

Fiche savoir 4 : Gérer les risques portant sur les données personnelles

I	Quand doit-on mener une AIPD ?	2
II	Nature des risques portant sur les données	3
III	Évaluer la vraisemblance du risque	3
1.1	Menaces et vulnérabilités	3
1.2	Les sources de menaces	3
1.3	Scénario de risque ou attaque	4
1.4	Niveau de vraisemblance	4
IV	Évaluer la gravité par les impacts potentiels	5
V	Typologie des mesures de sécurité	6
VI	Synthèse : cartographie des risques	7

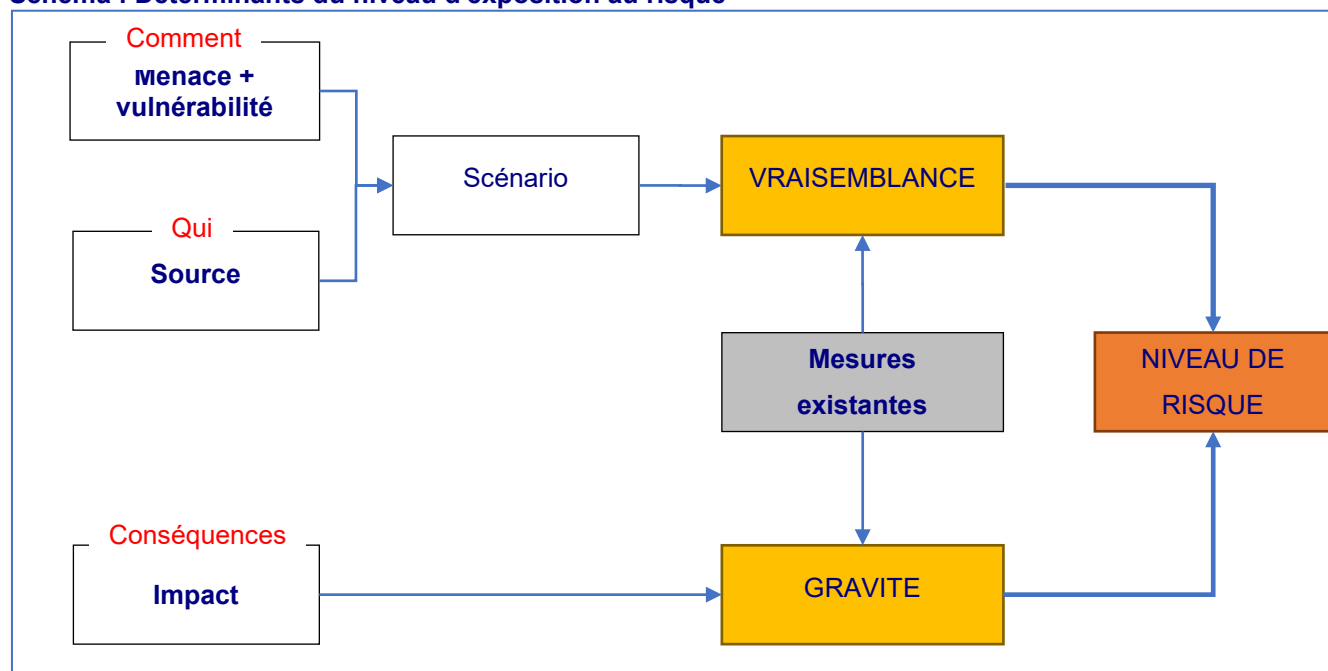
Une analyse des risques permet de se rendre compte des risques encourus, de faire le bilan des mesures existantes et de l'exposition résiduelle de l'organisation aux risques. Celle-ci peut alors envisager de nouvelles mesures.

Cette analyse, **lorsqu'elle concerne les données personnelles** peut être faite en utilisant la méthode d'Analyse d'Impact relative à la Protection des Données (AIPD ou PIA en anglais). Cette démarche est une adaptation de la méthode EBIOS de l'ANSSI qui concerne tous les aspects de la sécurité informatique d'une organisation.

L'objectif est d'identifier le **niveau d'exposition au risque** « résiduel » (étant données les mesures existantes) de l'organisation.

Le schéma ci-dessous synthétise les notions étudiées dans cette fiche et suggère une démarche : commencer par établir la vraisemblance, puis la gravité des risques identifiés pour enfin déduire le niveau d'exposition au risque.

Schéma : Déterminants du niveau d'exposition au risque



Sources

Fiche méthode 1 : Démarche de conformité RGPD partie « Gérer les données à risque »

⇒ En particulier : <https://www.cnil.fr/fr/gerer-les-risques>

<https://www.ssi.gouv.fr/administration/management-du-risque/la-methode-ebios-risk-manager/>

I Quand doit-on mener une AIPD ?

DOIS-JE FAIRE UNE AIPD ?

Les traitements de données doivent respecter le RGPD.
Tout traitement de données personnelles susceptible d'engendrer un risque élevé pour les droits et libertés des personnes concernées doit faire l'objet d'une analyse d'impact (AIPD).
L'analyse d'impact est un outil important de responsabilisation et de conformité qui permet de garantir le respect des principes du RGPD de façon opérationnelle et de pouvoir le démontrer.

Mon traitement est-il sur la liste
des cas pour lesquels une AIPD
n'est pas obligatoire ?

🔍 Consultez la liste

Non

Oui

Mon traitement est-il sur la liste
des cas pour lesquels une AIPD
est obligatoire ?

🔍 Consultez la liste

Oui

Non

Combien de critères mon
traitement remplit-il parmi les
suivants ?

- | | |
|---|---|
| 1. Évaluation/scoring (y compris le profilage) | 6. Croisement de données |
| 2. Décision automatique avec effet légal ou similaire | 7. Personnes vulnérables (patients, personnes âgées, enfants, etc.) |
| 3. Surveillance systématique | 8. Usage innovant (utilisation d'une nouvelle technologie) |
| 4. Données sensibles ou hautement personnelles (santé, géolocalisation, etc.) | 9. Exclusion du bénéfice d'un droit/contrat |
| 5. Collecte à large échelle | |

Au moins deux critères

Aucun critère

OU

Un critère mais je
considère que mon
traitement présente
un risque élevé



AIPD REQUISE

La CNIL vous propose une **boîte à outils** pour réaliser votre analyse d'impact.

Vous pouvez tout d'abord consulter les questions/réponses ainsi que les guides pratiques et les catalogues de bonnes pratiques.

Enfin, la CNIL met à votre disposition un **logiciel open source** pour faciliter la conduite et la formalisation de votre analyse.



AIPD NON REQUISE

Même non soumis à AIPD, les traitements doivent **respecter les principes de protection des données et les droits des personnes concernées**.

CNIL

sources :

https://www.cnil.fr/sites/default/files/atoms/files/infographie_aipd.pdf

<https://www.cnil.fr/sites/default/files/atoms/files/liste-traitements-aipd-non-requise.pdf>

<https://www.cnil.fr/sites/default/files/atoms/files/liste-traitements-avec-aipd-requise-v2.pdf>

Analyse des critères :

- données sensibles et à caractère hautement personnel : Fiche Savoir 1
- détails : https://www.cnil.fr/sites/default/files/atoms/files/wp248_rev.01_fr.pdf

II Nature des risques portant sur les données

Confidentialité	C'est le risque d'accès non légitime aux données. <u>Exemple</u> : les mots de passes sont divulgués.
Intégrité	Modification non désirée des données. <u>Exemple</u> : un article est modifié.
Disponibilité	Les données disparaissent ou sont inaccessibles. <u>Exemple</u> : les certifications et diplômes obtenus par le salarié sont supprimés.

III Évaluer la vraisemblance du risque

Évaluer la vraisemblance consiste à définir des scénarios et à évaluer leur probabilité d'advenir.

1.1 Menaces et vulnérabilités

Une **menace** correspond à la cause potentielle d'un incident. Exemple : « déni de service ».

Une menace peut être concrétisée en exploitant une **vulnérabilité**, c'est-à-dire une faiblesse. Exemple : un service DNS mal configuré a subi une attaque par déni de service.

Quatre principaux types de menaces sont mis en avant par l'ANSSI.

Menaces	Types d'attaques
Déstabilisation	Déni de service Défiguration Divulgaration de données
Espionnage	Attaque par point d'eau (<i>waterringhole</i>) Attaque par hameçonnage ciblé (<i>spearfishing</i>)
Sabotage	= panne organisée
Cybercriminalité	Rançongiciel (ransomware) Hameçonnage (phishing)

source : <https://www.ssi.gouv.fr/entreprise/principales-menaces/>

1.2 Les sources de menaces

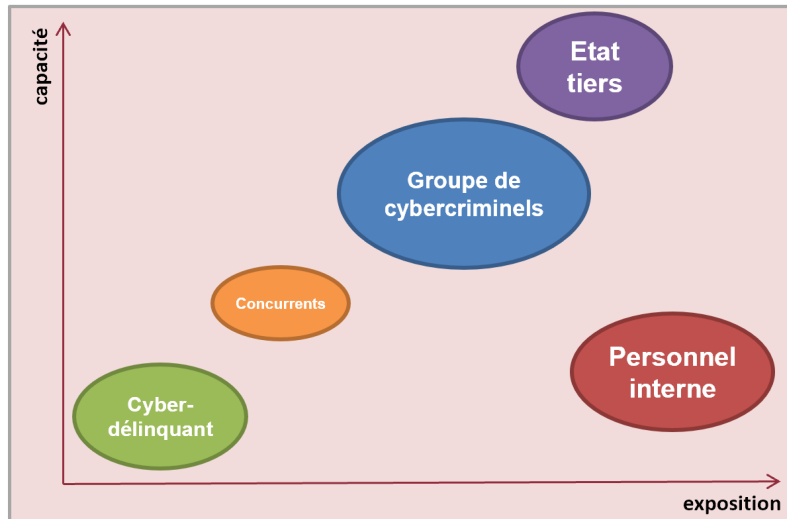
L'ANSSI regroupe les attaquants dans trois catégories : **organisation structurée** avec moyens importants, **groupes** avec motivation **idéologique**, **attaquants** avec moyens limités mais **spécialisés**.

source : https://www.ssi.gouv.fr/uploads/2018/10/fiches-methodes-ebios_projet.pdf p. 20

Autre typologie : source humaine interne, externe, non humaine.

<https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-3-fr-basesdeconnaissances.pdf> p. 3

Il est aussi possible de classer **les sources** de menaces selon leurs **capacités** et **l'exposition** de l'organisation.



Capacité

degré d'expertise et ressources de la source de menaces

Exposition

opportunités et intérêts de la source de menaces

Exemple d'une cartographie des principales sources de menaces qui pèsent sur un S.I.

1.3 Scénario de risque ou attaque

Un scénario décrit comment une source peut engendrer un risque pour l'organisation. Cette attaque représente la concrétisation d'une menace et nécessite l'exploitation d'une vulnérabilité.

1.4 Niveau de vraisemblance

On peut utiliser une échelle à quatre niveaux : négligeable, limité, important, maximal. La vraisemblance doit être évaluée en fonction des **mesures de sécurité existantes**.

IV Évaluer la gravité par les impacts potentiels

La gravité représente l'ampleur d'un risque.

Elle est essentiellement estimée au regard de la hauteur des **impacts potentiels** sur les personnes concernées, **compte tenu des mesures de sécurité existantes**.

On peut prendre la même échelle que pour la vraisemblance.

Niveau	Description générique	Impacts corporels	Impacts matériels	Impact moraux
1 - Négligeable	pas d'impact ou quelques désagréments surmontables sans difficulté			
2 - Limitée	désagréments significatifs surmontable malgré quelques difficultés	diffamation donnant lieu à des représailles physiques ou psychiques mais limitées		
3 - Importante	conséquences significatives surmontable mais avec des difficultés			
4 - Maximale	Conséquences significatives voire irrémediables parfois insurmontables			

source : <https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-3-fr-basesdeconnaissances.pdf> p. 5

V Typologie des mesures de sécurité

La CNIL distingue 3 types de mesures :

Mesures portant spécifiquement sur les données	chiffrement, anonymisation, cloisonnement des données, contrôle des accès logiques, traçabilité, contrôle d'intégrité, archivage, sécurité des documents papier
Mesures générales du système	sécurité de l'exploitation, lutte contre les logiciels malveillants, gestion des postes de travail, sécurité des sites web, sauvegardes, maintenance, sécurités des réseaux, surveillance, contrôle d'accès physique, sécurité des matériels, éloignement des sources de risque, protection contre les sources de risques non humaines
Mesures organisationnelles	organisation, gestion des règles, gestion des risques, gestion des projets, gestion des incidents et des violations de données, gestion des personnels, relations avec les tiers, supervision

sources :

<https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-2-fr-modeles.pdf> p. 22

<https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-3-fr-basesdeconnaissances.pdf> (analyse de chacune des mesures)

La typologie de l'ANSSI est plus générale mais peut aussi être utilisée :

Gouvernance et anticipation	gestion continue des risques (PIA par exemple) gestion des facteurs humains (sensibilisation, formation) veille
Protection	voir sécuriser les données dans la FM1
Défense	surveillance détection et classification des incidents procédure en cas d'attaque
Résilience	continuité, reprise d'activité gestion de crise cyber

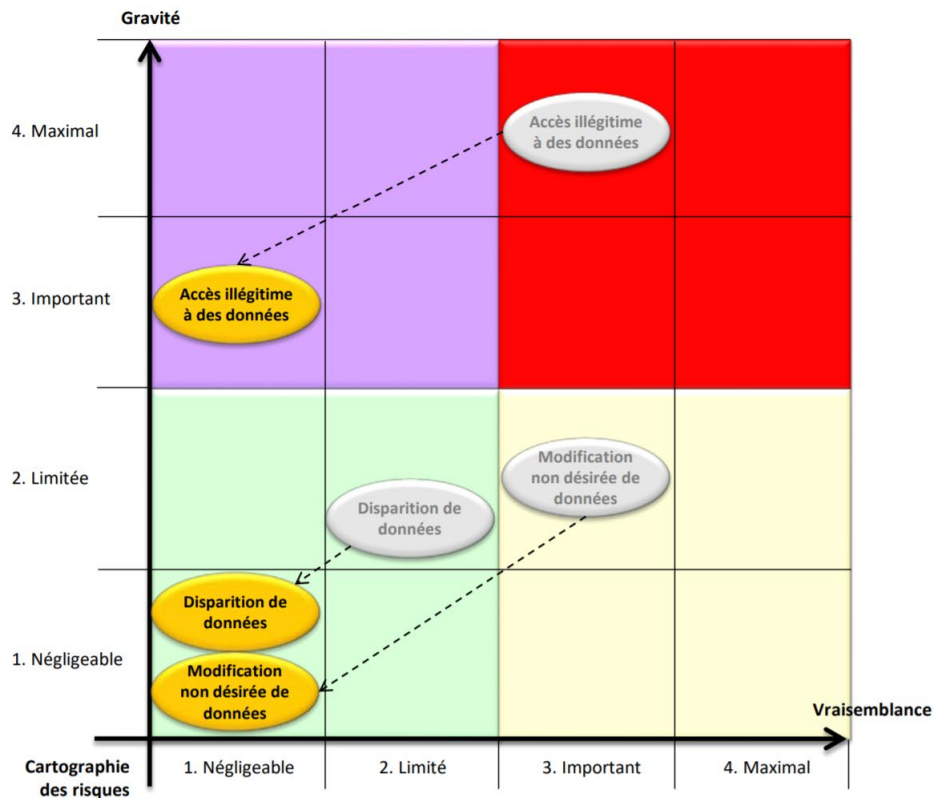
source : https://www.ssi.gouv.fr/uploads/2018/10/fiches-methodes-ebios_projet.pdf p. 72

VI Synthèse : cartographie des risques

Si on reprend **la même échelle pour la gravité et la vraisemblance** (négligeable, limité, important, maximal) il est possible de positionner les risques dans un graphique à 2 axes.

On peut aussi représenter **2 états** : avec les mesures actuelles et avec les mesures correctrices envisagées.

Élaboration de la cartographie des risques liés à la sécurité des données



source : <https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-2-fr-modeles.pdf> p. 23