Analyse de risques
ISO 27005, EBIOS, RGS

Walter YANGUERE

Mathieu CHARBOIS

Pierre-Yves DUCAS

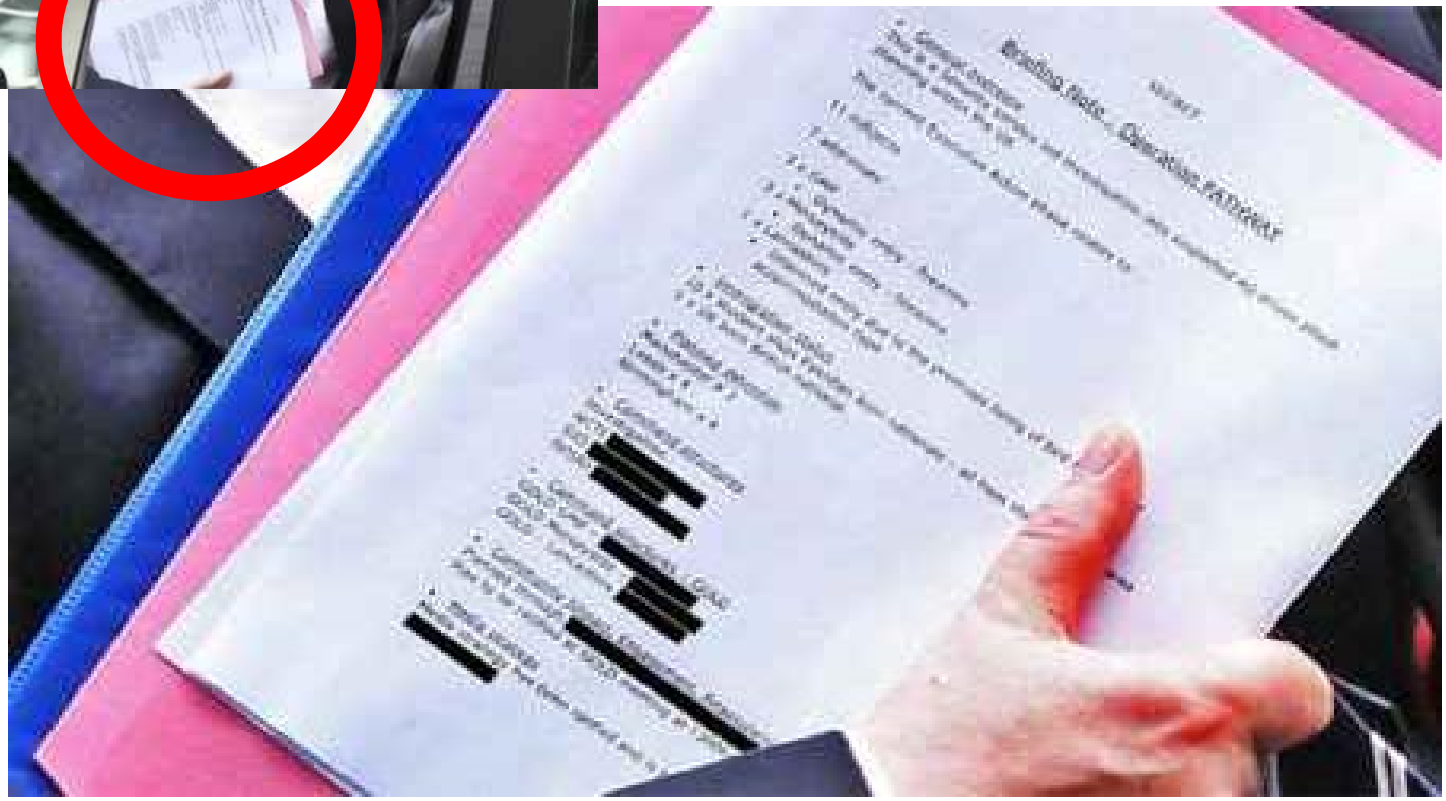
Sommaire

Quelques images pour commencer

Le digicode d'accès à une salle serveurs….

Quelques images pour commencer

Le patron de Scotland Yard …



Quelques images pour commencer

La protection de votre vie privée ….

Quelques images pour commencer

La protection physique des accès….

Quelques images pour commencer

La protection des

accès logiques

Ou …

Le manque de

Formation

Des employés

Quelques images pour commencer

La protection physique des installations ….

Quelques images pour commencer

Le respect des procédures ….

Quelques images pour commencer

La protection physique

des supports d'information….

Sommaire

Situation objective qui entraîne l'absence de **menace** sur les **biens** et qui détermine la **confiance**

Quelles actions pour bien gérer la sécurité

Activité	Description
Analyse de risques (ISO 27005, EBIOS)	• Savoir ce qui peut arriver, et quelle conséquence cela peut avoir. ➔ Prendre les mesures de réduction du risque.
Audit organisationnel (ISO 27001, 27002)	• Savoir comment l'organisation applique les bonnes pratiques de sécurité. ➔ Appliquer celles qui manquent.
Audit technique (Pentest, architecture)	• Savoir si le système possède des failles, où elles se situent, et quelle est leur criticité. ➔ Corriger les failles détectées.

Besoins en sécurité les plus utilisés

Disponibilité : Assure la fiabilité et la performance du stockage, du traitement et du transport (capacité à délivrer l'information souhaitée en temps voulu).

Intégrité : Assure la fiabilité du contenu (que l'information ne soit pas altérée ou perdue).

Confidentialité : Assure la protection, pour limiter l'accès aux seules personnes autorisées.

Autres besoins en sécurité utilisés

Traçabilité : Garantit qu'une action (traitement, transfert, accès, …) est mémorisée (nature, date, acteurs, résultat, …) et pourra être retrouvée et analysée a posteriori.

Authenticité : Garantit l'origine de l'information et la preuve de sa transmission (émetteur/destinataire ne peuvent nier avoir émis/reçu).

La diversité des métiers de la sécurité

Métiers	Activités
Gouvernance	Organisation et processus de gestion de la sécurité (politique, rôles, comités décisionnels, …)
Architecture	Construction et organisation des moyens techniques permettant d'assurer la sécurité (locaux, matériel, logiciels, …)
Production	Utiliser le système d'information pour servir le métier de l'organisme au quotidien.
Administration & Supervision	Moyens techniques mis en œuvre pour assurer le maintien en condition opérationnel et la remontée d'information pour les instances décisionnelles (prévisions, supervision, détection et traitement d'incidents, sauvegardes, opérations planifiées, …)
Audits	Evaluation du niveau de sécurité, comparaison aux niveaux souhaités, préconisations d'amélioration…
Juridique & Conformité	Définition, mise en application et contrôle des référentiels juridiques et réglementaires.
Recherche & Développement	Veille technologique et règlementaire, laboratoires, …

La complexité des systèmes d'information

Domaine	Activités
Organisation	Référentiels, politiques, procédures, homologations, …
Services	Locaux, alimentation électrique, climatisation, …
Matériels	Serveurs, équipements réseaux, postes de travail, baies de stockage, imprimantes, pare-feux, ….
Logiciels	Systèmes, middlewares, applications internes, logiciels éditeurs
Réseaux	Protocoles de communication, câble, fibre, …
Données	Bases de données métier, paramétrage, bureautique, …
Supports	SAN, NAS, disques durs, clefs USB, CD/DVD, imprimantes, papier, …
Personnes	Directions métiers, DSI, RSSI, RSI, RPCA, CIL, administrateurs, utilisateurs, opérateurs, prestataires, …

Sommaire

Définition du mot risque (dictionnaire)

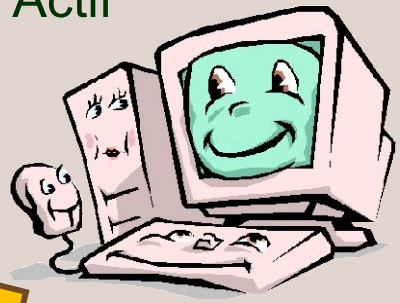
- Un danger éventuel plus ou moins prévisible
- Eventualité d'un évènement ne dépendant pas exclusivement de la volonté des parties et pouvant causer la perte d'un objet ou tout autre dommage
- **Le fait de s'exposer volontairement à un danger (dans l'espoir d'en tirer un avantage)**

Citation de Benjamin Franklin

- Il y a bien des manières de ne pas réussir, mais la plus sûre est de ne jamais prendre de risques

Représentation du risque

Actif

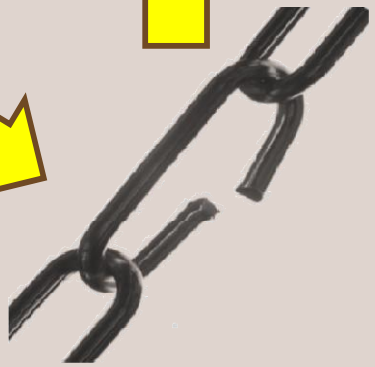


Menace
(et source)

Cible

Affecte

Exploite



Vulnérabilité

Génère

Impact

Conséquence

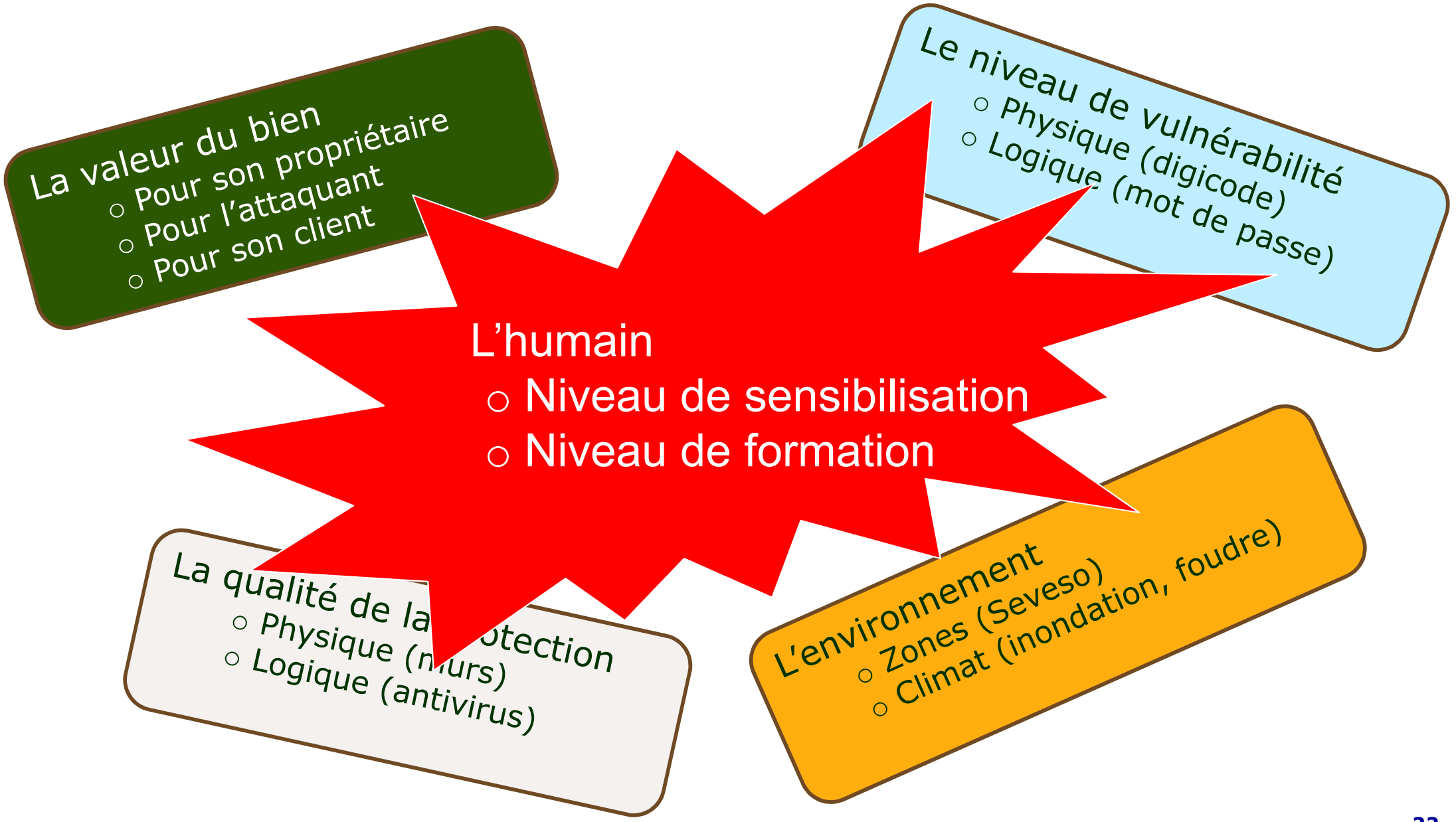
Le risque sans gestion

Menace		Vulnérabilité		Impact
	+		→	
	+		→	
	+		→	
	+		→	

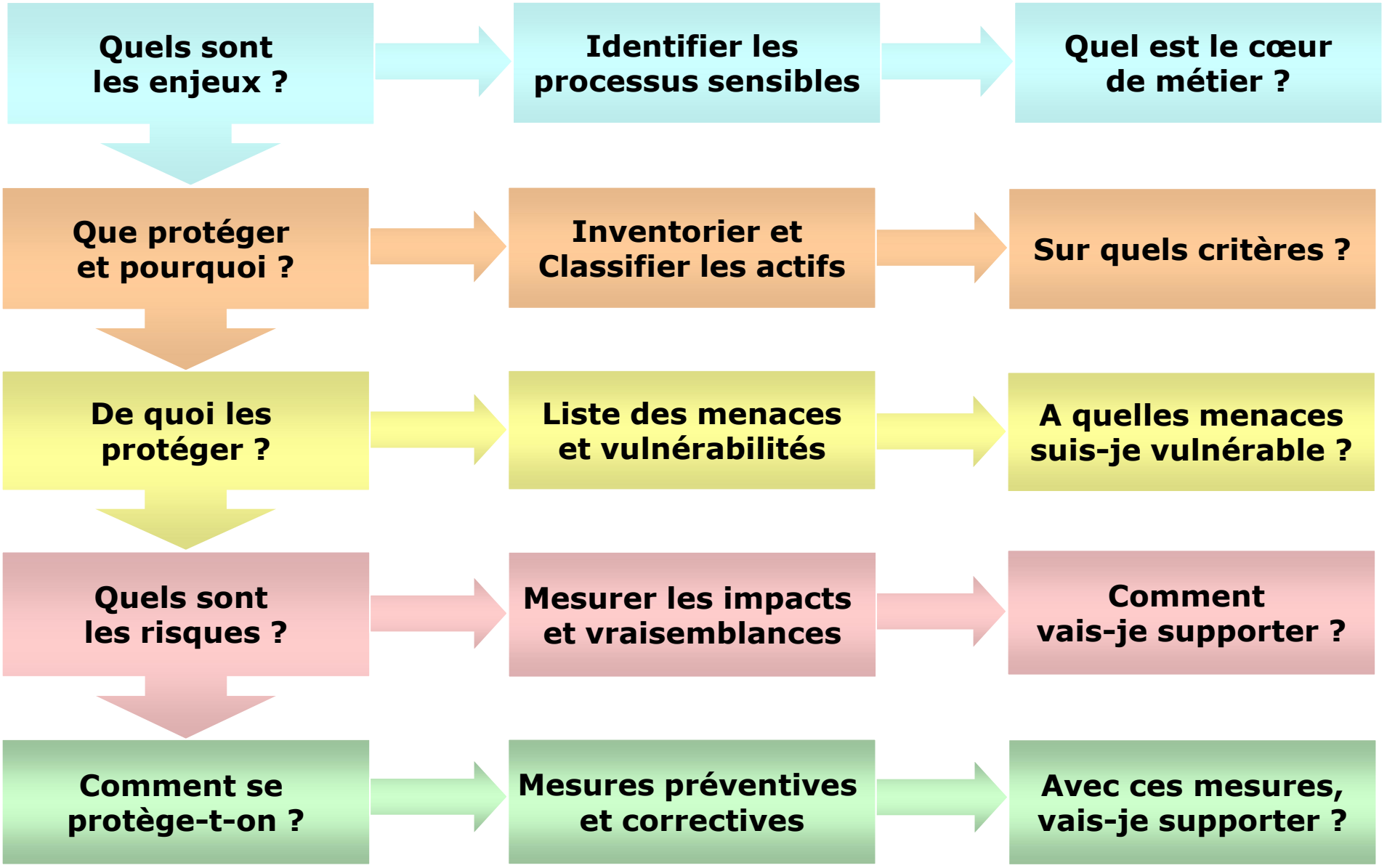
Le risque géré

Menace	Prévention Protection	Réaction Correction
		
		
		
		

Les facteurs qui influencent le risque



La démarche d'analyse du risque



Formule pour se souvenir…

$$R = M * V * I$$

R : Risque (niveau)

M : Menace (occurrence)

V : Vulnérabilité (facilité d'exploitation)

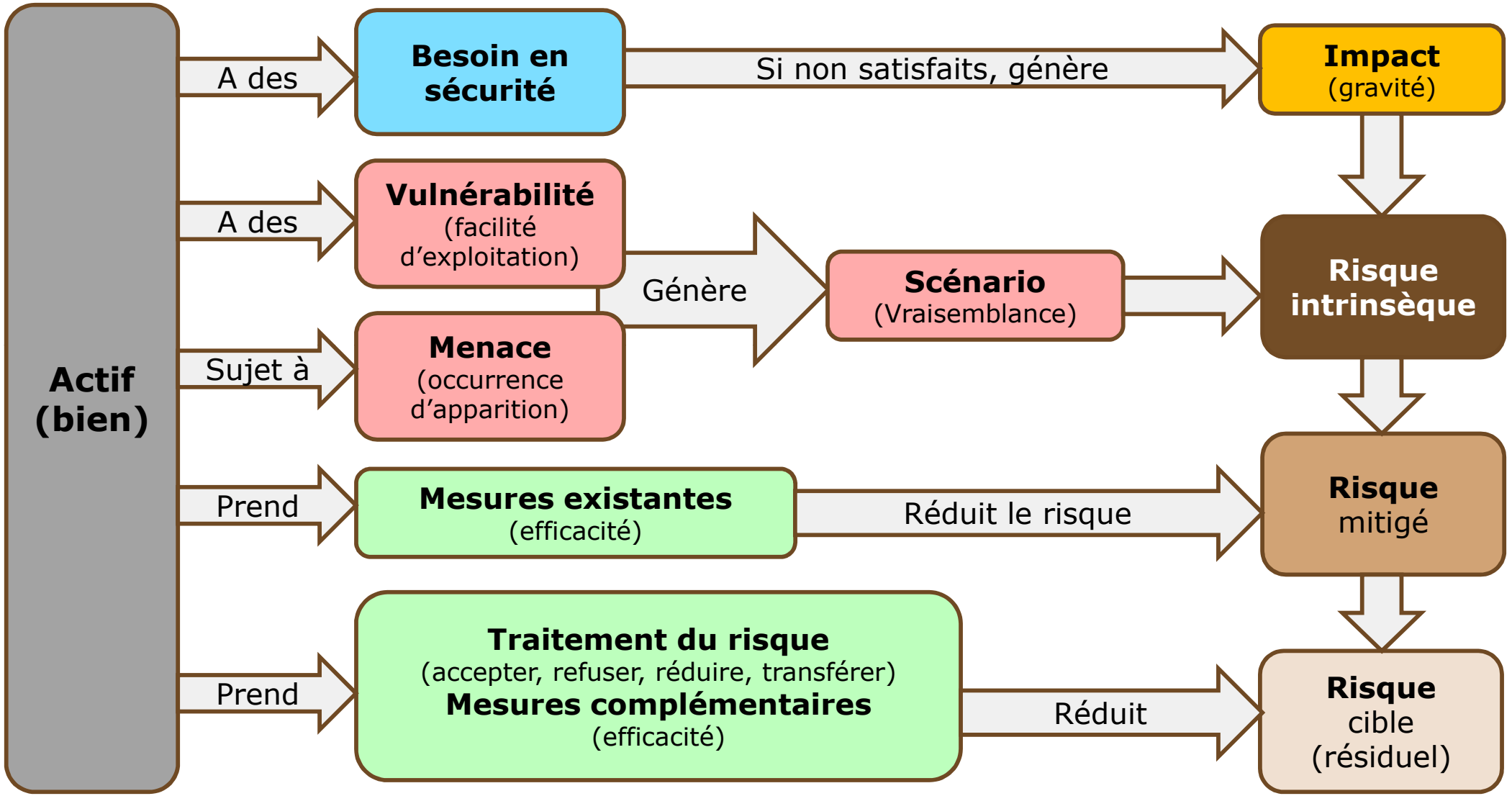
I : Impact (sur les biens)

S'il n'y a pas de menace, il n'y a pas de risque

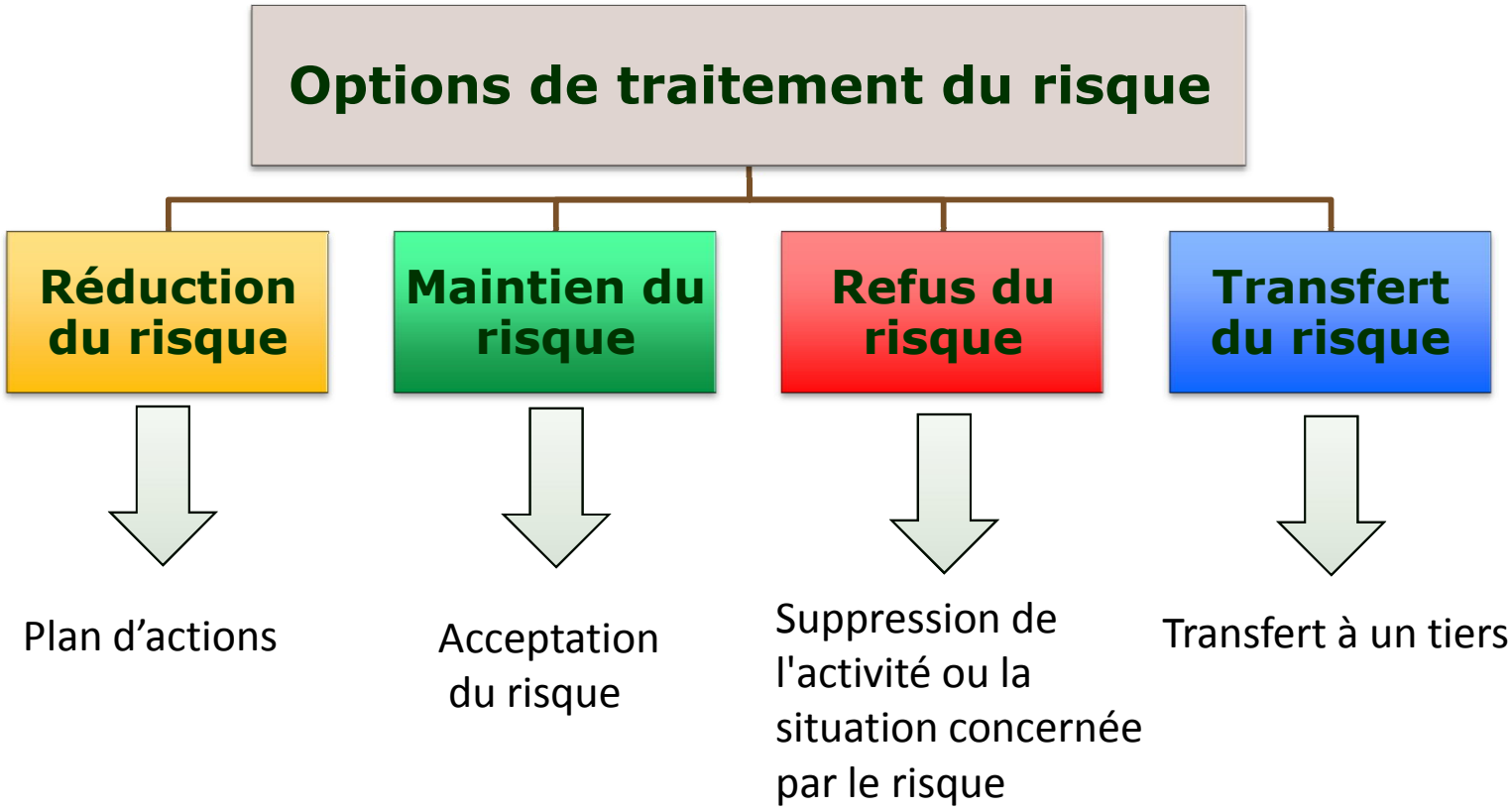
S'il n'y a pas de vulnérabilité, il n'y a pas de risque

S'il n'y a pas d'impact, il n'y a pas de risque

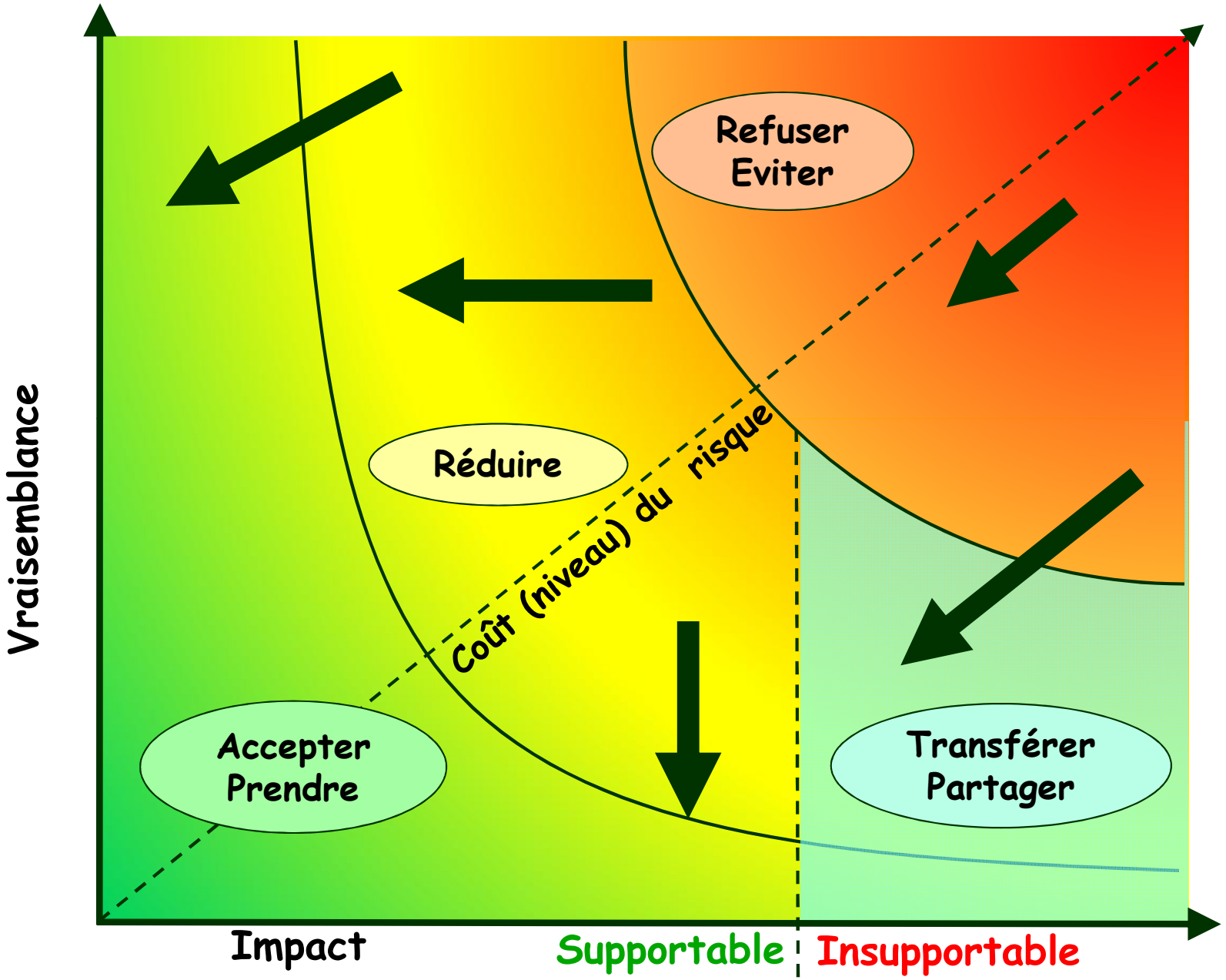
Evaluation et traitement du risque



Traitement des risques – Principe général



Les zones de traitement du risque



Sommaire

Objectif

- Guide de mise en œuvre de l'appréciation des risques de la sécurité de l'information décrite dans l'ISO 27001
- Processus de gestion du risque en sécurité de l'information

Méthode

- Méthodologie complète et structurée
- Non outillée

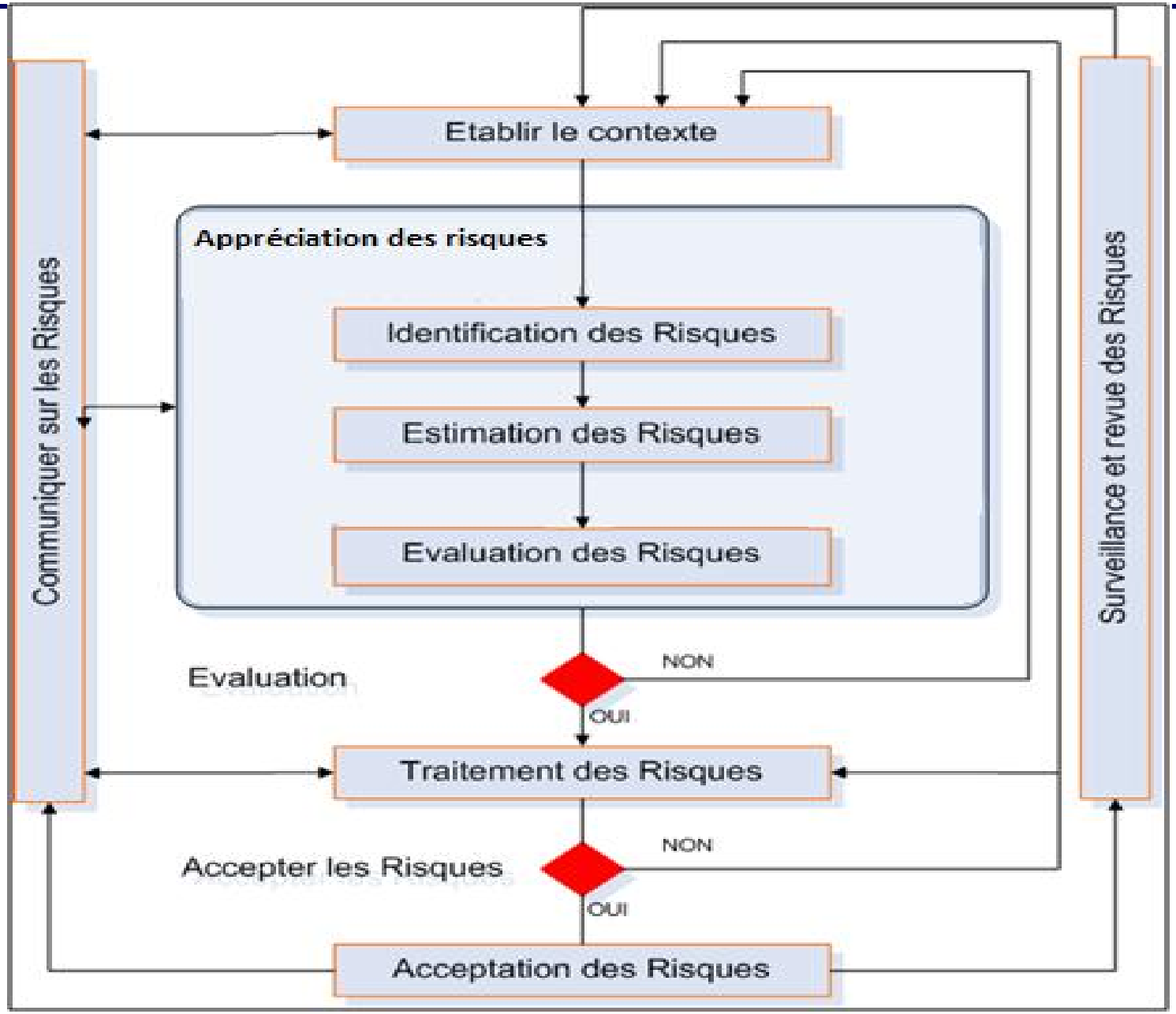
Version

- ISO/CEI 27005: (2011 par l'ISO , 2013 par l'AFNOR)

Approche

- **Systématique**
  - Nécessaire pour identifier les besoins organisationnels
  - Indispensable à la création d'un SMSI selon ISO 27001
- **Itérative**
  - Deux points décisionnels nécessitant une compréhension et une validation managériale
- **Continue**
  - S'intègre dans le processus PDCA d'un SMSI

ISO 27005 : schéma global



Avantages

- **Simple**
  - Le vocabulaire s'apparente au langage courant
  - Ne nécessite pas un grand niveau d'expertise
- **Pragmatique**
  - Structure une démarche de bon sens
- **Adaptative**
  - S'applique a une grand variété d'environnements

Inconvénients

- **Base de connaissance minimale**
  - nécessite des annexes ou outils complémentaires
- **Ouverte**
  - Ne fixe pas la « maille » et peut conduire à des analyses trop légères ou au contraire trop fines et donc inexploitables.

Norme ISO 27005 : Amélioration continue

PLANIFIER

- Établissement du contexte
- Appréciation des risques
- Élaboration du plan de traitement des risques
- Acceptation des risques

DEPLOYER

- Mise en œuvre du plan de traitement des risques

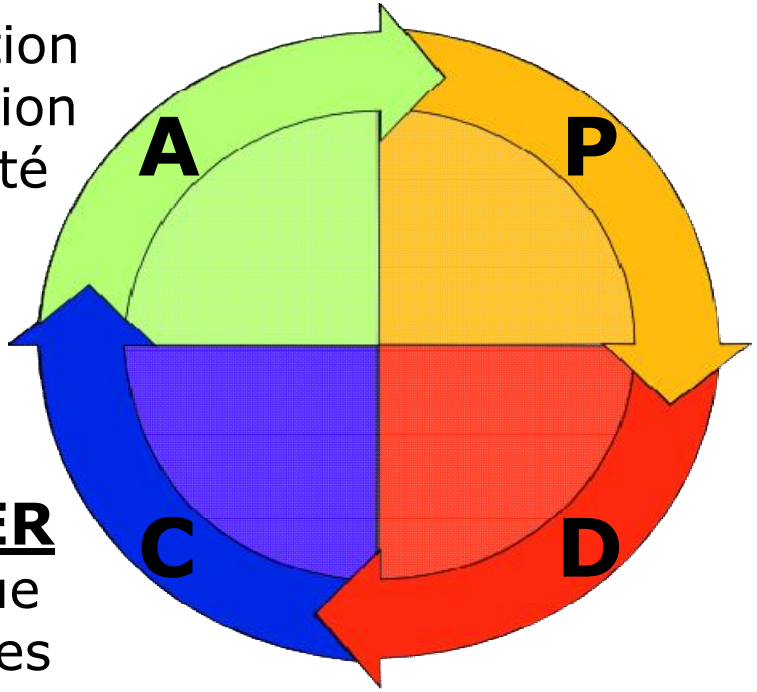
Les mesures de sécurité sélectionnées dans la 27002 et les mesures mises en place par l'organisme peuvent venir en réduction du risque.

CONTRÔLER

- Surveillance et revue continues des risques

AGIR

- Maintien et amélioration du processus de gestion des risques en sécurité de l'information



Sommaire

Méthode Française développée par l'ANSSI

- **EBIOS V1** : Outils de spécification SSI (1995)
- **EBIOS V2** : Méthode d'analyse de risques (2004)
- **EBIOS 2010** : Méthode de gestion des risques

  Compatible avec la norme ISO 27005
  Quasiment imposée aux administrations, …
  Boite à outil utilisable totalement ou partiellement
  Assortie d'un logiciel gratuit de mise en œuvre

EBIOS : les domaines d'application

Les administrations

- L'armée
- Collectivités territoriales
- Administrations d'état

Les industriels

- Automobile
- Aviation
- …

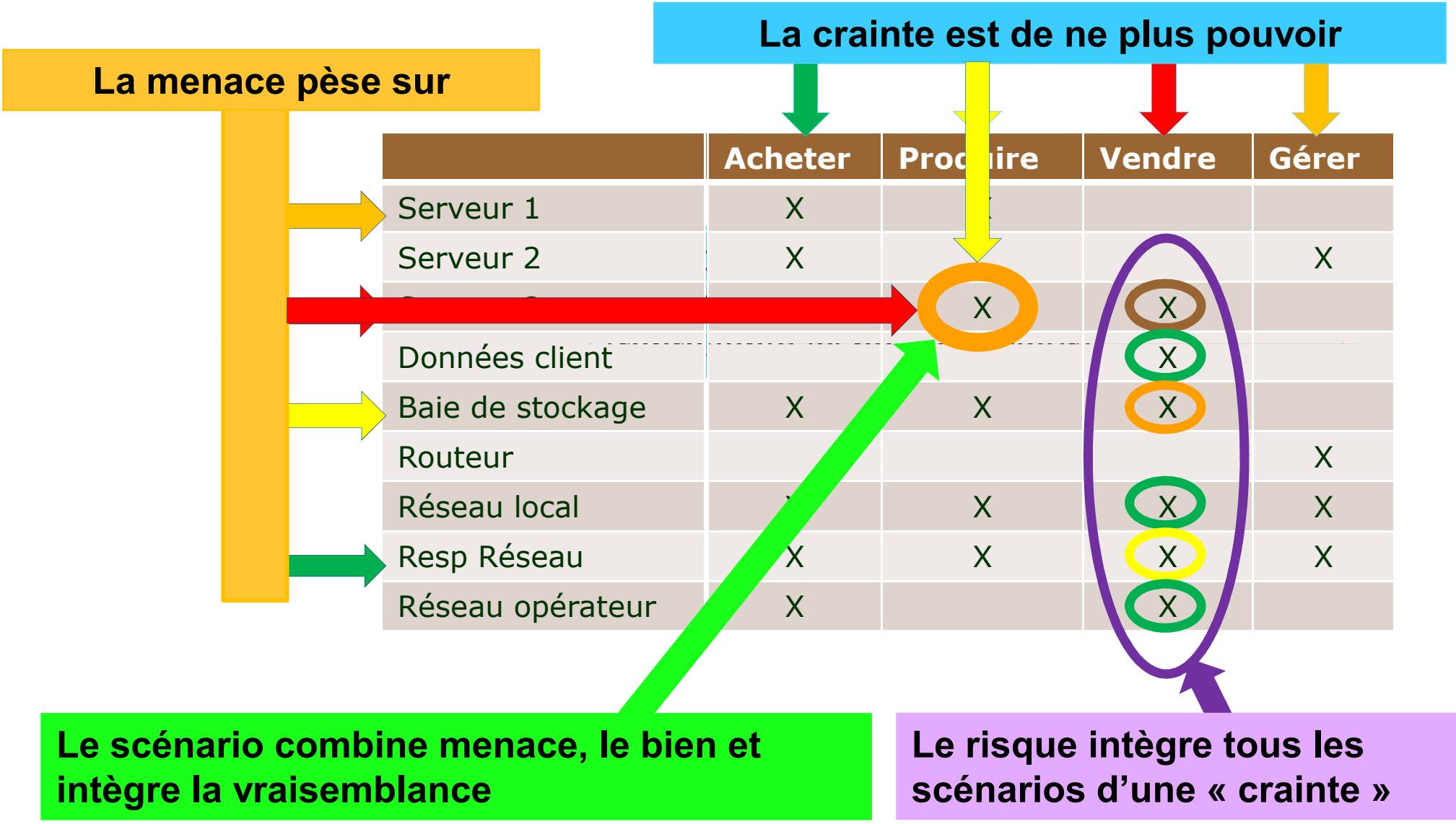
Les services

- Banques
- Assurances
- Santé
- …

EBIOS travaille sur 2 axes puis les relie

- **L'axe fonctionnel**
  - Les biens essentiels sont des processus, des fonctions, …
  - Ils ont des besoins en sécurité (DICP)
  - Si ces besoins ne sont pas satisfaits, un éventuel incident peut générer un évènement redouté dont on estime les impacts et la gravité
- **L'axe « technique »**
  - Les biens supports sont des équipements ou des personnes qui rendent des services
  - Ils ont des vulnérabilités plus ou moins importantes face à des menaces plus ou moins probables
  - Etablir les scénarios de menace sur les biens support, et leur vraisemblance
- **Les 2 axes sont ensuite reliés**
  - Relier les biens supports aux biens essentiels
  - En déduire le risque pour chaque évènement redouté par la combinaison impact / vraisemblance

EBIOS : démarche générale



EBIOS est décliné en :

- **Modules** : chacun à un objectif fonctionnel et décrit
  - **Activités** : chacune d'elle est une partie du module qui décrit :
    - Les objectifs et avantages
    - Les données d'entrée
    - Les rôles et responsabilités (RACI)
    - Les données produites (et l'usage qui peut en être fait)
  - **Actions** : décomposition de l'activité en actions élémentaires :
    - Les moyens d'y parvenir
    - Des conseils
    - Des exemples

EBIOS : démarche générale

Métrique

Module 1
Contexte

Bien essentiel | **Mesures** | **Bien support**

Besoin en sécurité → Evènement redouté → **Gravité**

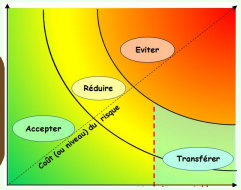
Module 2
Fonctionnel

Scénario ← Source, Menace, Vulnérabilité
Scénario → **Vraisemblance**

Module 3
Technique

Module 4
Risque

Risque mitigé → Traitement



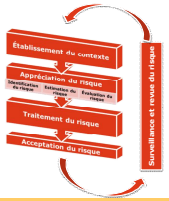
Module 5
Mesures

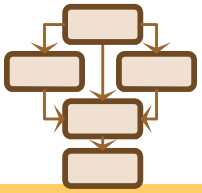
Mesures complémentaires → Risque Résiduel

Le rôle de chaque module

Module	Questions à se poser
1 Contexte	Pourquoi cette analyse et quel est le périmètre ? Comment va-t-on s'y prendre ?
2 Evènements redoutés	Que pourrait redouter **le métier** ? Quelle est la gravité liée aux manquements ?
3 Scénarios de menace	Que pourrait-il arriver (menaces, scénarios) ? Quelle est leur vraisemblance ?
4 Risques	Quelle est la cartographie des risques ? Comment traiter chacun de ces risques ?
5 Mesures de sécurité	Quelles mesures retenir et appliquer ? Quel est le risque résiduel ?

Sommaire





ISO 27005 ⇔ EBIOS

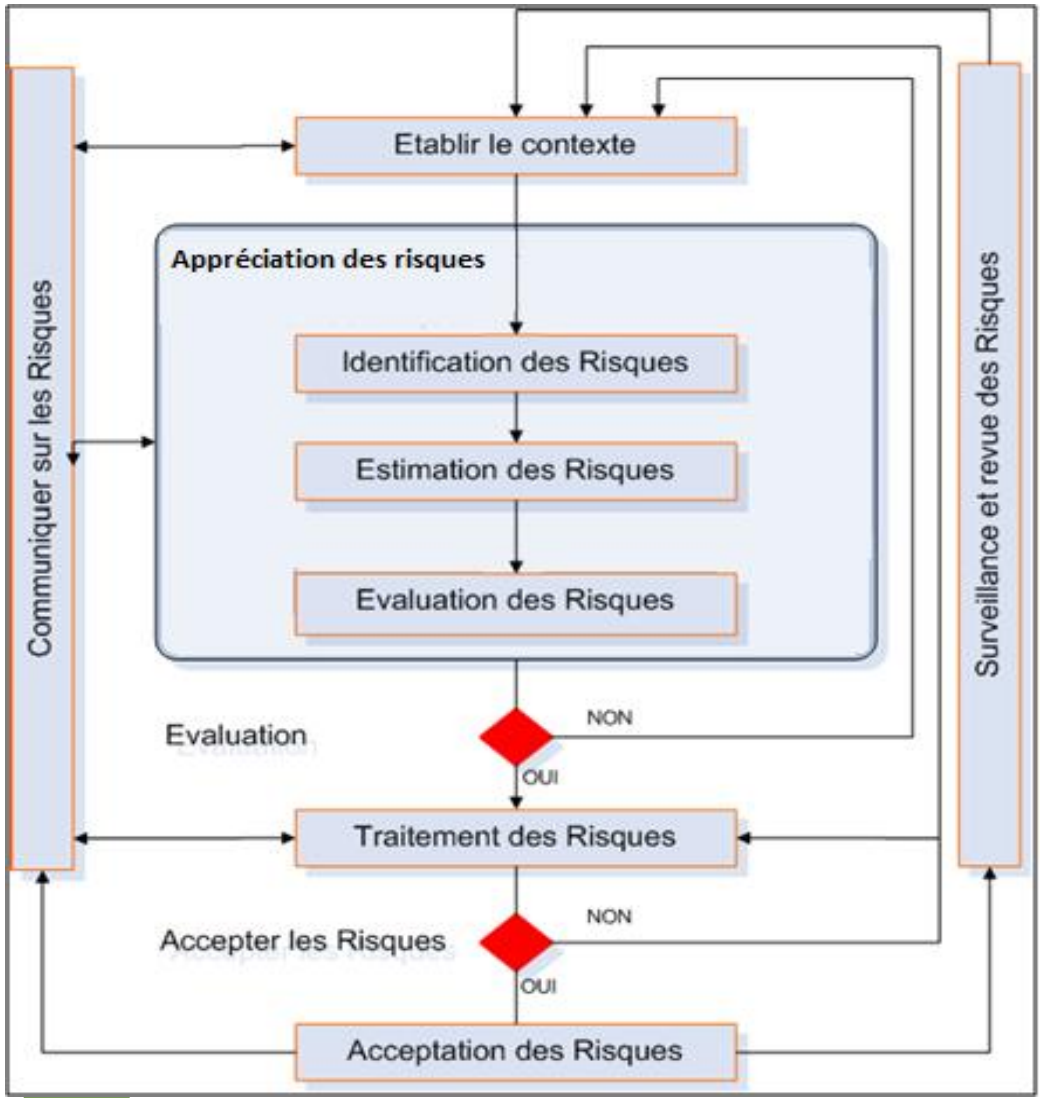
ISO 27005 : **Norme** (internationale)

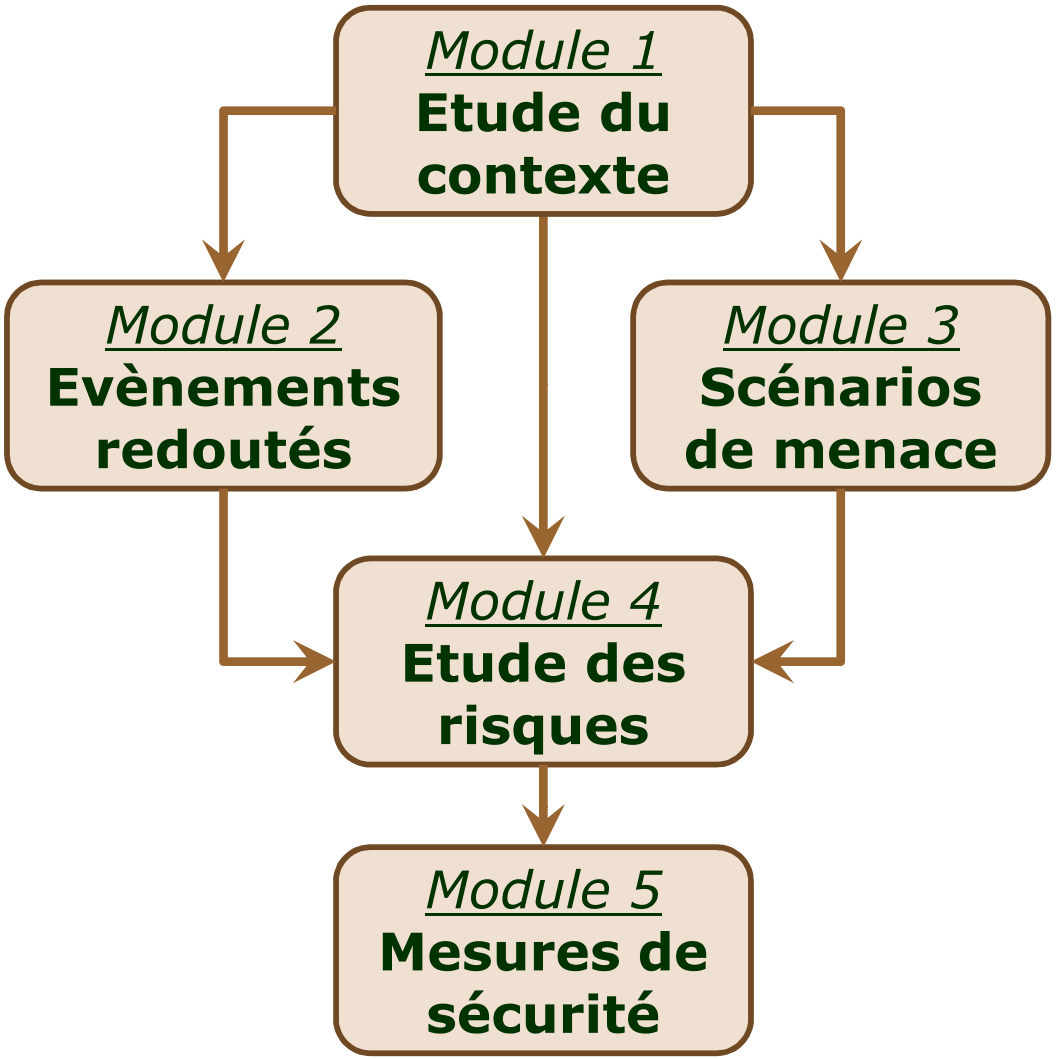
- Gestion de la sécurité
- Inclut un descriptif de résultat à atteindre
- Inclut un cycle d'amélioration permanente
- Inclut un module de communication
- Inclut le cycle d'amélioration permanente

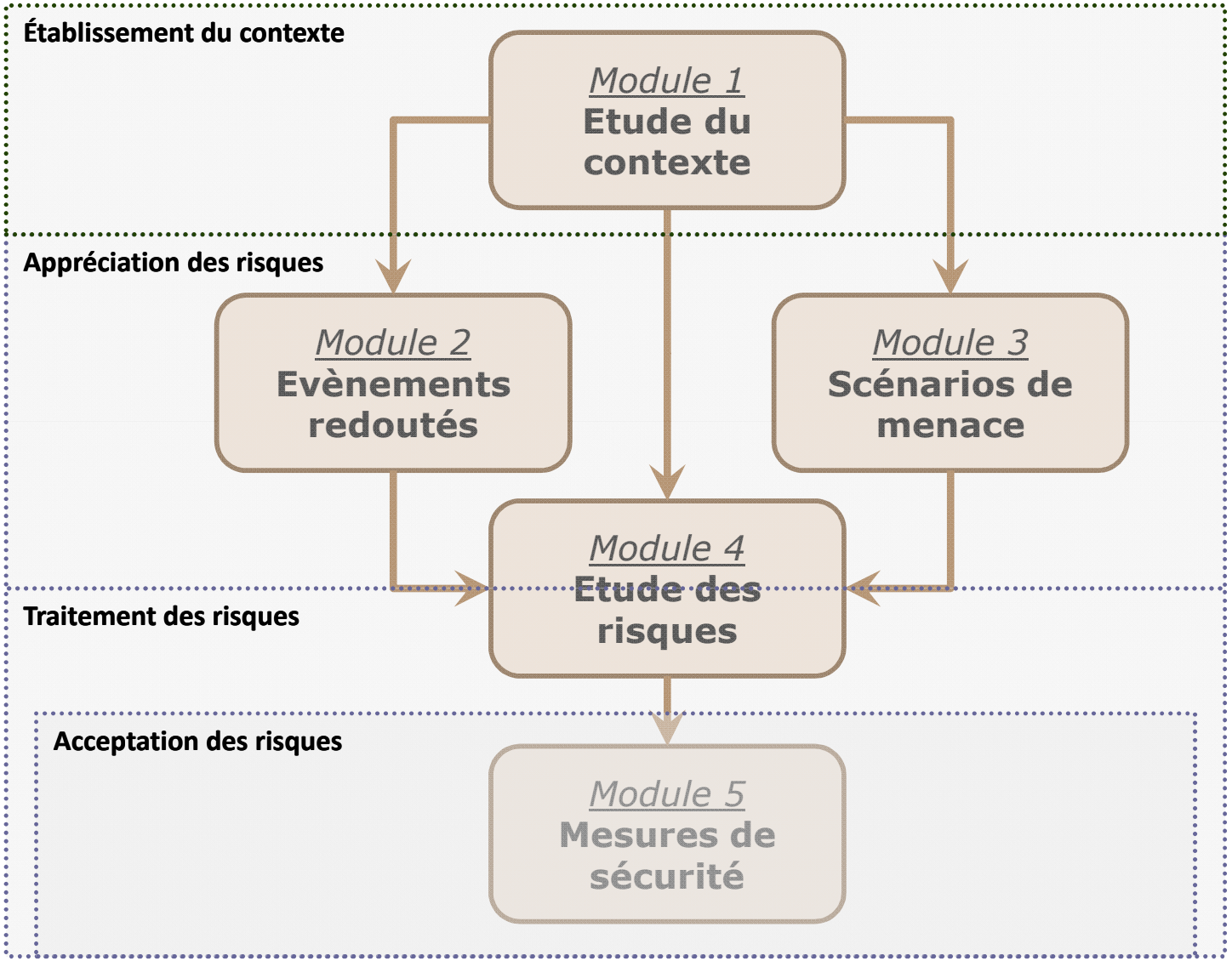
EBIOS : **Méthode** (française)

- Développée par l'ANSSI
- Décrit la méthode avec précision
- Compatible avec la partie analyse de 27005

ISO 27005 ⇔ EBIOS






Établissement du contexte
Module 1
Etude du contexte
Appréciation des risques
Module 2
Evènements redoutés
Module 3
Scénarios de menace
Module 4
Etude des risques
Traitement des risques
Acceptation des risques
Module 5
Mesures de sécurité

- Quelques différences :

  - **EBIOS** ne présente que l'analyse du risque
  - **ISO27005** y ajoute la gestion et le cycle PDCA

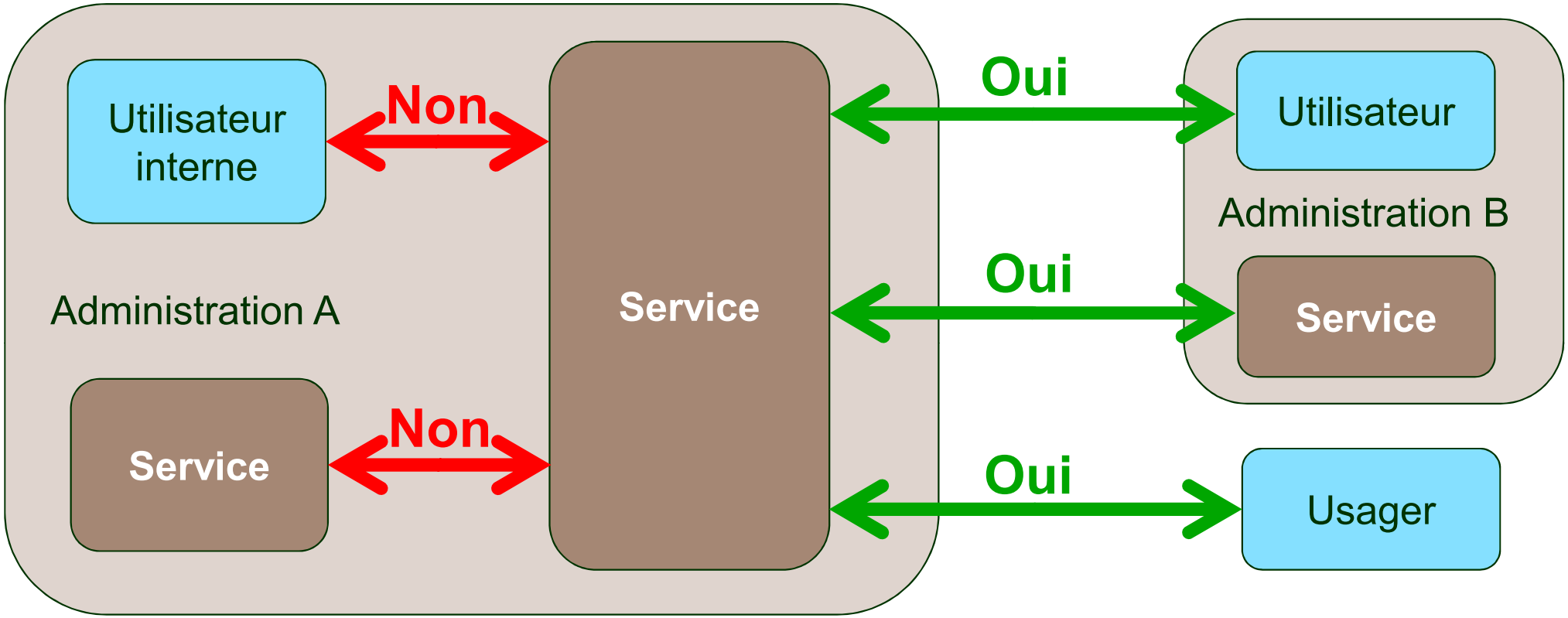
  - **ISO 27005** distingue les biens essentiels et les biens supports mais pas les critères et actions associées
  - **EBIOS** fait une distinction claire entre les critères et actions
    - **Biens essentiels** ➔critères de sécurité, évènements redoutés, gravité
    - **Biens support** ➔menaces, vulnérabilités, scénarios

Sommaire

Le référentiel Général de Sécurité

- D'où vient-il ?
  - Il a été mis en place pour répondre à la loi de 2005 (loi de confiance dans l'économie numérique)
- A qui s'adresse-t-il ?
  - Aux télé-services administratifs, c'est-à-dire :
    - Aux échanges entre une administration et un usager
    - Aux échanges entre les administrations
- Dans quelle version est-il ?
  - Dans la version 2 de 2014
- A quelle partie du SI s'adresse-t-il ?
  - A la partie échange de donnée entre l'utilisateur et le service

Le référentiel Général de Sécurité



Le RGS ne s'intéresse qu'à la transmission et à la sécurité des données transmises

Le référentiel Général de Sécurité

- Quelles sont les fonctions concernées par le RGS ?
  - **L'authentification** (de l'usager, du service)
  - **Le chiffrement** (des transferts)
  - **La signature** (par l'agent, le service)
  - **L'horodatage**
- Quelles sont les exigences du RGS ?
  - Homologuer les télé-services
  - Utiliser des produits et services agréés pour le niveau requis
  - Appeler des prestataires agréés pour les mettre en place
  - Appeler des consultants agréés pour les audits et analyses

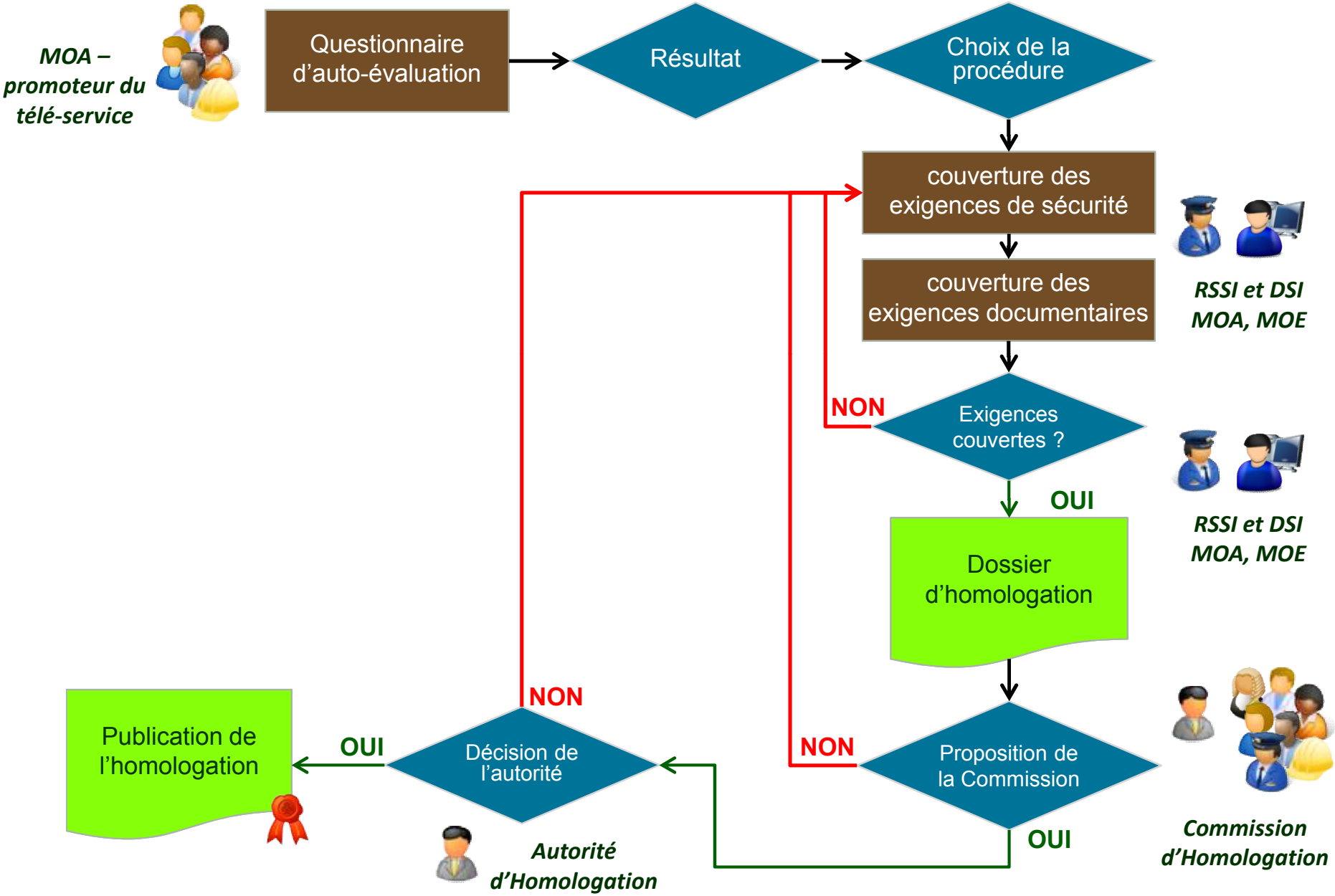
Le référentiel Général de Sécurité

- L'homologation se prononce en interne sur avis d'une commission après instruction du dossier
- Le processus d'homologation proposé par l'ANSSI est en 9 étapes :
  - Quel système d'information dois-je homologuer et pourquoi ?
  - Quel type de démarche dois-je mettre en œuvre ?
  - Qui contribue à la démarche ?
  - Comment s'organise-t-on pour recueillir et présenter les informations ?
  - Quels sont les risques pesant sur le système ?
  - La réalité correspond-elle à l'analyse ?
  - Quelles sont les mesures de sécurité supplémentaires à mettre en œuvre pour couvrir ces risques ?
  - Comment réaliser la décision d'homologation ?
  - Qu'est-il prévu pour maintenir la sécurité et continuer de l'améliorer ?

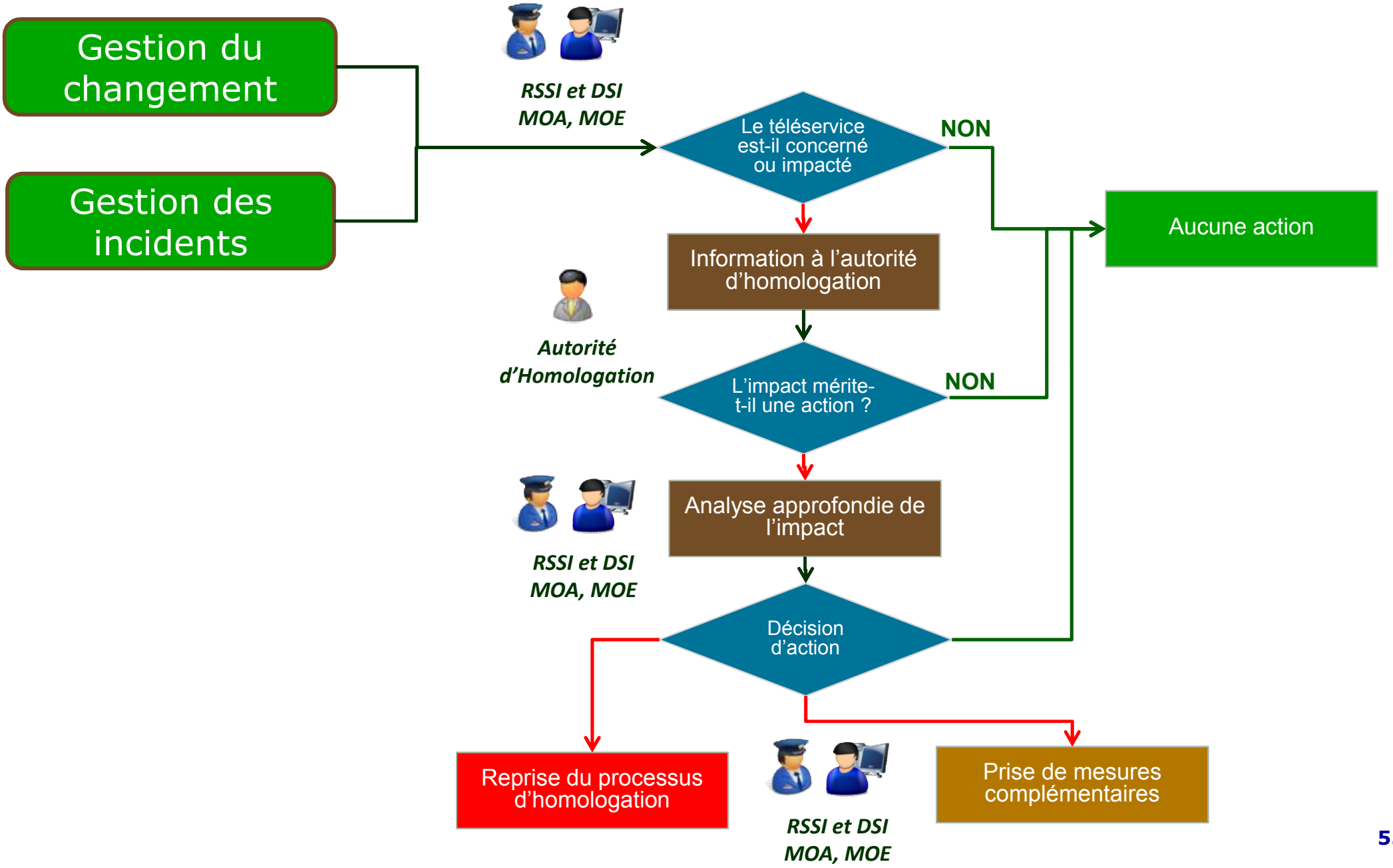
Le référentiel Général de Sécurité

- Le choix de la démarche dépend de l'évaluation:
  - De la maturité de l'administration
  - De la sensibilité du télé-service
- Suivant le résultat de l'évaluation, 4 niveaux de démarche peuvent être engagés (l'ANSSI s'est éclaté en musique):
  - Pianissimo
  - Mezzo-Piano
  - Mezzo-Forte
  - Forte

Démarche d'homologation



Démarche de révision de l'homologation



Le référentiel Général de Sécurité

- Suivant la démarche demande de produire tout ou partie des documents suivants :
  - Stratégie d'homologation
  - Référentiel de sécurité
  - Risques identifiés et objectifs de sécurité
  - Politique de sécurité des systèmes d'information
  - Procédures d'exploitation sécurisée du système
  - Journal de bord de l'homologation
  - Certificats de qualification des produits ou prestataires
  - Résultats d'audits
  - Liste des risques résiduels
  - Décision d'homologation
  - Tableau de bord des incidents et de leur résolution
  - Résultats d'audits intermédiaires
  - Journal des évolutions du système

Sommaire

Retours d'expérience

- Périmètre de l'analyse de risque :
  - Pourquoi le périmètre est essentiel ?
  - Quels biens essentiels retenir ?
  - Quelle granularité ?

- Définition des métriques de l'analyse de risques :
  - Combien de niveau ?
  - Quelle définition ?

Retours d'expérience

- Critères de traitement des risques :
  - Comment définir le plan de traitement ?
    - Objectifs de sécurité, budget, efficacité des mesures ?

- Difficulté de la validation des analyses par les décideurs
  - Cas de l'homologation RGS

Retours d'expérience

- Outillage de l'analyse de risques :
  - Document Excel, Word… (difficile à lire et à maintenir)
  - Des outils qui servent de guide :
    - EBIOS ANSSI http://www.ssi.gouv.fr/guide/ebios-2010-expression-des-besoins-et-identification-des-objectifs-de-securite/
    - M@RGERIDE (Excel – Ministère de la Défense)
  - Des outils à valeur ajoutée :
    - MEHARI (Excel automatisé réalisant des analyses de risques) https://www.clusif.asso.fr/fr/production/mehari/download.asp
    - SOGERISK (Développement Excel-Word automatisé réalisant des analyses de risques EBIOS)
    - EGERIE RiskManager (application web réalisant de la gestion des risques ISO 27005) http://www.egerie-software.com/

En conclusion !!!!!!

Merci

Analyse de risques, ISO 27005, EBIOS, RGS

Walter YANGUERE

Mathieu CHARBOIS

Pierre-Yves DUCAS