CHAPITRE 1

Fiche savoirs technologiques 1

La typologie des risques et leurs impacts

I Définitions de vulnérabilité, menace et risque

Vulnérabilité (Vulnerability en anglais)	Menace (Threat en anglais)	Risque (Risk en anglais)
En informatique, une vulnérabilité est une faiblesse de la sécurité du système d'information (SI) qui peut affecter son fonctionnement normal.	Une menace est une cause intentionnelle ou non-intentionnelle qui peut entraîner des dommages sur le SI.	Un risque de sécurité du SI est la probabilité de l'exploitation d'une vulnérabilité du SI par une menace. Le niveau d'un risque est estimé en fonction de sa gravité et de la vraisemblance de son apparition.

Les objectifs de la sécurité informatique consistent à limiter les vulnérabilités du SI.

II La typologie des risques informatiques

1. La méthode EBIOS

› EBIOS Risk Manager : www.lienmini.fr/6988-104
› Fiche méthode 5, p. 211

Créée en 2009, l'Agence nationale de la sécurité des systèmes d'information (ANSSI) est l'autorité nationale en matière de cybersécurité. Sa mission est de comprendre, prévenir et répondre au risque cyber.

La méthode EBIOS Risk Manager (Expression des besoins et identification des objectifs de sécurité) développée par l'ANSSI (Agence nationale de la sécurité des systèmes d'information) et retenue par la CNIL (Commission nationale de l'informatique et des libertés) permet d'identifier et de hiérarchiser les différents risques dans un contexte clairement défini.

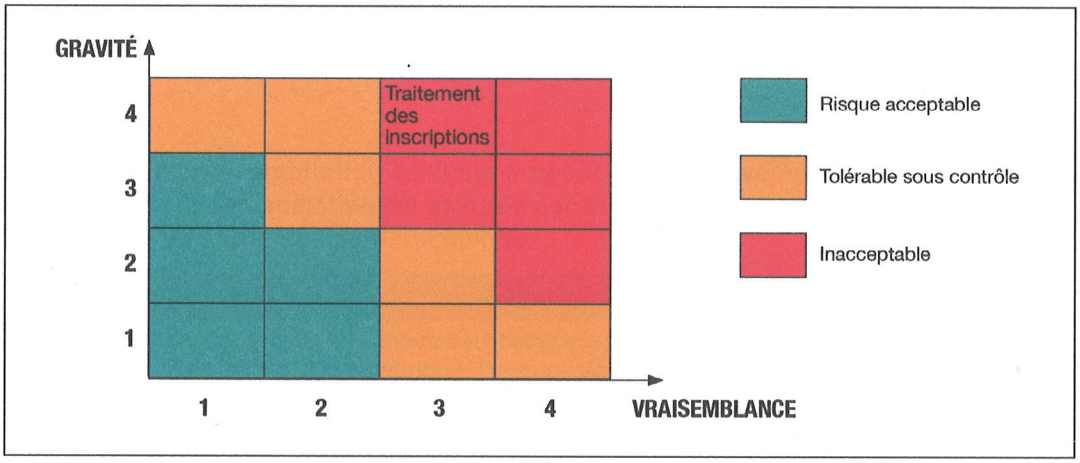
Un risque est défini par l'ANSSI comme « un scénario qui combine un événement redouté et un ou plusieurs scénarios de menaces ». Un événement redouté désigne par exemple la possibilité d'atteindre des données avec des conséquences probables sur la vie privée des personnes concernées.

La (CNIL) est le régulateur des données personnelles. Elle accompagne les professionnels dans leur mise en conformité et aide les particuliers à maîtriser leurs données personnelles et exercer leurs droits.

2. L'évaluation des risques

L'évaluation des impacts des risques informatiques est réalisée par le croisement de son niveau de vraisemblance et de gravité.

Exemple de cartographie des risques



La vraisemblance reflète la probabilité ou la possibilité que l'un des modes opératoires de l'attaquant aboutisse à l'objectif visé. Elle dépend des vulnérabilités des supports face aux menaces et des capacités des sources de risque à les exploiter.

La gravité évalue l'enjeu d'un événement redouté sur des « valeurs métier », c'est-à-dire stratégiques pour l'organisation (informations confidentielles, processus métier, matériels, logiciels, etc.).

Exemple de mesure de la gravité

Valeur métier	Évènement redouté	Impacts	Gravité
Facturation	Altération des informations sur les factures	• Impossibilité de recevoir un paiement • Perte de crédibilité • Impossibilité de remplir les obligations légales	G3 - Grave

III Les impacts des risques informatiques

L'ANSSI, au travers de sa méthode EBIOS, identifie différentes catégories d'impacts.

Impacts sur les missions et les services de l'organisation	Conséquences directes ou indirectes sur la réalisation des missions et services.
Impacts humains, matériels ou environnementaux	• **Impacts sur la sécurité ou sur la santé des personnes :** conséquences sur l'intégrité physique de personnes. • **Impacts matériels :** dégâts matériels ou destruction de biens supports. • **Impacts sur l'environnement :** conséquences écologiques à court ou long terme.
Impacts sur la gouvernance	• **mpacts sur la capacité de développement ou de décision :** conséquences sur la liberté de décider, de diriger, de mettre en œuvre la stratégie de développement. • **Impacts sur le lien social interne :** conséquences sur la qualité des liens sociaux au sein de l'organisation. • **Impacts sur le patrimoine intellectuel ou culturel :** conséquences sur les connaissances non-explicites accumulées par l'organisation sur le savoir-faire, les capacités d'innovation, les références culturelles communes.
Impacts financiers	Conséquences pécuniaires.
Impacts juridiques	Conséquences suite à une non-conformité légale, réglementaire, normative ou contractuelle.
Impacts sur l'image et la confiance	Conséquences sur l'image de l'organisation, la notoriété, la confiance des clients.

> Voir lexique BTS SIO, p. 221