



5

GESTION DES RISQUE SSI

L'analyse de Risque SSI

- La gestion des risques
- Menaces, vulnérabilités et impacts
- Quelques normes :
 - ISO27005
 - EBIOS
 - MEHARI
 - NIST SP-800

5 Le risque

« Le risque est l'effet de l'incertitude sur l'atteinte des objectifs »

Guide ISO « Management du risque – Vocabulaire »

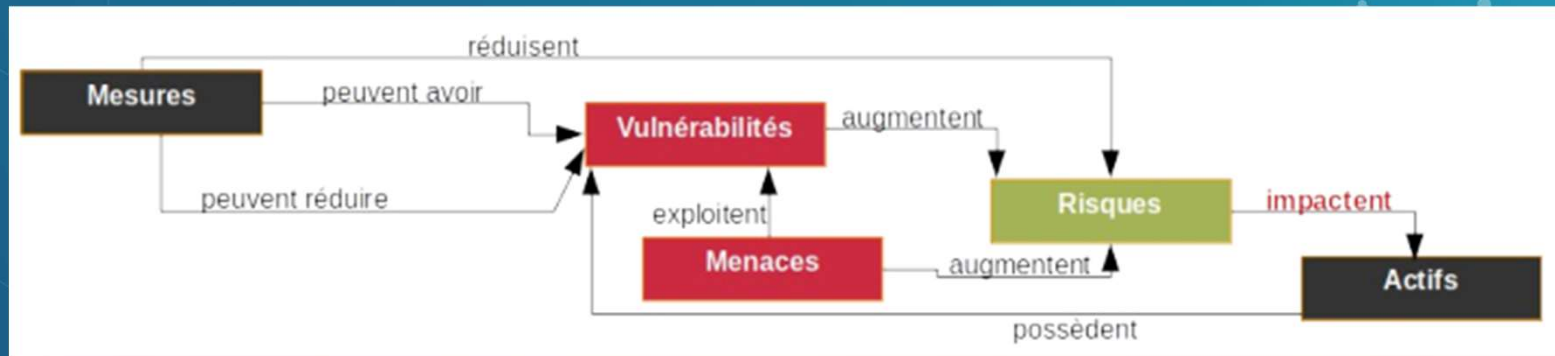
Les principaux objectifs de la sécurité :

- ◆ Disponibilité
- ◆ Confidentialité
- ◆ Intégrité
- ◆ Traçabilité

CIA pour Confidentiality, Integrity, Availability



5 Relations entre les concepts de la sécurité des SI



Exemples de relation en vulnérabilité et menace (= un scénario)

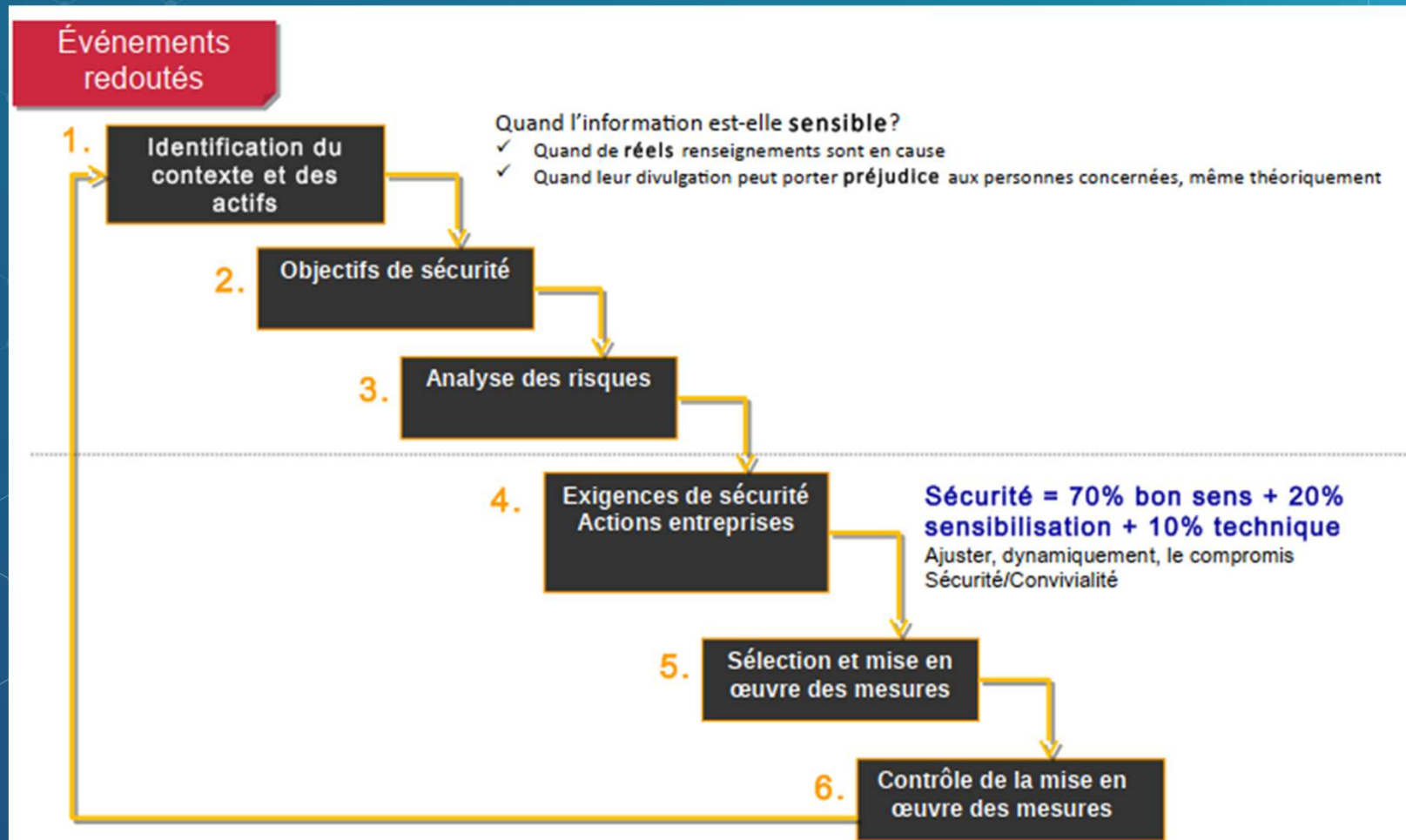
Vulnérabilités	Menaces
Entrepôt non protégé et sans surveillance	Vol
Procédures compliquées de traitement des données	Erreur d'entrée des données par le personnel
Pas de séparation des tâches	Fraude, utilisation non autorisée d'un système
Données non chiffrées	Vol d'information
Utilisation de logiciels piratés	Procès, virus
Pas de revue des droits d'accès	Accès non autorisé par des personnes qui ont quitté l'organisme
Pas de procédures de sauvegarde	Perte d'information

Un scénario peut être catégorisé en **Accident**, **Erreur** ou **Malveillance**.

5 La gestion des risques (Risk Management)



5 Processus simple de gestion des risques








5 Le traitement du risques

4 traitements possibles :

- ◆ Réduire le risque (contraintes financières, temporelles, techniques, opérationnelles, légales, techniques...)
- ◆ Accepter le risque (critères d'acceptation des risques, coût du traitement du risque trop élevé)
- ◆ Éviter les risques (risques trop élevés)
- ◆ Transférer/partager les risques (assurance, sous-traitance)

IMPACT	catastrophique 5	5	10	15	20	25
	significatif 4	4	8	12	16	20
	modéré 3	3	6	9	12	15
	bas 2	2	4	6	8	10
	négligeable 1	1	2	3	4	5
		1 improbable	2 faible	3 assez fréquente	4 probable	5 très fréquente
		PROBABILITÉ				

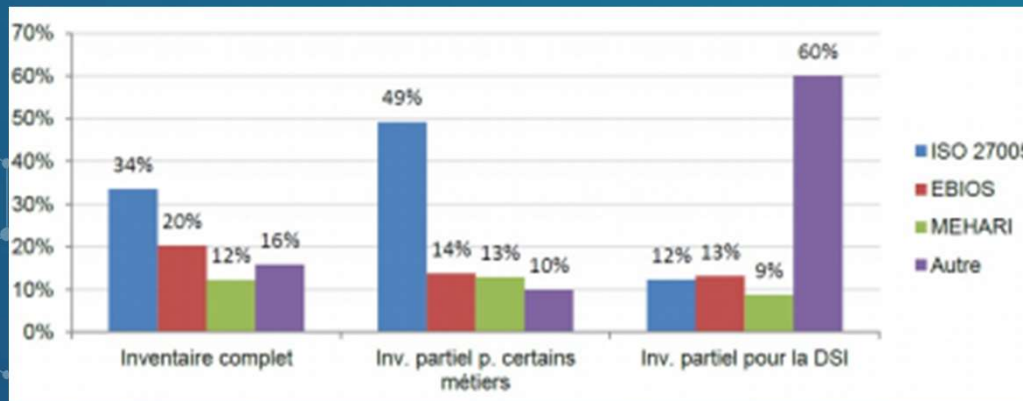
	Critique : à éviter, action à stopper
	Inacceptable : à éviter, à transférer
	Indésirable : à réduire ou transférer
	Acceptable : à accepter en surveillant
	Insignifiant : à accepter sans action

5 Les méthodes d'analyse de risques

Les principales méthodes normalisées pour les Analyses de Risques sont :

- ◆ **EBIOS RM** (Expression des Besoins et Identification des Objectifs de Sécurité - Risk Manager)
- ◆ **MEHARI** (MÉthode Harmonisée d'Analyse des Risques)
- ◆ **ISO 27005**

Les référentiels des analyses de risques utilisés par les entreprises françaises :



L'analyse de risque – RISQUE = menaces X vulnérabilité X impacts

5 Les menaces

Selon ISO 27001,

Une **menace** est une **cause** pouvant affecter la sécurité d'un actif.
(threat) (asset)

C'est **le facteur le plus difficile à évaluer**, car la menace est :

- ◆ **Évolutive** dans le temps et dans l'espace
- ◆ N'est réellement quantifiable qu'au moment où elle se manifeste

Il est pourtant capital de l'estimer au mieux, sachant que :

- ◆ la **sous-estimer** entraîne des risques inconsiderés (par définition)
- ◆ la **sur-estimer** entraîne un risque de paranoïa aiguë

L'analyse de risque – RISQUE = menaces X vulnérabilité X impacts

5 Support méthodologique pour l'estimation des menaces

Méthode STRIDE,

- ◆ - Spoofing (**usurpation**, menace l'authenticité)
- ◆ - Tampering (**falsification**, menace l'intégrité)
- ◆ - Repudiation (**répudiation**, menace l'irrépudiabilité)
- ◆ - Information Disclosure (**divulgation d'informations**, menace la confidentialité)
- ◆ - Denial of Service (**refus de service**, menace l'accessibilité)
- ◆ - Elevation of Privilege (**élévation de privilèges**)

L'analyse de risque – RISQUE = menaces X vulnérabilité X impacts

5 Support méthodologique pour l'estimation des menaces

Méthode EBIOS,

- ◆ INCENDIE,
- ◆ DÉGÂTS DES EAUX,
- ◆ POLLUTION,
- ◆ CRUE,
- ◆ ACCIDENTS MAJEURS,
- ◆ PHÉNOMÈNE CLIMATIQUE,
- ◆ PHÉNOMÈNE SISMIQUE,
- ◆ PHÉNOMÈNE VOLCANIQUE,
- ◆ DÉFAILLANCE DE LA CLIMATISATION,
- ◆ PERTE D'ALIMENTATION ÉNERGÉTIQUE,
- ◆ PERTE DES MOYENS DE TÉLÉCOMMUNICATIONS,
- ◆ RAYONNEMENTS ÉLECTROMAGNÉTIQUES,
- ◆ INTERCEPTION DE SIGNAUX PARASITES
- ◆ COMPROMETTANTS,
- ◆ ESPIONNAGE À DISTANCE,
- ◆ VOL DE SUPPORTS OU DE DOCUMENTS,
- ◆ VOL DE MATÉRIELS,
- ◆ DIVULGATION INTERNE,

- ◆ PANNE MATÉRIELLE,
- ◆ DYSFONCTIONNEMENT MATÉRIEL,
- ◆ SATURATION DU MATÉRIEL,
- ◆ DESTRUCTION DE MATÉRIELS,
- ◆ PIÉGEAGE DU MATÉRIEL,
- ◆ UTILISATION ILLICITE DES MATÉRIELS,
- ◆ ALTÉRATION DU LOGICIEL,
- ◆ PIÉGEAGE DU LOGICIEL,
- ◆ COPIE FRAUDULEUSE DE LOGICIELS,
- ◆ UTILISATION DE LOGICIELS CONTREFAITS
- ◆ OU COPIÉS,
- ◆ ALTÉRATION DES DONNÉES,
- ◆ ERREUR DE SAISIE,
- ◆ ERREUR D'UTILISATION,
- ◆ ABUS DE DROIT,
- ◆ USURPATION DE DROIT,
- ◆ RENIEMENT D'ACTIONS,
- ◆ FRAUDE,
- ◆ ATTEINTE À LA DISPONIBILITÉ DU
- ◆ PERSONNEL
- ◆ Etc.

L'analyse de risque – *RISQUE = menaces X vulnérabilité X impacts*

5 Complément à l'estimation des menaces

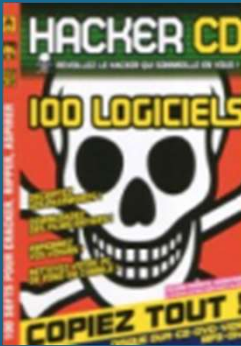
Estimer la **vraisemblance, la proportion, la tendance** :

- ◆ Des menaces d'**origine naturelle**
- ◆ Des **menaces intentionnelles**, ciblées
- ◆ Des **vecteurs et modes opératoires** employés par les menaces potentielles
- ◆ De l'**origine interne** des menaces
- ◆ Du niveau de **structuration des menaces**
- ◆ etc.



L'analyse de risque – *RISQUE = menaces X vulnérabilité X impacts*

5 Devenir une menace ? Une large source d'inspiration



Logiciel



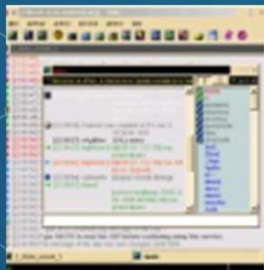
Magazines



Web



Littérature / Cinéma



Forum, IRC



Séminaire /Conf

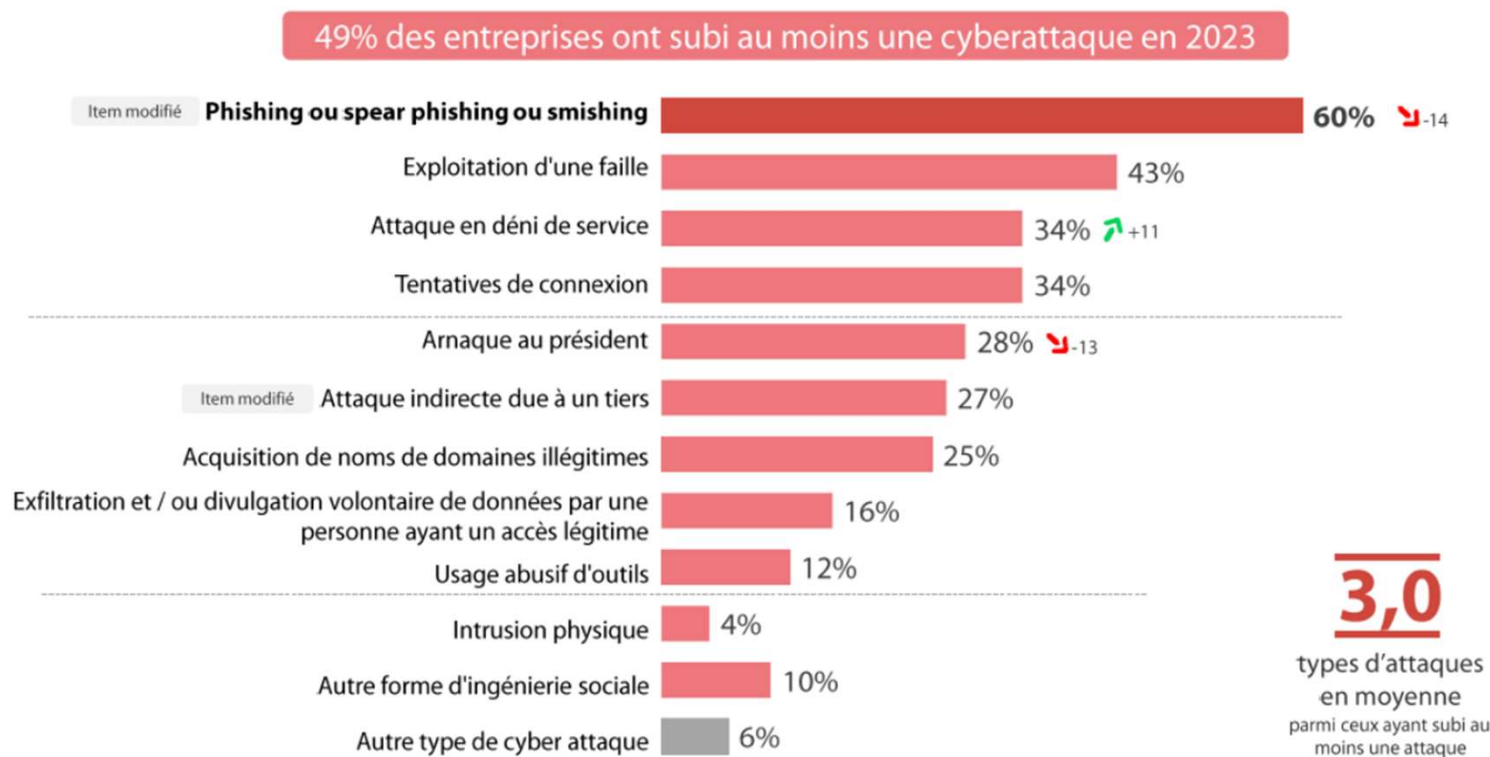


WEB TV

L'analyse de risque – *RISQUE = menaces X vulnérabilité X impacts*

5 Etat des menaces

Type d'attaques subies par les entreprises au cours de l'année 2023



L'analyse de risque – *RISQUE = menaces X vulnérabilité X impacts*

5 Les vulnérabilités

ISO 27000:2018

Faible dans un actif ou dans une mesure de sécurité qui peut être exploitée par une ou plusieurs menaces



Si vous connaissez vos ennemis et que vous vous connaissez vous-même, mille batailles ne pourront venir à bout de vous.
Si vous ne connaissez pas vos ennemis mais que vous vous connaissez vous-même, vous en perdrez une sur deux.
Si vous ne connaissez ni votre ennemi ni vous-même, chacune sera un grand danger."

Sun Tzu, L'art de la Guerre

L'analyse de risque – RISQUE = menaces X vulnérabilité X impacts

5 Les vulnérabilités opérationnelles

Vulnérabilités découlant des activités régulières

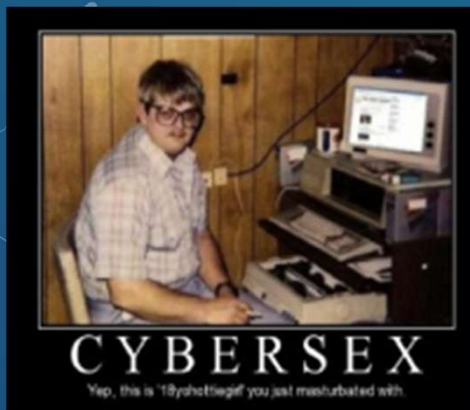
- Prédicibilité des opérations
- Procédures et leurs mise en œuvre
- Les traces (voyages, cartes de crédits, factures, etc.)
- Multiplication des lieux de travail
- Gestion des contractants
- Juridiques (CNIL, archives, classifications)
- etc.



L'analyse de risque – RISQUE = menaces X vulnérabilité X impacts

5 Les vulnérabilités humaines

- Ingénierie Sociale
- Personnalités (profiling)
- MISE (Money, Ideology, Sex, Ego) ou MICE (Money, Ideology, Constrain, Ego)
- PDH (Pain, Drug and Hypnosis), etc.
- SANSOUCIS (Solitude, Argent, Nouveauté, Sexe, Orgueil, Utilité, Contrainte, Idéologie, Suffisance)
- Phases de déstabilisation (divorces, faillites personnelles, décès, etc.)
- Atteinte au « moral des troupes » (mauvais management, harcèlements, plan sociaux, etc.)



bonsoir,
comment tu vas?
moi, pas trop bien!!
dis moi, ou es tu actuellement? jespere
que je ne te derange pas?
j'aurais besoin de ton aide.
contacte moi par mail uniquement (je suis
injoignable via mon telephone)
surtout je veux que ca reste discret
dans l'attente de te lire.

merci

Charles



L'analyse de risque – RISQUE = menaces X vulnérabilité X impacts

5

Les vulnérabilités physiques

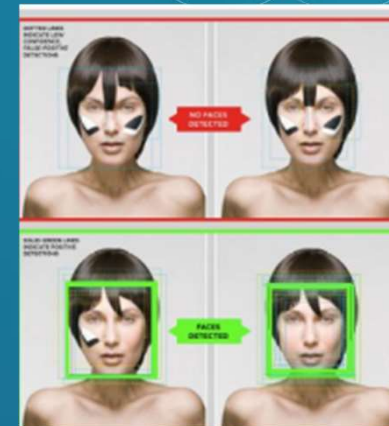
- Protection physique
- Voisinage
- Protection incendie
- etc.



L'analyse de risque – RISQUE = menaces X vulnérabilité X impacts

5 Les vulnérabilités techniques

- Informatique, téléphonie, sonorisation, etc.
- Failles logicielles, erreurs de configuration
- Gestion des accès (mots de passes, tokens, SSO, etc.)
- Canaux de transmissions
- etc



Iso 27005:2022

Sécurité de l'information, cybersécurité et protection de la vie privée – Préconisations pour la gestion des risques liés à la sécurité de l'information

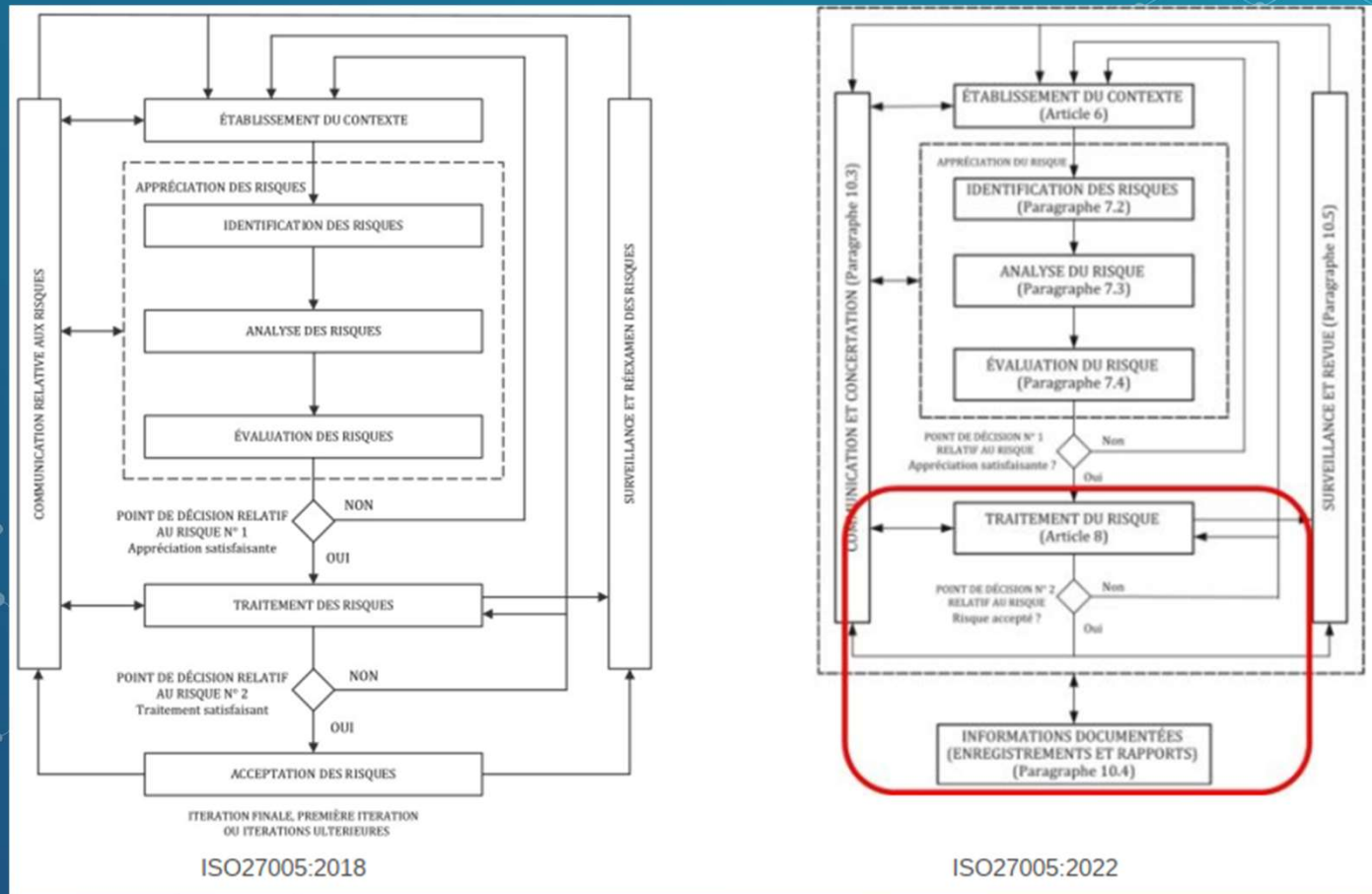
- . Définir une démarche de gestion de risques appropriée à la mise en place d'un SMSI
 - . Base GMITS, puis ISO 13335
 - . Participation française (SGDN) importante
 - . Delta entre démarche et méthode
 - . 2022 : Rapprochement avec la méthodologie d'analyse de risques EBIOS Risk Manager
 - . **Guide** pour la gestion des risques liés à la sécurité de l'information pour :
 - . évaluer
 - . traiter / accepter
 - . communiquer sur
- les risques liés à la sécurité de l'information**
- . Une gestion adaptée des risques inhérents au SI conduit à un SMSI opérationnel et efficace, tel que défini dans l'**ISO 27001**.
 - . Démarche itérative, selon le modèle **PDCA**.

5

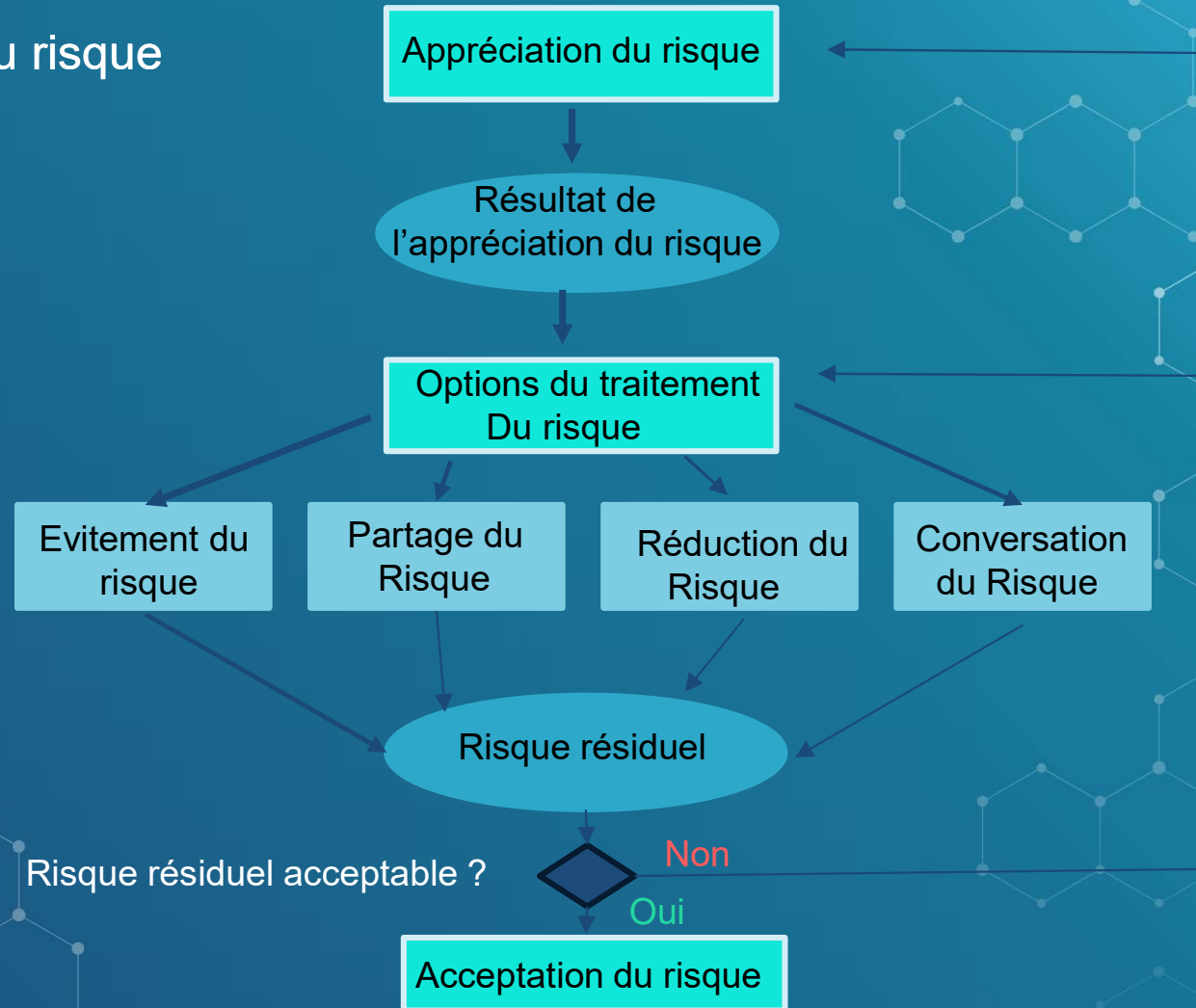
Concept et définition ISO 27005

- **Actif (« asset ») ou Bien** : tout ce qui représente de la valeur :
 - Actifs primaires : processus et activités, informations
 - Actifs secondaires : matériel, logiciel, réseau, personnel, site, support organisationnel
- Dégradation, dommage, conséquences
- **Menace** : élément ayant le potentiel de causer un dommage à un actif
- **Vulnérabilité** :
 - Point d'application potentiel de menace
 - Défaut / faille dans les dispositifs de protection d'un actif contre une menace
- **Identification du risque** : processus permettant de trouver, lister et caractériser les éléments à risque
- **Estimation du risque** : processus permettant d'affecter des valeurs à la probabilité et aux conséquences d'un risque (niveau de risque)

5 Aperçu général du processus

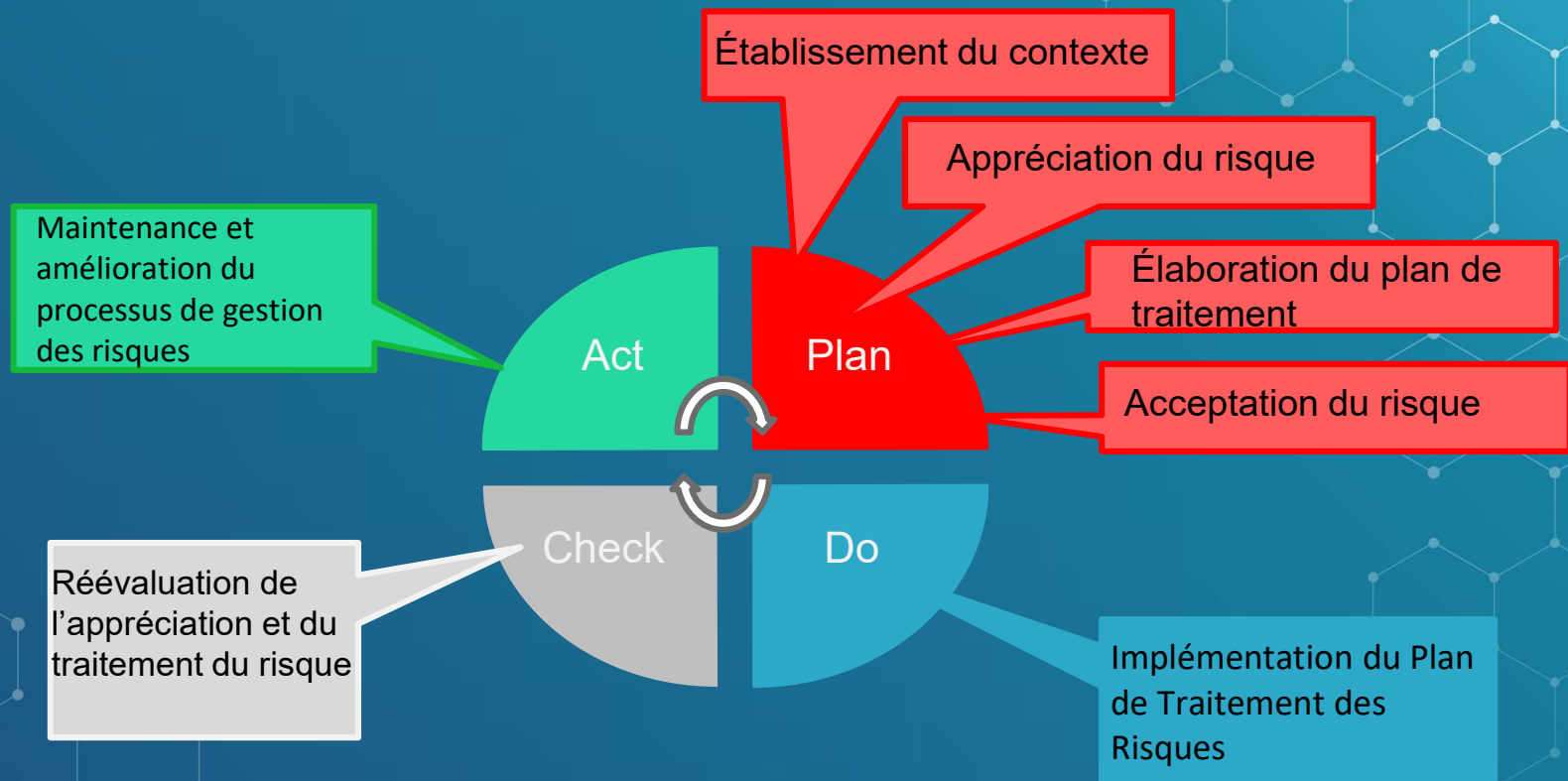


5 Traitement du risque



5

Modèle PDCA appliqué au SMSI et à la gestion des risques



5

Mise en œuvre de la démarche

Un projet supporté par la direction

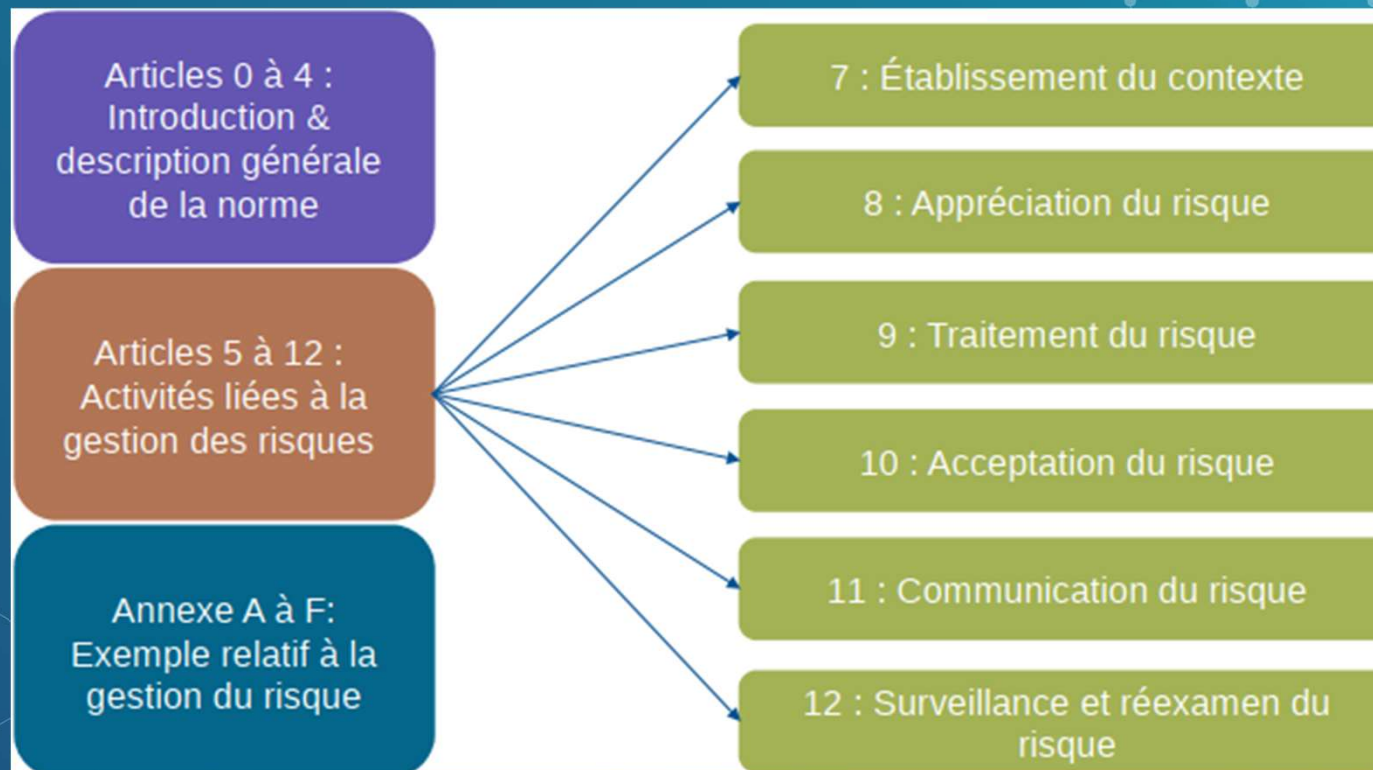
- Des motivations en ligne avec la stratégie de l'entreprise
- Périmètre
- Enjeux
- Un processus de gestion des risques formalisé
- Un planning
- Des réunions périodiques
- Des ressources identifiées

Un choix de méthodes, d'outils et métriques

- Choix d'une méthode d'analyse de risques,
- Choix de métriques pour l'évaluation des actifs, des impacts, des risques

5

Structure du document de la norme



5

Établissement du contexte

Actions

- Choix de la méthode d'analyse de risque
- Choix des critères de base:
 - critères d'impact
 - critères d'évaluation et d'acceptation du risque

Sélection du **périmètre** sur lequel portera la gestion des risques

Définition de **l'organisation impliquée**

- Rôles
- Responsabilités

5 Objectif du processus

- Il est important de **définir l'objectif** de la démarche de gestion du risque :
- Une réponse aux exigences d'un SMSI ?
- La conformité avec la loi, ou la fourniture de preuves ?
- La préparation d'un plan de continuité de l'activité ?
- La préparation d'un plan de réponse aux incidents ?
- La description des exigences sécurité pour un produit ou un service ?
- L'objectif influera sur l'ensemble du processus :
 - Actifs
 - Périmètre
 - Critères de base

5 Critères d'estimation des risques

Choisir des critères d'estimation dans le contexte de l'entreprise :

- La **valeur stratégique** des processus de traitement des informations
- La **criticité** des informations
- Les exigences **légal**es et **réglementaires**, obligations contractuelles
- Pour les types d'actifs, importance **opérationnelle** et **stratégique** :
 - de la disponibilité
 - de la confidentialité
 - de l'intégrité
- Les attentes et perception des acteurs concernés
- Les conséquences négatives en termes d'image ou de motivation
- Aide pour définir des **priorités de traitements**

Etablissement du contexte

5

Critères d'impact

Choisir des **critères de mesure d'impact** selon :

- L'importance des dommages
- Coûts pour l'organisation

Quelques pistes :

- Le niveau de classification des informations
- La nature de l'incident (perte de D, I ou C)
- La nature des opérations concernées (internes ou tierce partie)
- Les pertes de business et la valeur financière
- Les impacts sur les plannings ou le respect des délais
- Les atteintes à la réputation et à l'image
- Les non respects d'exigences légales, réglementaires, ou contractuelles

Etablissement du contexte

5 Critères d'évaluation et d'acceptation des risques

- **Accepter les risques** est un moyen de les traiter
- L'organisation doit définir **ses propres critères d'acceptation**
- L'échelle d'acceptation doit être en ligne avec :
 - la politique
 - la stratégie
 - les objectifs
 - les intérêts

Quelques pistes :

- Plusieurs **seuils** avec des conditions d'acceptation différentes
- Différents niveaux hiérarchiques autorisés à accepter
- Un ratio **Profit** attendu / **Risque** estimé
- Des critères différents selon les classes de risques :
 - Aucune acceptation pour les **risques légaux**,
 - Acceptation de risques élevés dans le cadre de **certains contrats**
- Des actions exigées pour rendre le risque acceptable : avertir certains partenaires, actionnaires...
- La **durée** pendant laquelle le risque est encouru

5 Appréciation du risque

Actions

- Identifier
- Mesurer
- Prioriser les risques,
 - selon les critères d'évaluation définis au départ
 - selon les objectifs significatifs pour l'organisme

Démarche d'appréciation en **2 étapes** :

- **Analyse de risque** :
 - Identification des risques = inventoirer
 - Estimation des risques = mesurer
- **Évaluation des risques** : quantification selon les critères définis

5 Traitement des risques

Action : Traitement possible pour chaque risque :

- Réduire le risque (contraintes financières, temporelles, techniques, opérationnelles, légales, techniques...)
- Accepter le risque (critères d'acceptation des risques, coût du traitement du risque trop élevé)
- Éviter les risques (se mettre en situation où le risque n'existe pas)
- Transférer les risques (assurance, sous-traitance)
- Un plan de traitement du risque doit être défini

Pré-requis :

- Liste des risques priorisés, échelle d'estimation des niveaux de risques résiduels.
- **Objectif :** établir un plan d'action et identifier les risques résiduels

5 Acceptation du risques

Action : approuver le plan de traitement des risques proposé / accepter formellement les risques

- La Direction approuve formellement le plan de traitement des risques
- Le cas contraire, la Direction décide d'accepter les risques et les responsabilités qui en découlent (décision doit formellement enregistrée)

Objectif :

- Établir un plan de traitement de risques et des risques résiduels sous réserve de La décision d'acceptation de la Direction.
- Établir une liste des risques acceptés accompagnés de leur justification en cas de non respect des critères d'acceptation du risque usuel à l'organisation

5 Communication du risques

Action : les informations sur les risques doivent être échangées entre la Direction et les différents interlocuteurs concernés.

Objectif :

- Responsabiliser l'ensemble des interlocuteurs face aux risques
- Améliorer la sensibilisation à la sécurité de l'information au sein de l'organisation
- Coordonner les activités liées à la gestion des risques

Résultat :

- Une bonne compréhension du processus de gestion des risques et de ses résultats par tous les acteurs de l'entreprise.

5 Communication du risques

La communication est un moyen essentiel de la coordination.

Difficultés :

- Parler des risques, c'est parfois aussi les augmenter...
- Parler des risques ce n'est pas juger le travail des autres...
- La culture de « la sécurité par l'obscurité » a la vie longue !

Guidelines :

- Communiquer au quotidien
- Anticiper la communication pour les temps de crise
- Communication bidirectionnelle entre la direction et les personnes concernées

5 Surveillance du risque

Action : surveiller, revoir régulièrement et perfectionner la liste des risques identifiés et leurs facteurs (biens sensibles, impacts, menaces, vulnérabilités, potentialité d'occurrence) :

- Les risques ne sont pas statiques
- Le système d'information évolue, les risques également
- Quelques pistes conduisant à une revue des risques :
 - Nouveaux biens sensibles
 - Nouvelles menaces non évaluées
 - Nouvelles vulnérabilités
 - Amplification de l'impact

Objectif :

- assurer que la gestion des risques reste alignée sur les objectifs stratégiques de l'entreprise

5 Assurer la revue du processus

Action : surveiller, revoir régulièrement et perfectionner le processus de gestion des risques lui-même

- S'assurer que le plan de traitement des risques reste pertinent
- Surveiller les évolutions du contexte qui pourraient imposer de revoir la stratégie
- S'assurer de la disponibilité permanente des ressources nécessaires à la gestion des risques

Objectif :

- permettre une amélioration continue du processus de gestion des risques

Cette tâche est réalisée au cours des Revues de Direction prévues dans le SMSI