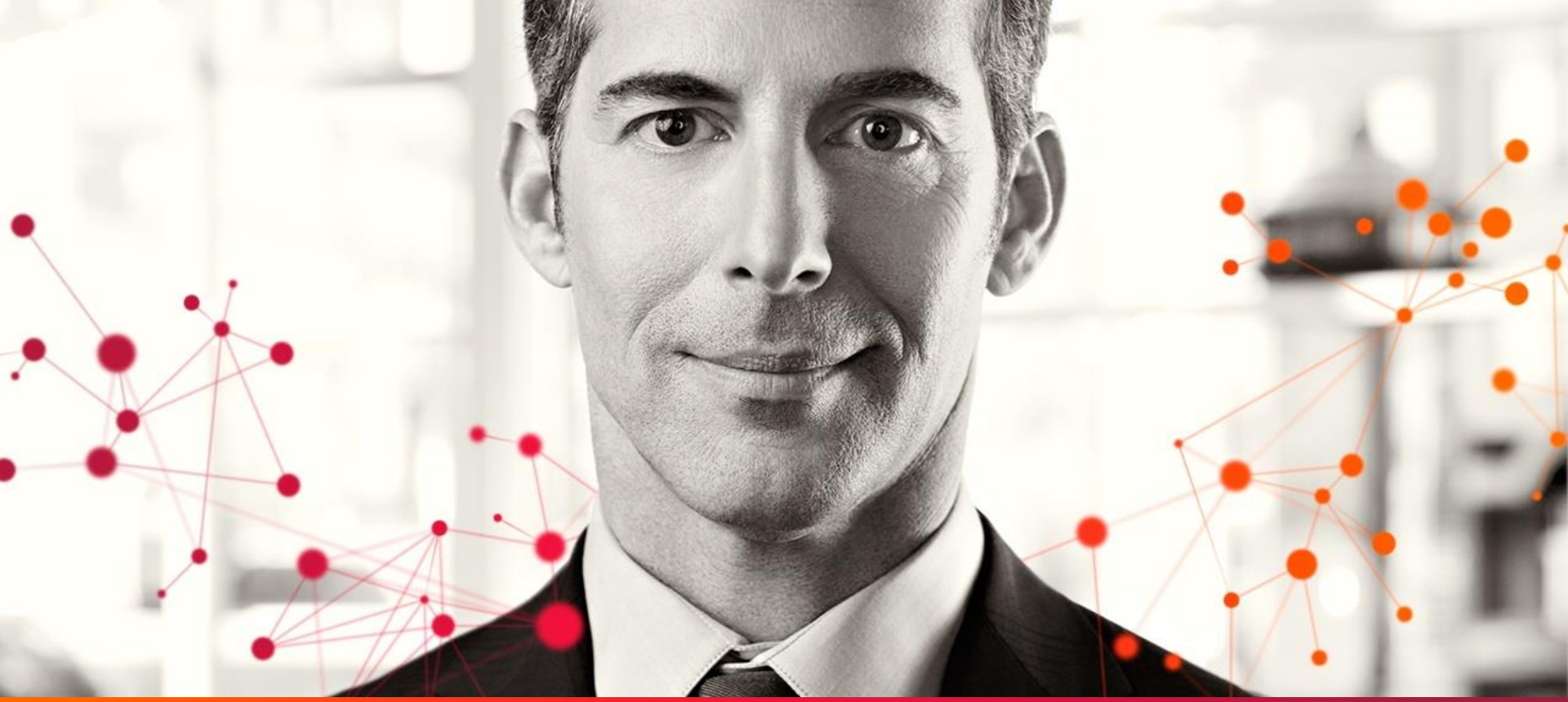


La gestion des risques

CGI | Business Consulting

Généralités

CGI | Business Consulting

Pourquoi faire de la gestion du risque

Se **Prémunir** contre des risques inacceptables

Cibler les efforts et investissements en matière de sécurité

Maintenir un niveau acceptable

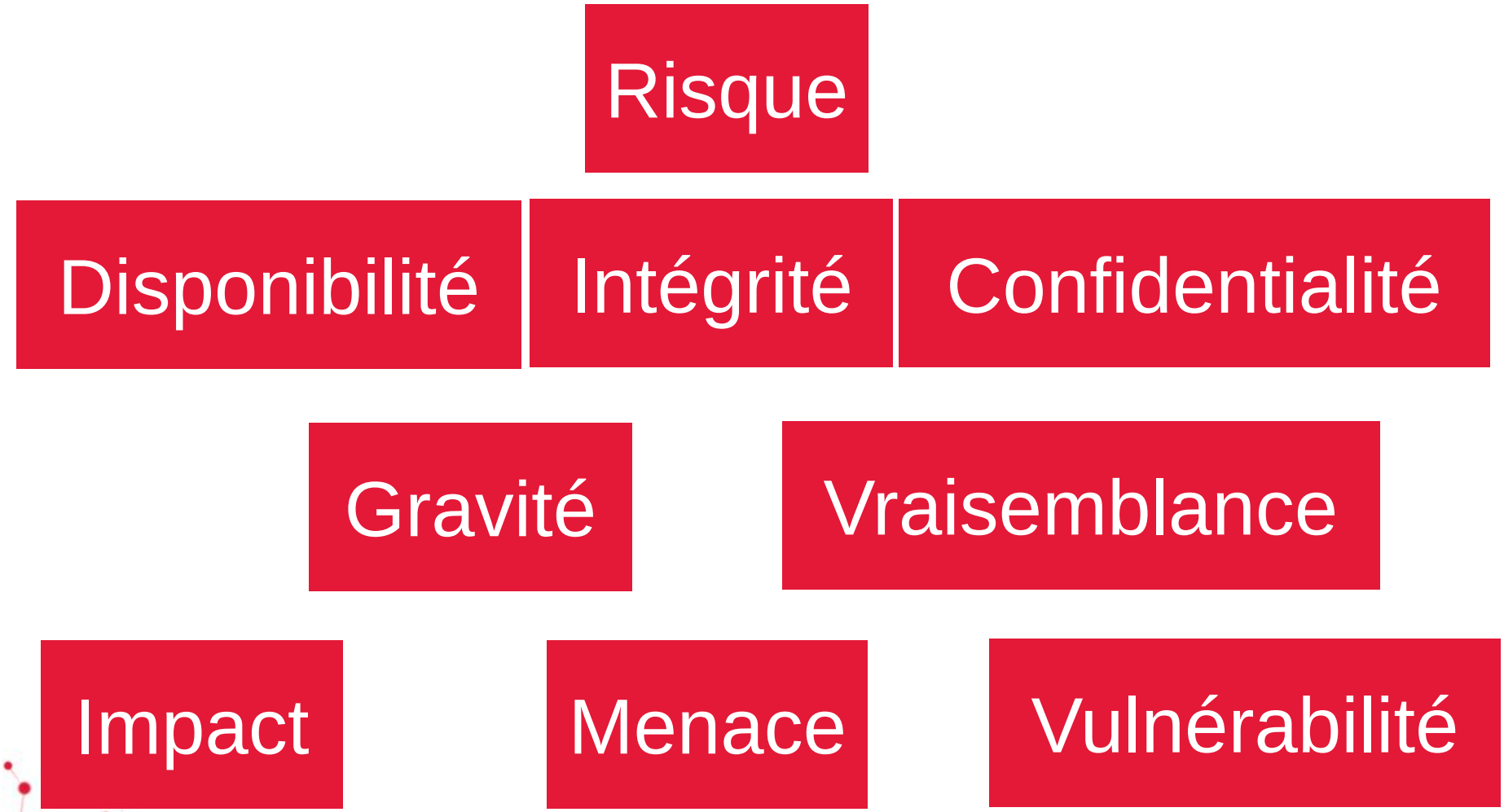
Concepts de la gestion des risques

CGI | Business Consulting

Manque de pot

Quels sont, d'après vous, les risques de cette situation ?

Vue d’ensemble

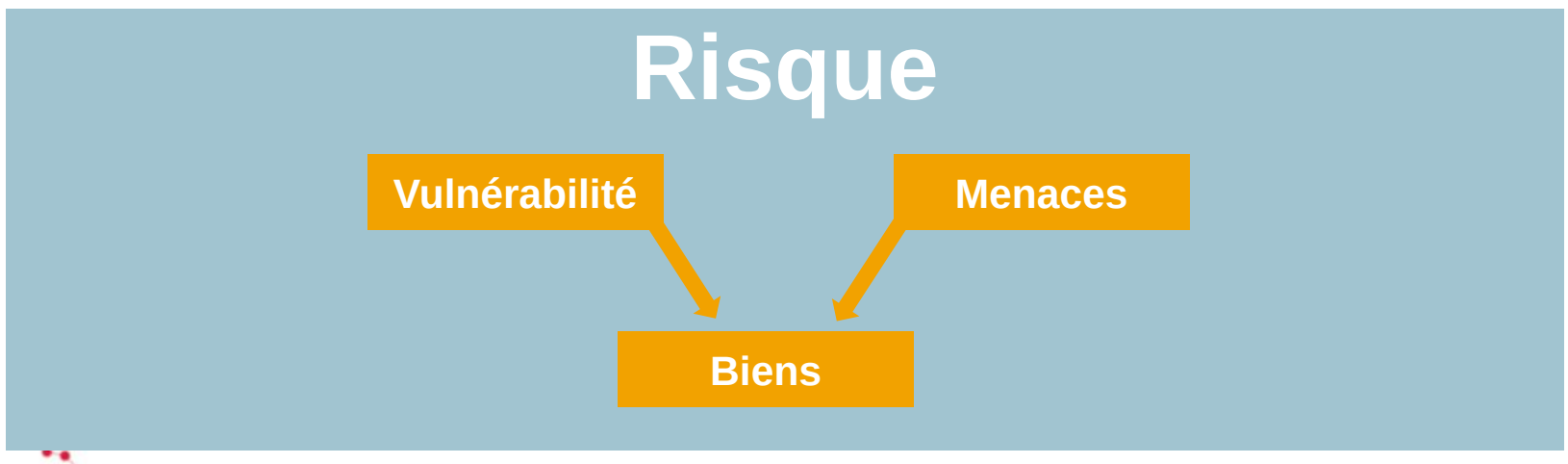


Qu’est-ce qu’un risque ?

Définition d’un **risque**

« Possibilité qu’une menace donnée exploite les vulnérabilités d’un bien (actif) ou d’un groupe de biens (actifs) et nuise donc à l’organisation »

Définition issue de l’ISO 27005



Bien essentiel

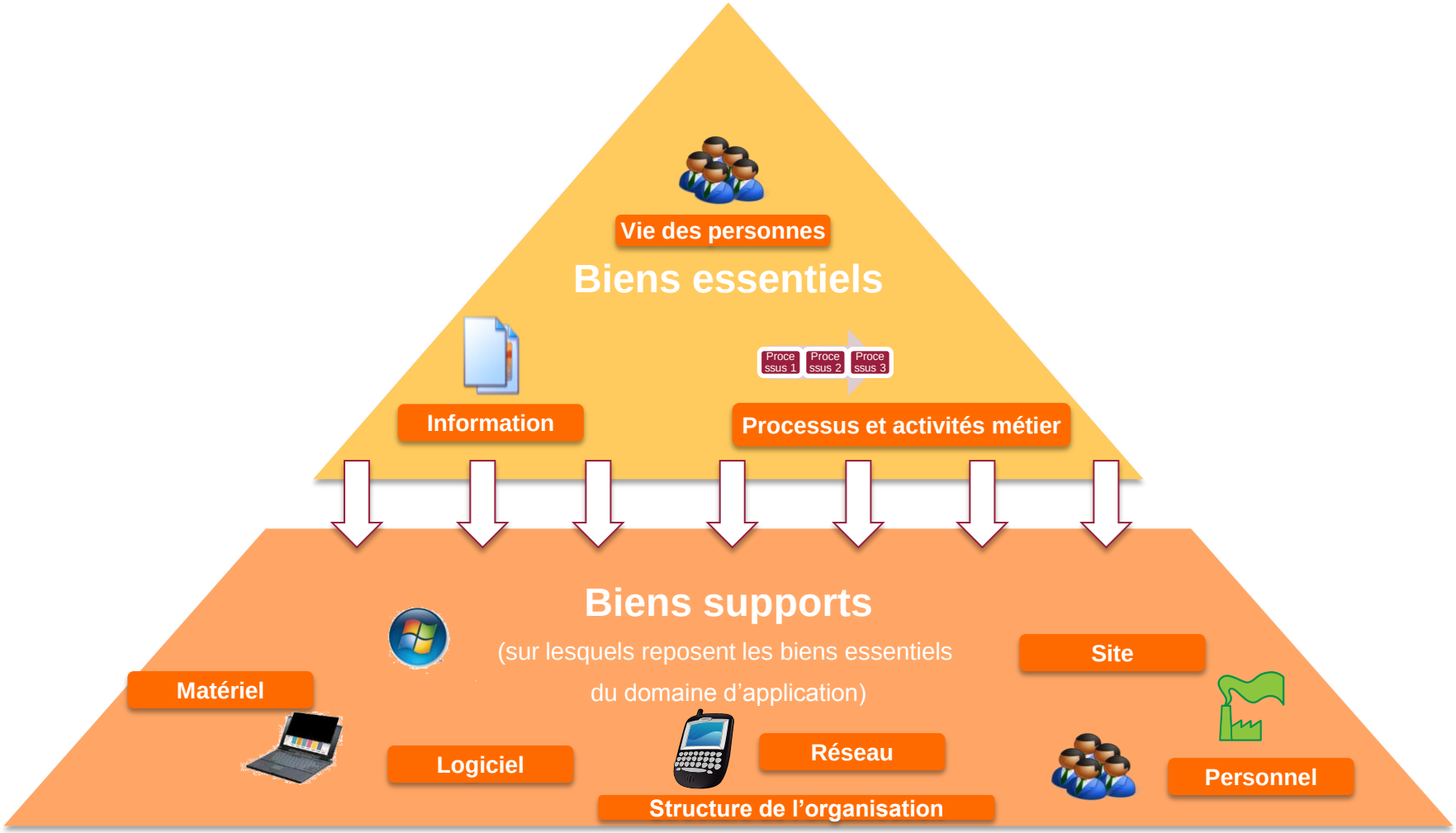
Définition d'un **bien essentiel**

Information ou processus jugé comme important pour l'organisme. On appréciera ses besoins de sécurité, mais pas ses vulnérabilités.

Exemple

Nom d'un salarié
Processus de paye
Processus de délivrance de certificats

Biens essentiels et supports



Besoin de sécurité

Définition d'un **besoin de sécurité**

Définition précise et non ambigüe du niveau d'exigences opérationnelles relatives à un bien essentiel pour un critère de sécurité donné (disponibilité, confidentialité, intégrité, etc.)

Exemple

Le bien essentiel doit être disponible dans les 72 heures
Le bien essentiel doit être rigoureusement intègre
Le bien essentiel est public
Le bien essentiel est confidentiel

Critères de sécurité

Disponibilité

Reflète le besoin que les données soient accessibles : cela peut correspondre à la durée nécessaire pour avoir accès à la donnée ou au taux

Intégrité

État de données (ou d'un traitement) qui lors de leur traitement, de leur conservation ou de leur transmission ne subissent aucune altération ou destruction volontaire ou accidentelle.

Confidentialité

Le fait de s'assurer que l'information n'est seulement accessible qu'à ceux dont l'accès est autorisé

Preuve

Le fait d'apporter les éléments relatifs à la preuve de l'exécution d'une opération ou à l'authenticité d'un acte

Accès

Le fait de s'assurer qu'un traitement n'est réalisable que par des personnes autorisées

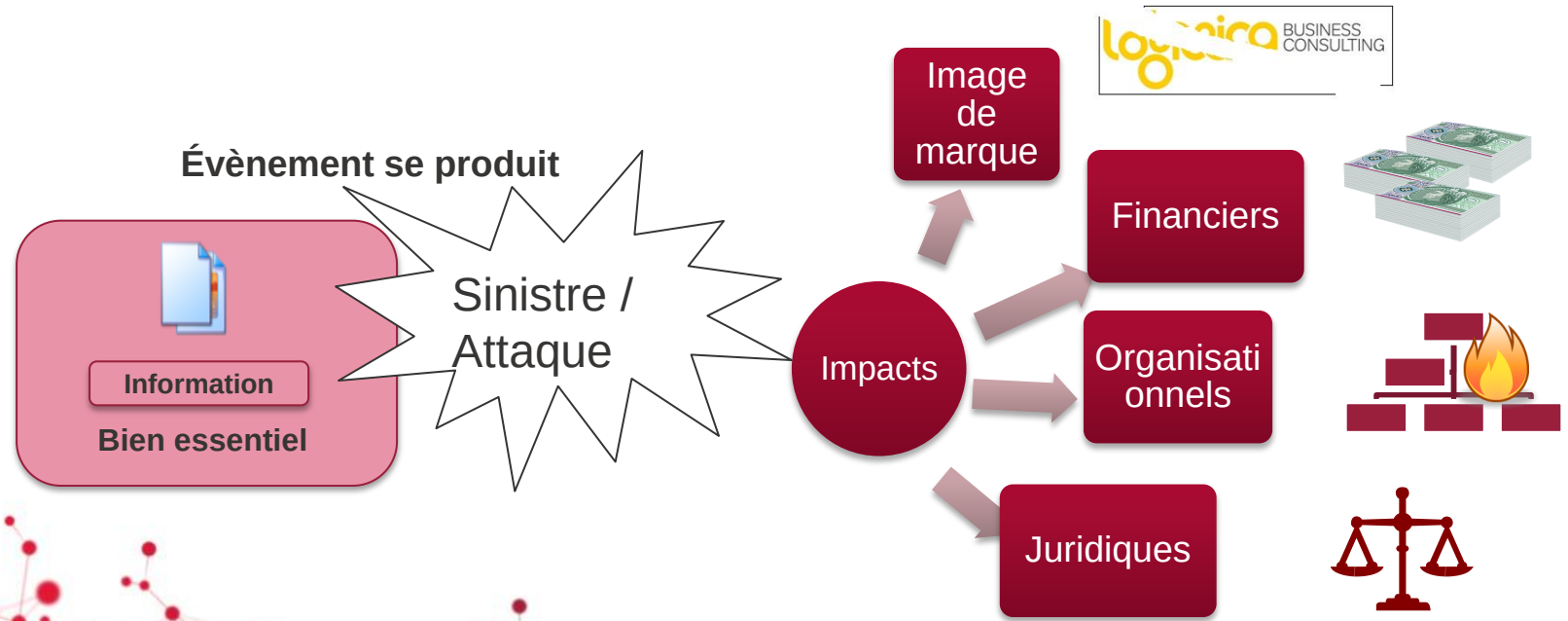
Impact

Définition d'un **impact**

Conséquence directe ou indirecte de l'insatisfaction des besoins de sécurité sur l'organisme ou sur son environnement.

Exemple

Dégradation de l'image de marque
Perte financière à hauteur de 1 million d'euros



CGI | Business Consulting

Gravité

Définition d'une **gravité**

Estimation de la hauteur des effets d'un évènement redouté ou d'un risque. Elle représente ses conséquences.

Exemple

L'entreprise ne surmontera pas les conséquences, l'entreprise surmontera les conséquences sans difficulté

Source de menace

Définition d'une **source de menace**

Chose ou personne à l'origine de menaces. Elle peut être caractérisée par son type (humain ou environnemental), par sa cause (accidentelle ou délibérée) et selon le cas par ses ressources disponibles, son expertise, sa motivation, etc.

Exemple

Administrateur
Client
Pirate
Incendie
Catastrophe
Virus

Bien support

Définition d'un **bien support**

Bien sur lequel reposent des biens essentiels. On distingue notamment les systèmes informatiques, les organisations et les locaux. On appréciera ses vulnérabilités, mais pas ses besoins de sécurité.

Menace

Définition d'une **menace**

Une menace est une méthode utilisée par une source de menace pour provoquer un risque

Délibérée	Non délibérée
• Détournement d'usage • Espionnage • Saturation d'un canal • …	• Destruction • Perte • Saturation d'un canal • …

Vraisemblance

Définition d'une **vraisemblance**

Estimation de la possibilité qu'un scénario de menace ou un risque se produise. Elle représente sa force d'occurrence.

Exemple

Si je suis administrateur de mon poste, la vraisemblance qu'un virus infecte mon ordinateur connecté à Internet est ***très forte.***

La vraisemblance qu'un séisme touche la ville de Paris est ***très faible.***

Vulnérabilité

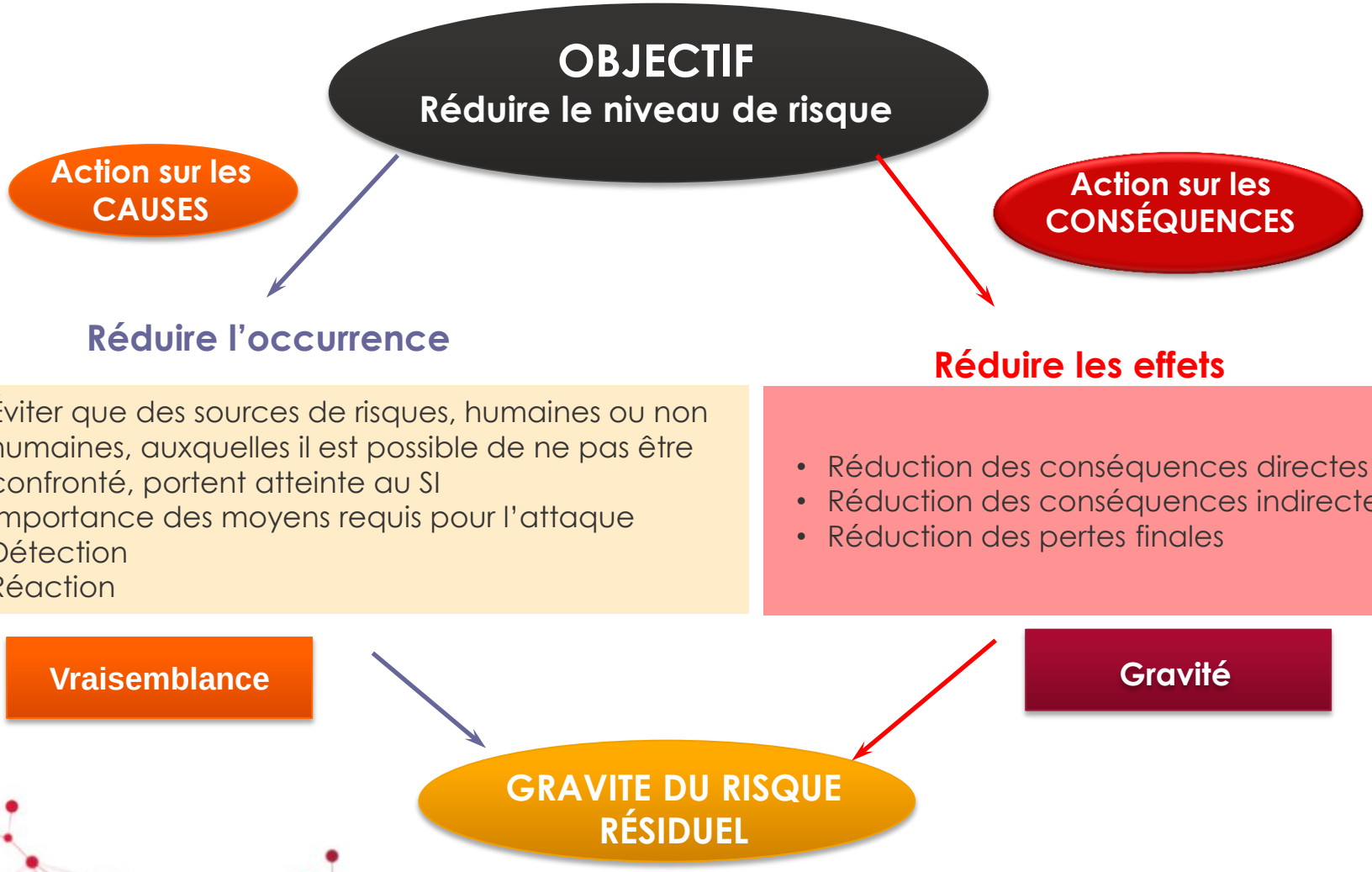
Définition d'une **vulnérabilité**

Caractéristique d'un bien support qui peut constituer une faiblesse ou une faille au regard de la sécurité des SI

Exemples de vulnérabilités

- Émets des signaux compromettants
- Dimensionnement inapproprié
- Sensible aux variations électriques
- Fragile
- Personnel manipulable
- Support falsifiable
- Support observable

Mesures de sécurité



Exercice : classer les notions

Date de naissance d'un membre du personnel

Absence de révision des habilitations

Application de gestion RH

Pirate informatique

Serveur central de l'entreprise

Membre du personnel

Le mécontentement du personnel

Dégradation de l'image de marque de l'entreprise

Classer ces notions parmi les concepts vus dans les diapositives précédentes

De quoi a-t-on besoin ?

- Valeur du bien essentiel considéré
- Exposition aux menaces considérées
- Facilité d'exploitation des vulnérabilités
- Existence de vulnérabilités
- Capacité et motivation des sources de menaces
- Hauteur et nombre des impacts identifiés

- Gravité
- Vraisemblance

Exercice : décomposition du risque SSI

2. Israël – Divulgation d'un projet de raid sur Facebook

Gizmodo.fr du 05.03.2010, The New York Times du 05.03.2010

Un raid surprise a dû être annulé avant-hier à cause d'un soldat israélien qui avait mis à jour son statut Facebook pour indiquer "mercredi nous nettoyons Qatanah, et jeudi, si Dieu le veut, nous rentrons à la maison". Le soldat a depuis été relevé de son poste de combat.

Bien essentiel	
Besoin de sécurité	
Impact	
Source de menace	
Critère de sécurité	
Bien support	
Menace	
Vulnérabilité	

Exercice : décomposition du risque SSI

2. Israël – Divulgation d'un projet de raid sur Facebook

Gizmodo.fr du 05.03.2010, The New York Times du 05.03.2010

Un raid surprise a dû être annulé avant-hier à cause d'un soldat israélien qui avait mis à jour son statut Facebook pour indiquer "mercredi nous nettoyons Qatanah, et jeudi, si Dieu le veut, nous rentrons à la maison". Le soldat a depuis été relevé de son poste de combat.

Bien essentiel	Informations sur un raid surprise
Besoin de sécurité	Secret Défense
Impact	Vies humaines, perte d'une bataille, annulation du raid
Source de menace	Soldat
Critère de sécurité	Confidentialité
Bien support	Soldat
Menace	Divulgation
Vulnérabilité	Maladroit, étourdi, etc.

Synthèse

Méthode EBIOS

CGI | Business Consulting

Introduction

La gestion des risques est largement décrite et préconisée dans la presse, les normes, la règlementation, etc.

EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité) est la **méthode de gestion des risques** de l'ANSSI.

Mais de quoi s'agit-il exactement ?

Rappels

Le risque SSI : Définitions

- Risque SSI
  - ISO/IEC 27005
    - Possibilité qu'une menace donnée exploite les vulnérabilités d'un bien ou d'un groupe de biens et nuise donc à l'organisation.
  - EBIOS
    - **Scénario, avec un niveau donné, combinant un événement redouté et un ou plusieurs scénarios de menaces.**

- Événement redouté
  - EBIOS
    - **Scénario, avec un niveau donné, représentant une situation crainte par l'organisme.**

- Scénarios de menaces
  - EBIOS
    - **Scénarios, avec un niveau donné, décrivant des modes opératoires.**

Le risque SSI : éléments constitutifs

- Un **événement redouté** combine :
  - Les **sources de menace** susceptibles d'en être à l'origine
    - Ex. : un adolescent de 15 ans agissant de manière délibérée par appât du gain
  - Un **bien essentiel**
    - Ex. : résultats scolaires
  - Un **critère de sécurité**
    - Ex. : intégrité
  - Un **besoin de sécurité** concerné
    - Ex. : parfaite intégrité
  - Les **impacts potentiels**
    - Ex. : l'adolescent évite des difficultés scolaires, image du collège.

- Un **scénario de menace** combine :
  - Les **sources** de menaces susceptibles d'en être à l'origine
    - Ex. : l'adolescent de 15 ans
  - Un **bien support**
    - Ex. : système informatique du collège
  - Un **critère de sécurité**
    - Ex. : intégrité
  - Des **menaces**
    - Ex. : intrusion, élévation de privilèges et modification de contenu
  - Les **vulnérabilités** exploitables pour qu'elles se réalisent
    - Ex. : facilité d'accès aux données, possibilité de modifier les données

Le niveau de risque SSI

- Définition
  - Il correspond à l'estimation de sa gravité et de sa vraisemblance.

- Gravité
  - Définition
    - Estimation de la hauteur des effets d'un évènements redouté ou d'un risque. Elle représente ses conséquences.
  - Dépendance
    - de la hauteur et du nombre des impacts,
    - de la valeur du bien considéré,
    - de la motivation des sources de menaces.

- Vraisemblance
  - Définition
    - Estimation de la possibilité qu'un scénario de menace ou qu'un risque se produise. Elle représente sa force d'occurrence.
  - Dépendance
    - de l'exposition aux menaces considérées,
    - de l'existence plus ou moins avérée de vulnérabilités,
    - de la facilité d'exploitation des vulnérabilités identifiées,
    - de la capacité des sources de menaces.

Généralités

EBIOS est le « tout terrain » pour gérer les risques

Management

Doctrine
Stratégie
Politique
Tableau de bord
Plan d'action

Projets

Cadrage
Cahier des charges
FEROS [Guide 150]
Cible de sécurité
Procédures d'exploitation

Produits

Profil de protection [ISO15408]
Cible de sécurité [ISO15408]

Sensibilisation aux risques et mesures, responsabilisation des parties prenantes…

La notion de boîte à outils

- EBIOS est une boîte à outils à usage variable, qui ne sera pas utilisée de la même manière selon :
  - Le sujet étudié (variation de la focale)
    - Ex. : un organisme dans son intégralité, une application particulière…
  - Les livrables attendus (variation des actions et de la forme)
    - Ex. : doctrine SSI, cible de sécurité…
  - L'état du projet (variation de la profondeur)
    - Ex. : étude de faisabilité, maintien en conditions opérationnelles…

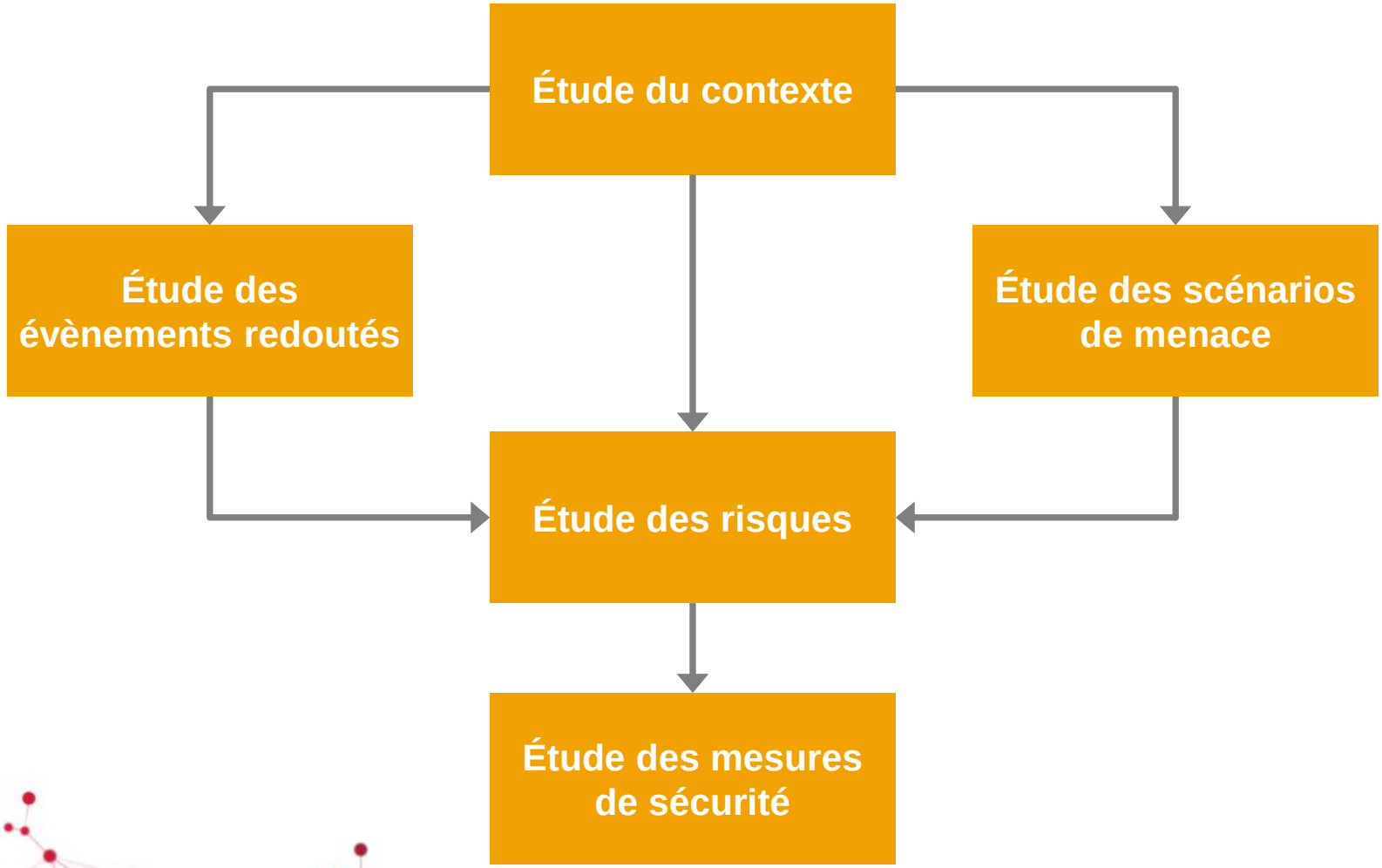
- Une réflexion préalable sur la stratégie de mise en œuvre est donc nécessaire.

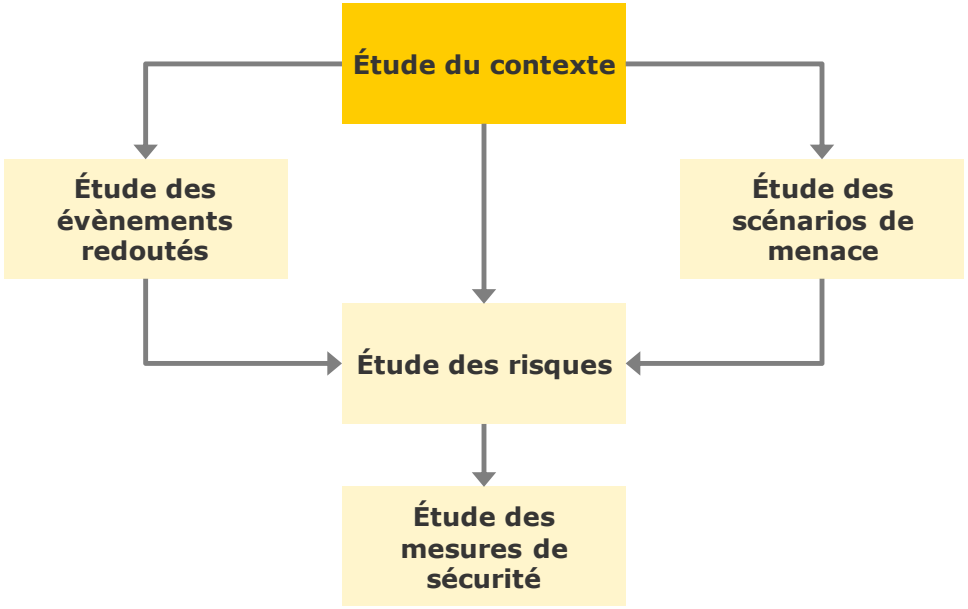
Une application souple

- L'application d'EBIOS s'inscrit dans un cadre de référence.
  - Un cadre lié au sujet de l'étude :
    - Le niveau de maturité SSI,
    - Des référentiels applicables (réglementation, normes, méthodes internes…),
    - Une culture spécifique à l'organisme,
  - Un cadre lié à des parties prenantes variées qui doivent être impliquées :
    - Responsables du périmètre de l'étude
    - Responsables de la sécurité de l'information / RSSI
    - Gestionnaire de risques
    - Autorités de validation
    - Dépositaires de biens essentiels (utilisateurs ou maîtrises d'ouvrage)
    - Propriétaires de biens supports

- Le vocabulaire et les pratiques employés doivent donc être souples pour que la démarche soit efficace.

Les étapes de la méthode





Module 1 – Étude du contexte

La suite ….

…. au TP/TD

Des questions ?