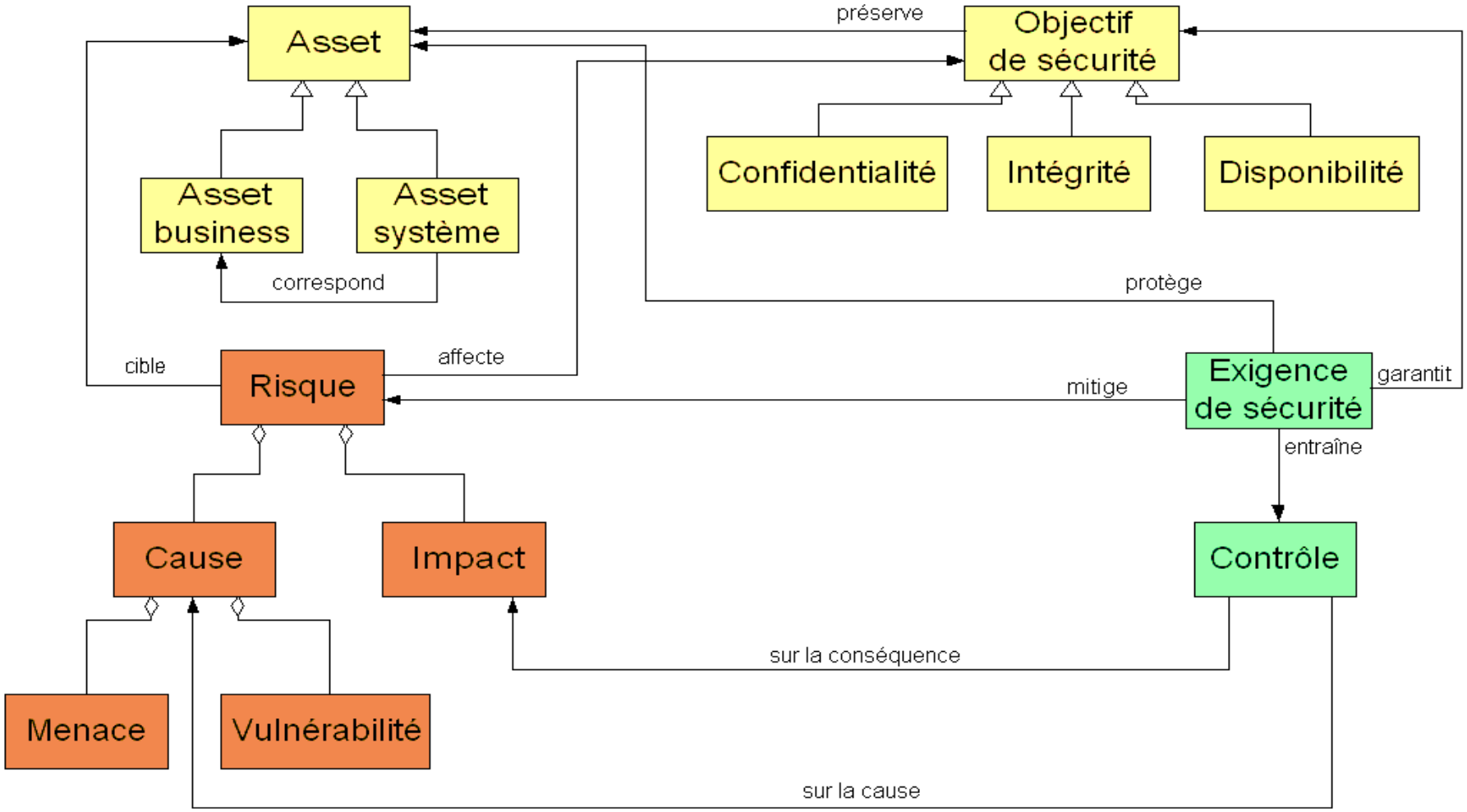
ANALYSE DES RISQUES

Gestion des risques

- La gestion des risques est définie par l'ISO comme l'ensemble des activités coordonnées visant à diriger et piloter un organisme vis-à-vis du risque. On dégage en général trois finalités à la gestion des risques pour les SI :

1. Améliorer la sécurisation des systèmes d'information.
2. Justifier le budget alloué à la sécurisation du système d'information.
3. Prouver la crédibilité du système d'information à l'aide des analyses effectuées.

Les concepts de la gestion des risques



Les assets

Les assets sont définis comme étant l'ensemble des biens, actifs, ressources ayant de la valeur pour l'organisme et nécessaires à son bon fonctionnement.

Du côté des assets business, on retrouve principalement des informations (par exemple des numéros de carte bancaire) et des processus (comme la gestion des transactions ou l'administration des comptes).

On retrouve dans les **assets système** les éléments techniques, tels les matériels, les logiciels et les réseaux, mais aussi l'environnement du système informatique, comme les utilisateurs ou les bâtiments.

Les objectifs de sécurité

C'est cet ensemble qui forme le SI. Le but de la gestion des risques est donc d'assurer la sécurité des assets, sécurité exprimée la plupart du temps en termes de confidentialité, intégrité et disponibilité, constituant les objectifs de sécurité.

Les risques de sécurité

Les assets à protéger sont soumis à des risques de sécurité. Le guide de l'ISO définit un risque par la combinaison de la probabilité d'un événement et de ses conséquences. Cette définition est généralement étendue et défini à l'aide de l'équation du risque :

RISQUE = MENACE * VULNÉRABILITÉ * IMPACT

Cette équation est celle qui est la plus couramment utilisée et la plus reconnue dans le domaine de la gestion des risques. Elle joue un rôle fondamental dans l'identification et l'évaluation du risque.

Les risques de sécurité

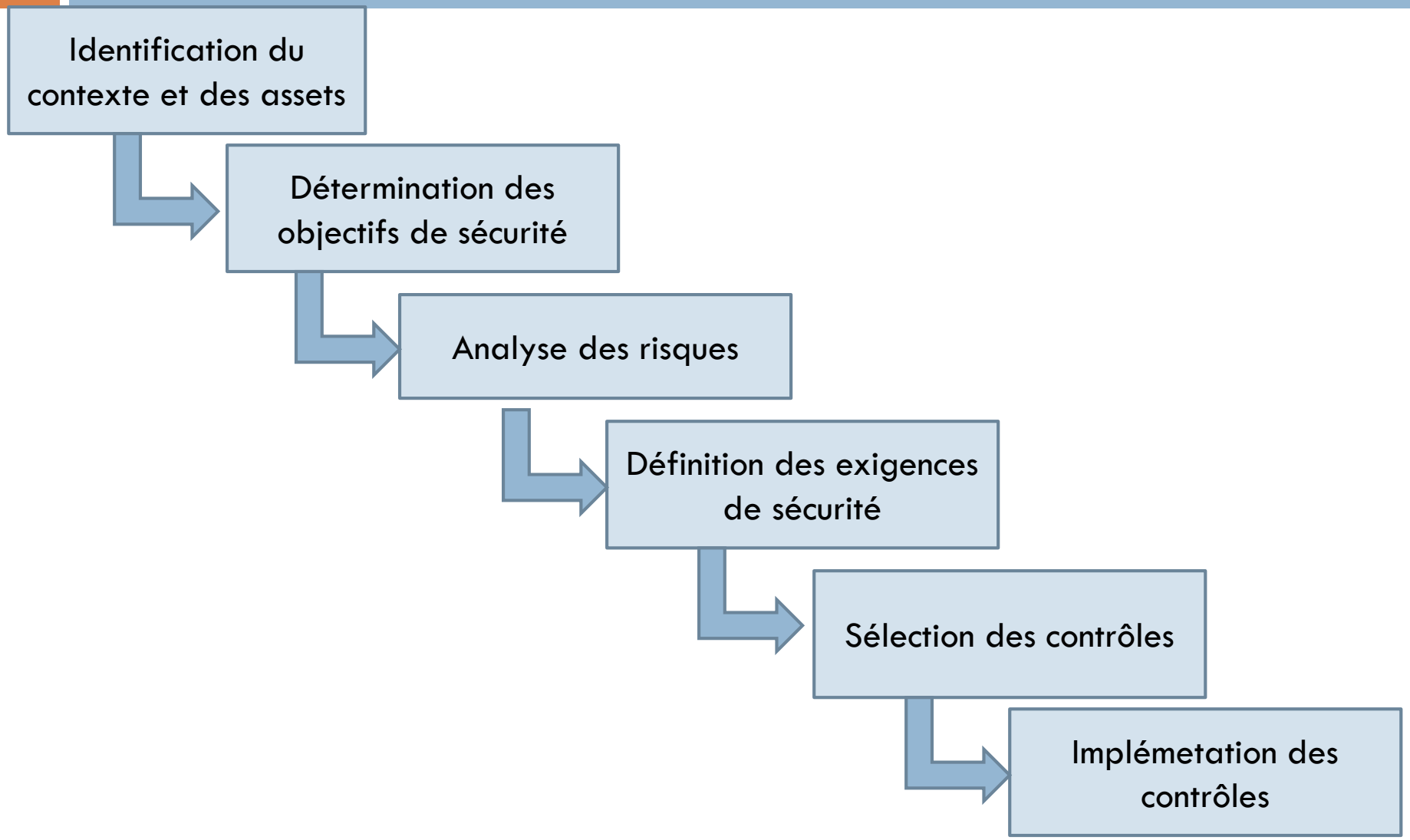
La menace (la source du risque) est l'attaque possible d'un élément dangereux pour les assets. C'est l'agent responsable du risque.

La vulnérabilité est la caractéristique d'un asset constituant une faiblesse ou une faille au regard de la sécurité.

L'impact représente la conséquence du risque sur l'organisme et ses objectifs.

La menace et la vulnérabilité, représentant la cause du risque, peuvent être qualifiées en termes de potentialité. L'impact peut, quant à lui, être qualifié en termes de niveau de sévérité.

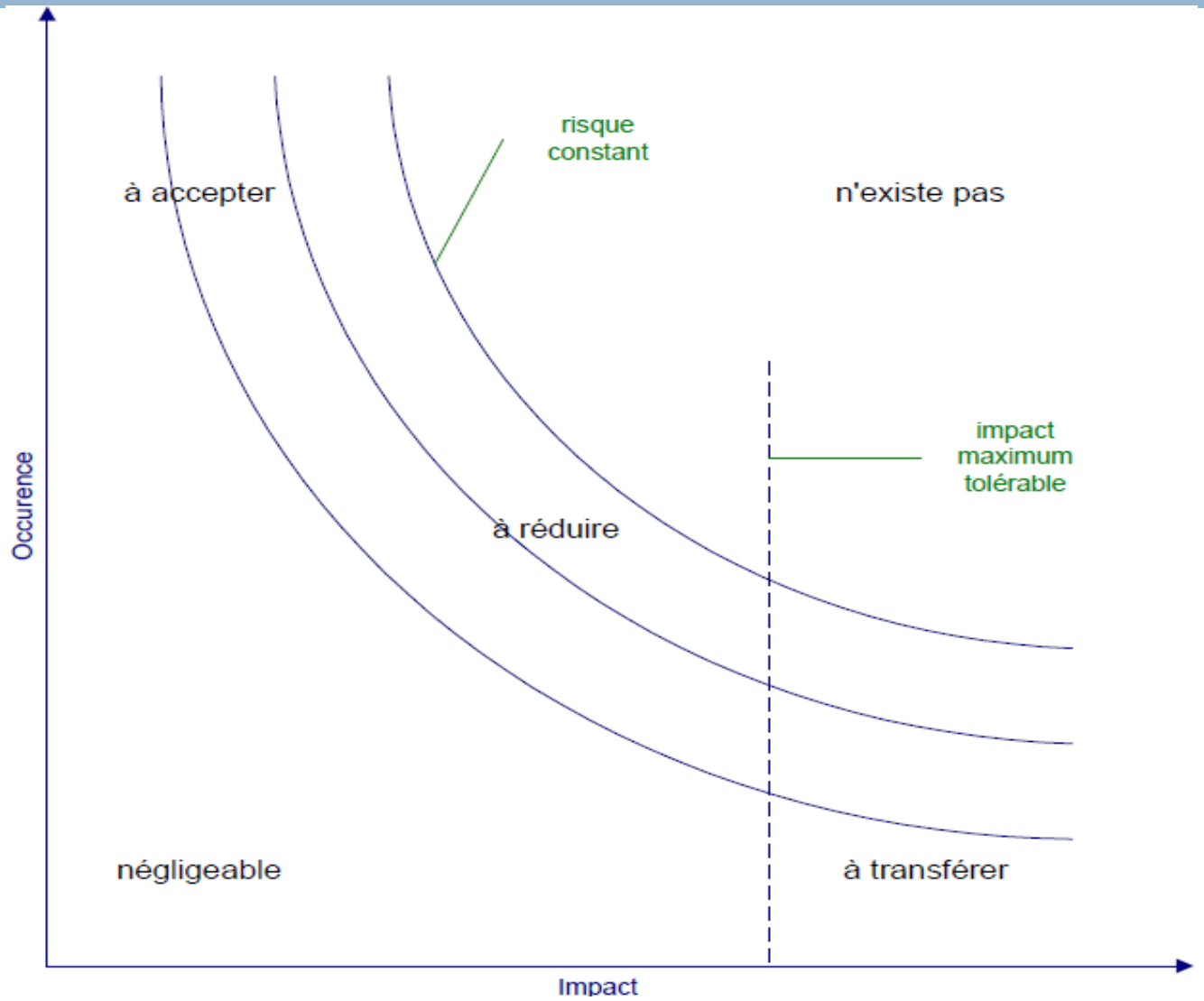
Le processus de gestion des risques



Le processus de gestion des risques

- **L'identification du contexte des assets** consiste à prendre connaissance avec l'organisation, son environnement, son SI et de déterminer précisément les limites du système sur lequel va porter l'étude de gestion des risques.
- **La détermination des objectifs de sécurité** vise à spécifier les besoins en termes de confidentialité, intégrité et disponibilité des assets au niveau business et au niveau du système.
- **L'analyse des risques** a pour finalité l'identification et l'estimation de chaque composante du risque (menace/vulnérabilité/impact), afin d'évaluer le risque et d'apprécier son niveau,

Les différentes zones de risque



Les différentes zones de risque

- Les risques ayant une occurrence et un impact faible sont négligeables.
- Les risques ayant une forte occurrence et un impact important ne doivent pas exister, autrement une remise en cause des activités de l'entreprise est nécessaire.
- Les risques ayant une occurrence forte et un impact faible sont acceptés, leur coût est généralement inclus dans les coûts opérationnels de l'organisation.
- Les risques ayant une occurrence faible et un impact lourd sont à transférer. Ils peuvent être couverts par une assurance ou un tiers.
- Les autres risques, en général majoritaires, sont traités au cas par cas et sont au centre du processus de gestion des risques ; l'objectif, étant de diminuer les risques en les rapprochant au maximum de l'origine de l'axe (mitigation du risque à l'aide de contrôles).

Le processus de gestion des risques

- **La définition des exigences de sécurité** est souvent effectuée de manière incrémentale et par raffinement successif. En effet, on conseille bien souvent de débuter par des exigences générales (de niveau stratégique) pour les raffiner ensuite en des exigences plus précises (vers le niveau opérationnel).
- **La sélection des contrôles:** Les contrôles sont l'instanciation des exigences de bas niveau pour le système cible étudié. Ici sont définis les choix techniques des solutions de sécurité, influencés par le système déjà en place, les compétences disponibles …
- Une fois les contrôles sélectionnés, il reste alors à les **Implémenter** dans le SI et à éventuellement les tester et les évaluer.

Méthodes d'analyse des risques

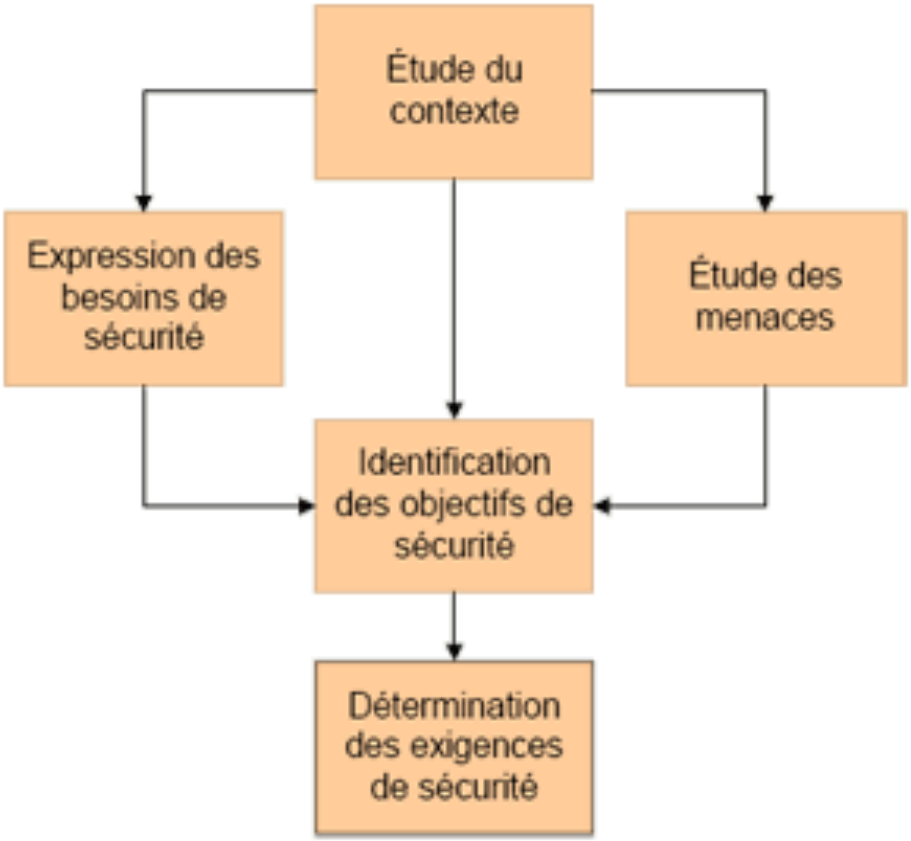
- Plus de 200 méthodes de gestion/analyse des risques sont déclinées actuellement à travers le monde.
  - **EBIOS** (Expression des Besoins et Identification des Objectifs de Sécurité) .
  - **MEHARI** (Méthode Harmonisée d'Analyse de RIsques).
  - **OCTAVE** (Operationally Critical Threat, Asset, and Vulnerability Evaluation).

EBIOS

Créée en 1995, se compose de cinq guides (Introduction, Démarche, Techniques, Outillages pour l'appréciation des risques et Outillages pour le traitement des risques) et d'un logiciel support. Sa diffusion est gratuite. La méthode a pour objectif la formalisation d'objectifs de sécurité adaptés aux besoins du système audité (et de son contexte).

EBIOS

Démarche EBIOS globale



EBIOS

- L'**étude du contexte** Cette étape délimite le périmètre de l'étude : architecture du système d'information, contraintes techniques et réglementaires, le détail des équipements, des logiciels et de l'organisation humaine de l'entreprise...
- L'**expression des besoins de sécurité** permet d'estimer les risques et de définir les critères de risque. Les utilisateurs du SI expriment durant cette étape leurs besoins de sécurité en fonction des impacts .
- L'**étude des menaces** permet d'identifier les risques en fonction non plus des besoins des utilisateurs mais en fonction de l'architecture technique du système d'information (matériels, de l'architecture réseau et des logiciels employés).

EBIOS

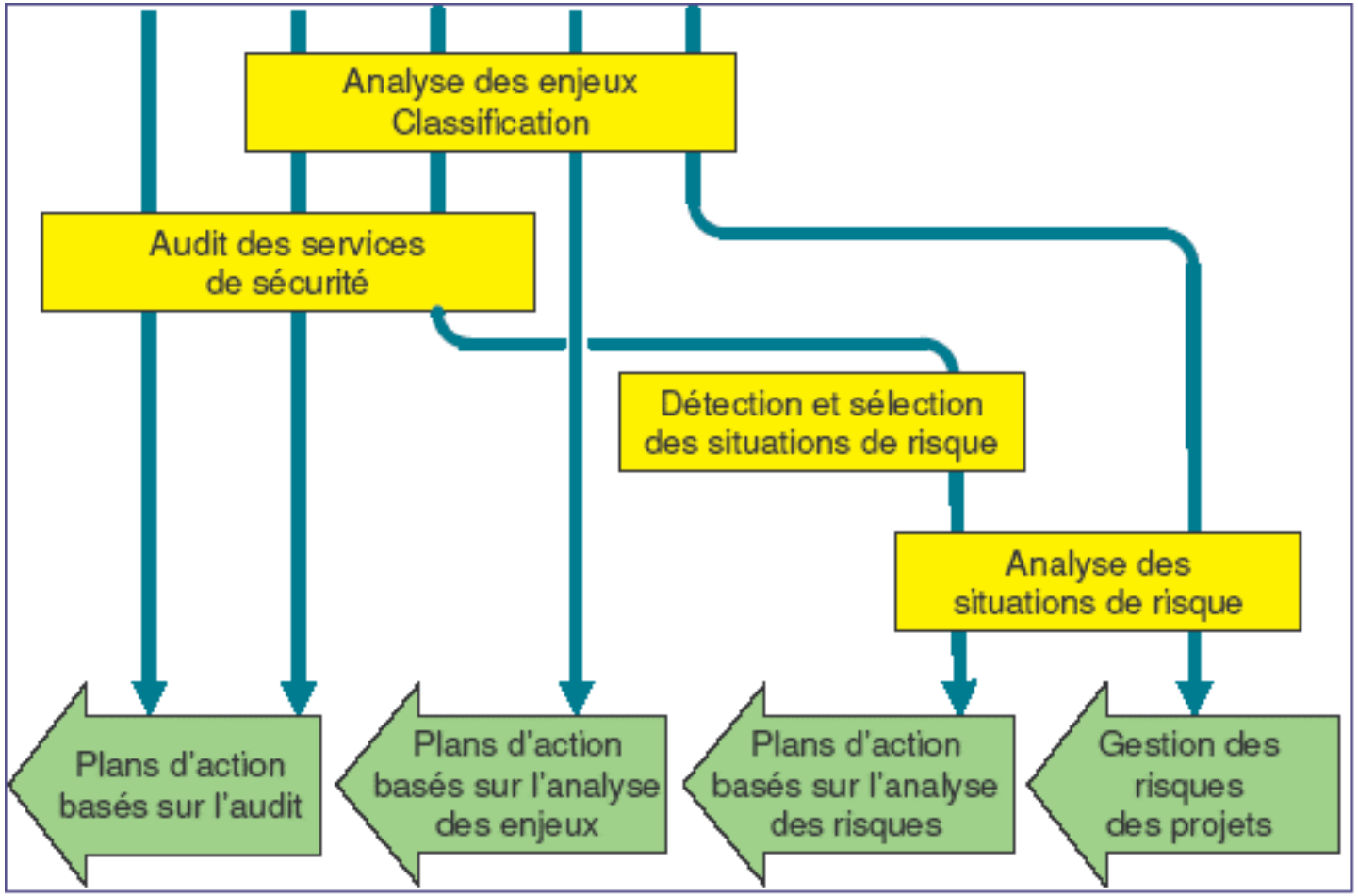
- L'**identification des objectifs de sécurité** confronte les besoins de sécurité exprimés et les menaces identifiées afin de mettre en évidence les risques contre lesquels le SI doit être protégé.
- La **détermination des exigences de sécurité** permet de déterminer jusqu'où on devra aller dans les exigences de sécurité. Il est évident qu'une entreprise ne peut faire face à tout type de risques, certains doivent être acceptés afin que le coût de la protection ne soit pas exhorbitant.

EBIOS fournit donc la méthode permettant de contruire une politique de sécurité en fonction d'une analyse des risques qui repose sur le contexte de l'entreprise et des vulnérabilités liées à son SI

MEHARI

- MEHARI demeure une des méthodes d'analyse des risques les plus utilisées actuellement. Elle est dérivée de deux autres méthodes d'analyse des risques (MARION et MELISA). MEHARI est maintenue en France par le CLUSIF (Club de la Sécurité des Systèmes d'Information Français) , via notamment le Groupe de Travail dédié à cette méthode.

MEHARI



Source CLUSIF

MEHARI

MEHARI est composée de plusieurs modules permettent notamment :

- • D'**analyser les enjeux de la sécurité** (en décrivant les types de dysfonctionnements redoutés) et de classifier les ressources et informations selon les trois critères sécurité de base (Confidentialité, Intégrité, Disponibilité).
- • D'**auditer les services de sécurité**, de manière à prendre en compte l'efficacité de chacun, son contrôle, et de synthétiser les vulnérabilités.
- • D'**analyser les situations de risques**, permettant d'évaluer les potentialités et les impacts intrinsèques, ainsi que les facteurs d'atténuation de risque, puis, enfin, de déduire un indicateur de gravité de risque.

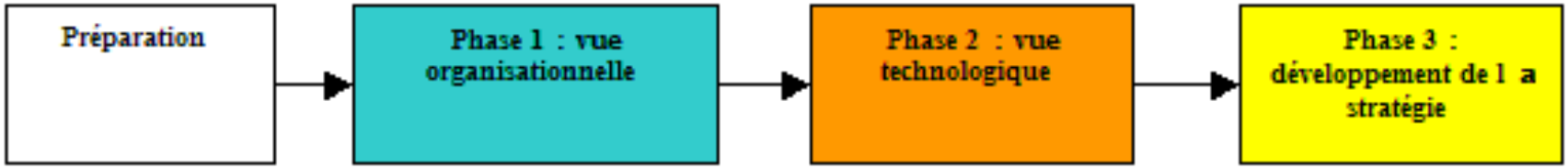
MEHARI

Mehari s'articule autour de 3 types de livrables :

- Le **Plan Stratégique de Sécurité** fixe les objectifs de sécurité ainsi que les métriques permettant de les mesurer. Il définit la politique de sécurité ainsi que la charte d'utilisation du SI pour ses utilisateurs.
- Les **Plans Opérationnels de Sécurité** définissent les mesures de sécurité qui doivent être mises en œuvre. Une évaluation de chaque risque (probabilité, impact) est réalisée permettant d'exprimer les besoins de sécurité, et par la même les mesures de protections nécessaires. Enfin, une planification de la mise à niveau de la sécurité du SI est faite.
- Le **Plan Opérationnel d'Entreprise** assure le suivi de la sécurité par l'élaboration d'indicateurs sur les risques identifiés et le choix des scénarios de catastrophe contre lesquels il faut se prémunir.

OCTAVE

OCTAVE est une méthode d'évaluation des vulnérabilités et des menaces sur les actifs opérationnels. Une fois ces derniers identifiés, la méthode permet de mesurer les menaces et les vulnérabilités pesant sur eux.



OCTAVE

Les trois phases suivantes déclinées au cœur d'OCTAVE, respectent l'analyse progressive des trois blocs des concepts de gestion des risques présentés en amont :

- **La phase 1** (vue organisationnelle) permet d'identifier les ressources informatiques importantes, les menaces associées et les exigences de sécurité qui leur sont associées.
- **La phase 2** (vue technique) permet d'identifier les vulnérabilités de l'infrastructure (ces dernières, une fois couplées aux menaces, créant le risque).
- **La phase 3** de la méthode décline le développement de la stratégie de sécurité et sa planification (protection et plan de réduction des risques).

Critères de choix

- l'origine géographique de la méthode, la culture du pays jouant beaucoup sur le fonctionnement interne des entreprises et leur rapport au risque.
- la langue de la méthode, il est essentiel de maîtriser le vocabulaire employé
- la qualité de la documentation
- la compatibilité avec une norme nationale ou internationale

Critères de choix

- le coût de la mise en œuvre
- la quantité de moyens humains qu'elle implique et la durée de mobilisation
- la taille de l'entreprise à laquelle elle est adaptée
- le support de la méthode par son auteur, une méthode abandonnée n'offre plus la possibilité de conseil et de support de la part son éditeur
- sa popularité, une méthode très connue offre un réservoir de personnels qualifiés pour la mettre en œuvre