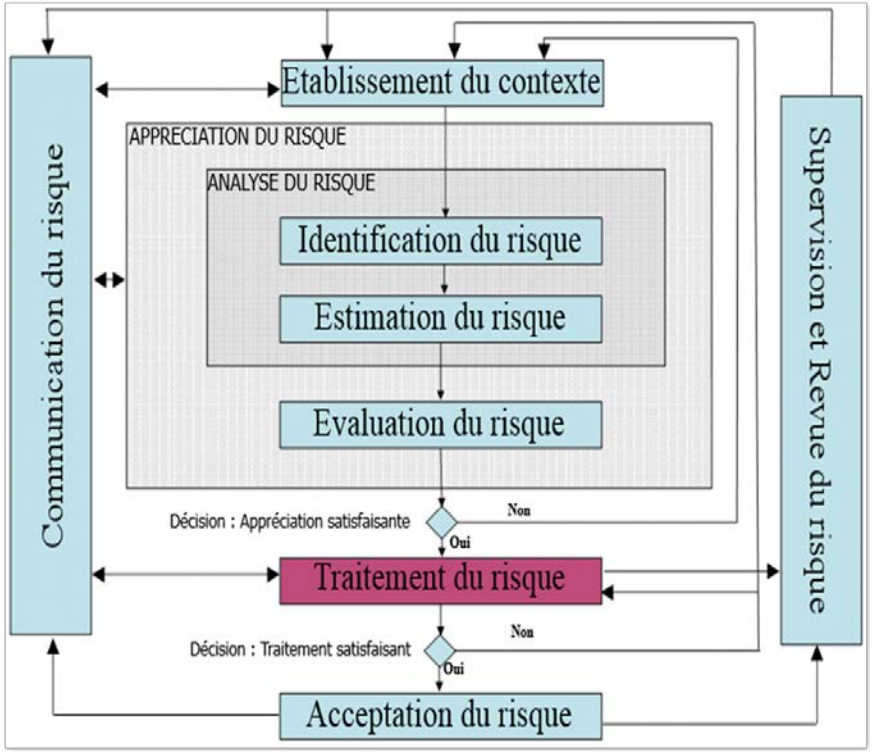
3.2 Élaboration du plan de traitement du risque



Processus de gestion des risques (ISO 27005)

3. Traitement du risque

- **Le plan de traitement du risque**
  - Identifier et planifier les activités de traitement du risque
  - Les activités doivent être classées par ordre de priorité
  - Les ressources nécessaires doivent être allouées au plan de traitement



Processus de gestion des risques (ISO 27005)

3. Traitement du risque

❑ Plan de traitement du risque

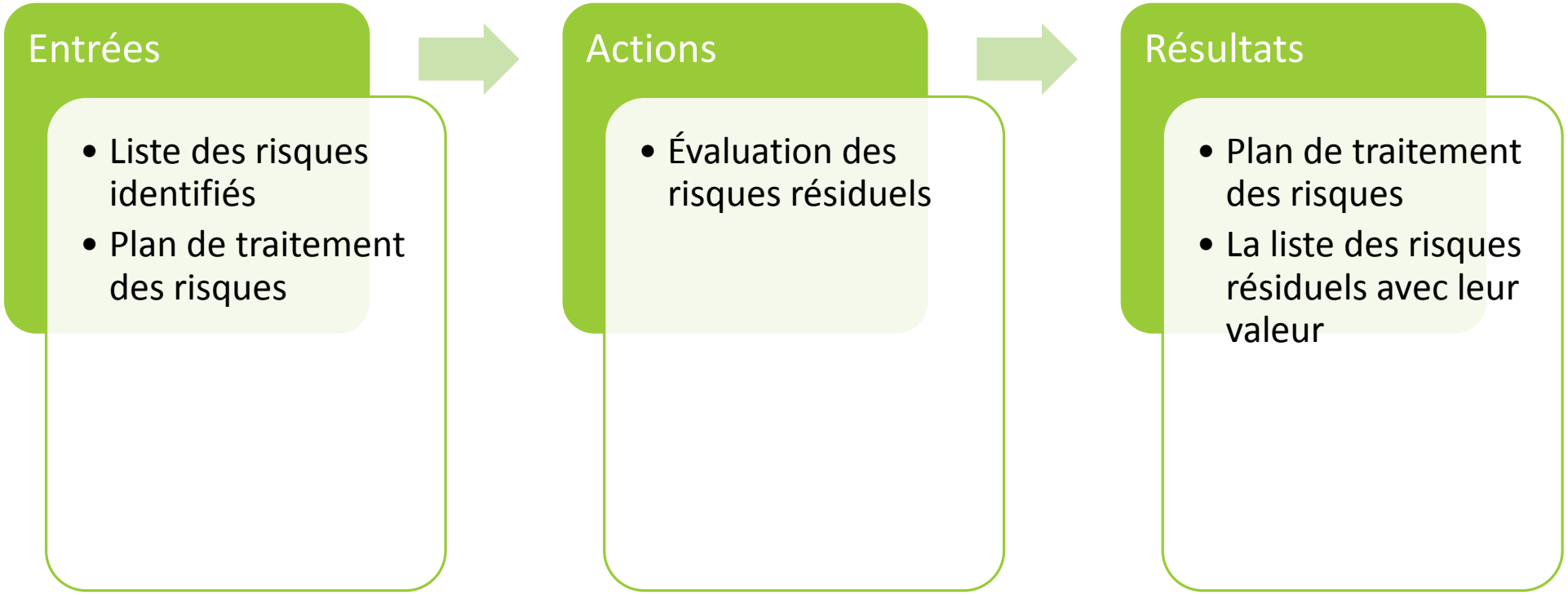
Exemple

Risque (Paire Vulnérabilité/Menace)	Niveau de risque	Degré de priorité	Option de traitement	Détail de la mesure	Ressources nécessaires	Responsable	Date de début/date de fin	Maintenance nécessaire/ commentaires
Des utilisateurs non autorisés peuvent se connecter via l'extranet sur Sharepoint et rechercher des fichiers sensibles de l'organisme avec l'ID invité	6	Haut	Évitement	Rendre inaccessible Sharepoint	10 heures pour reconfigurer et tester le système	Ahmed, administrateur Sharepoint; Mustapha, administrateur pare-feu	01-06-2022 à 02-06-2022	Faire des revues de sécurité périodiques pour s'assurer qu'une sécurité adéquate est fournie pour Sharepoint

Processus de gestion des risques (ISO 27005)

3. Traitement du risque

3.3 Évaluation des risques résiduels

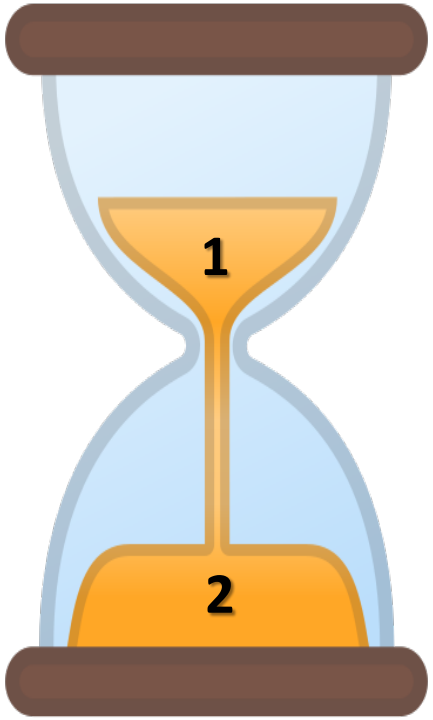


Processus de gestion des risques (ISO 27005)

3. Traitement du risque

3.3 Évaluation des risques résiduels

Risque inhérent
Ensemble des risques sans prise en compte des mesures de sécurité



1. **Risque résiduel**
Risque subsistant après le traitement du risque

2. **Risque traité**
Risque supprimer par les mesures de sécurité

Processus de gestion des risques (ISO 27005)

3. Traitement du risque

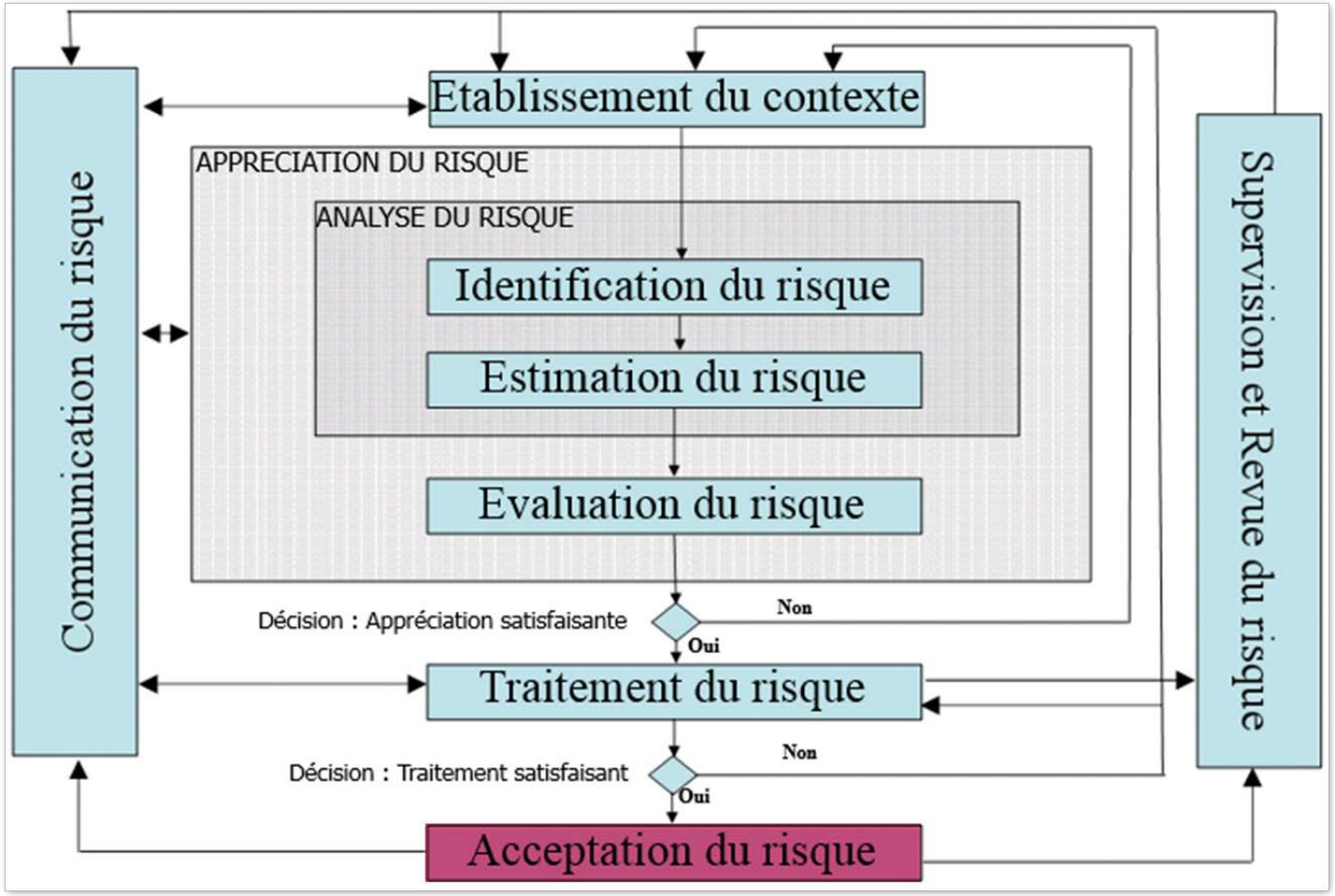
❑ Calcul du risque résiduel

Exemple

Scénario	Valeur du risque	Valeur du contrôle	Valeur du risque résiduel
Scénario A	10	3	7
Scénario B	8	1	7
Scénario C	15	6	9
Scénario D	3	0	3
Scénario E	4	0	4
Scénario F	8	2	6

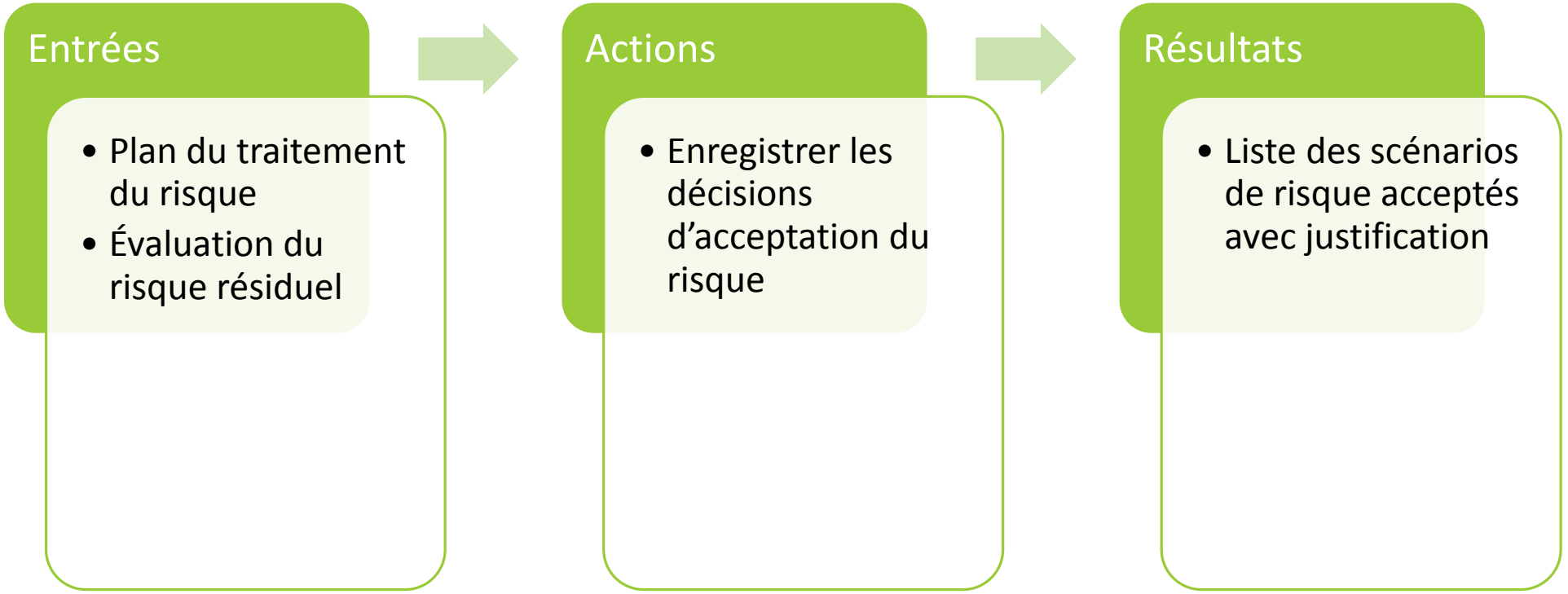
Processus de gestion des risques (ISO 27005)

4. Acceptation du risque



Processus de gestion des risques (ISO 27005)

4. Acceptation du risque



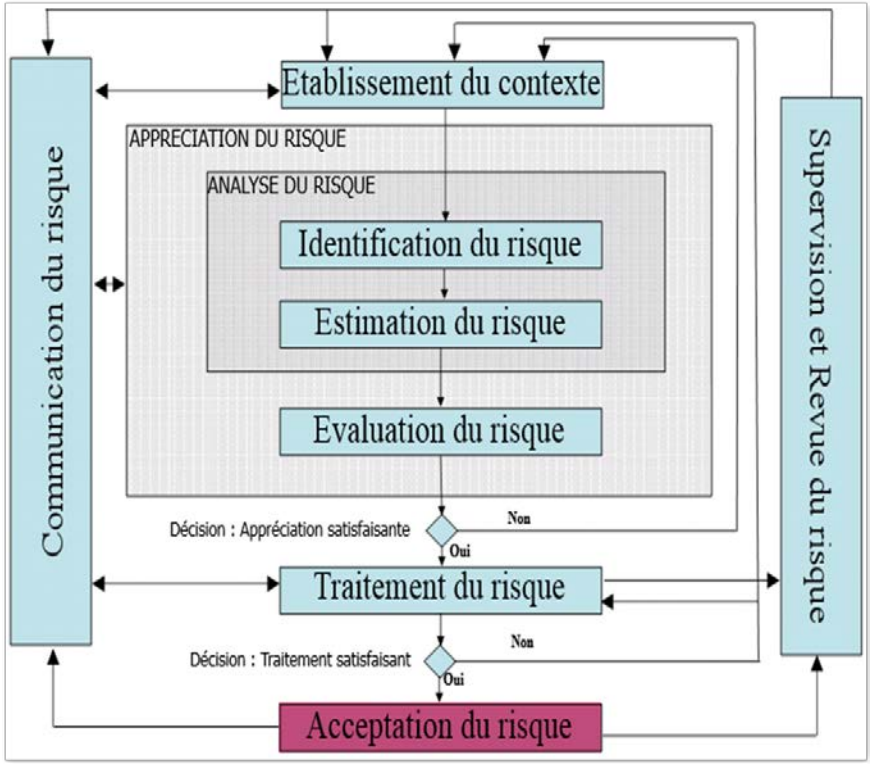
Processus de gestion des risques (ISO 27005)

4. Acceptation du risque

- **Acceptation des risques résiduels**

Acceptation des risques résiduels par la direction

- Il est important que les dirigeants en charge réexaminent et approuvent les plans de traitement des risques proposés et les risques résiduels associés, puis enregistrent les conditions associé à l'approbation
- Les critères d'acceptation des risques peuvent être plus complexe et ne pas consister simplement à savoir si un risque résiduel de situe au-dessus ou au-dessous d'un seuil unique



Processus de gestion des risques (ISO 27005)

4. Acceptation du risque

- **Niveau de risque résiduel dépasse le seuil d'acceptation du risque ?**

Lignes directrices

- Dans certains cas, il est possible que le niveau des risques résiduels ne remplisse pas les critères d'acceptation des risques car les critères appliqués ne tienne pas compte des circonstances prédominantes
- Par exemple, il peut être avancé qu'il est nécessaire d'accepter les risques car les bénéfices liés à ces risques sont très avantageux, ou parce que le coût de la réduction du risque est trop élevé
- De telles circonstances indiquent que les critères d'acceptation des risques sont inadaptés et qu'il convient, de les réviser