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

[I Quand doit-on mener une AIPD ? 2](#_Toc53570444)

[II Nature des risques portant sur les données 3](#_Toc53570445)

[III Évaluer la vraisemblance du risque 3](#_Toc53570446)

[1.1 Menaces et vulnérabilités 3](#_Toc53570447)

[1.2 Les sources de menaces 3](#_Toc53570448)

[1.3 Scenario de risque ou attaque 4](#_Toc53570449)

[1.4 Niveau de vraisemblance 4](#_Toc53570450)

[IV Évaluer la gravité par les impacts potentiels 5](#_Toc53570451)

[V Typologie des mesures de sécurité 6](#_Toc53570452)

[VI Synthèse : cartographie des risques 7](#_Toc53570453)

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**

**Impact**

**Menace +**

**vulnérabilité**

**Source**

Scénario

VRAISEMBLANCE

GRAVITE

**Mesures**

**existantes**

NIVEAU DE RISQUE

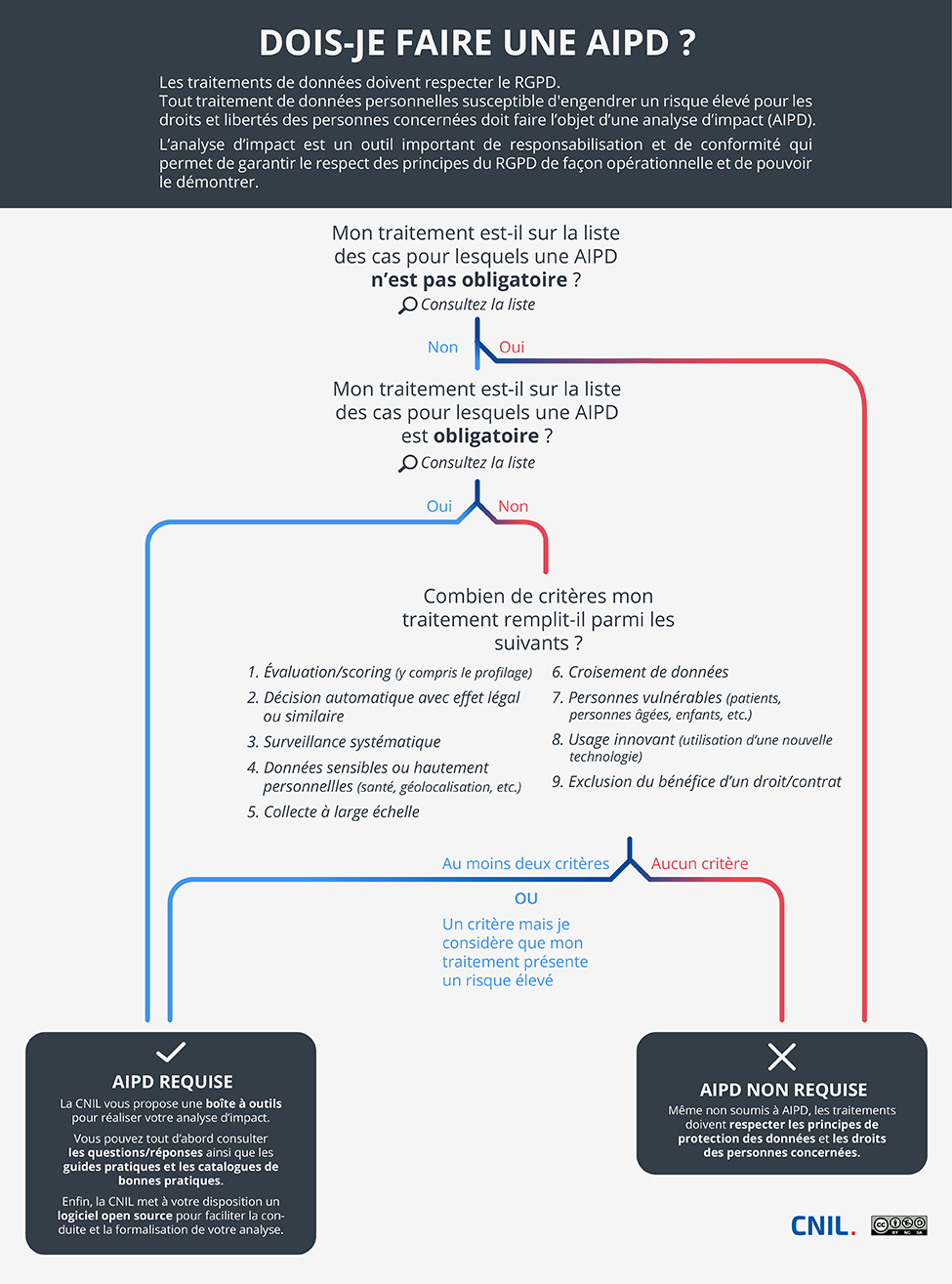
Conséquences

Comment

Qui

|  |
| --- |
| 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/> |

#### Quand doit-on mener une AIPD ?



|  |
| --- |
| 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> |

#### Nature des risques portant sur les données

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

#### Évaluer la vraisemblance du risque

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

###### 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  Divulgation de données |
| **Espionnage** | Attaque par point d'eau (*waterringhole*)  Attaque par hameçonnage ciblé (*spearfishing*) |
| **Sabotage** | = panne organisée |
| **Cybercriminalité** | Rançongiciel (ransomware)  Hameçonnage (phishing) |

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

###### Les sources de menaces

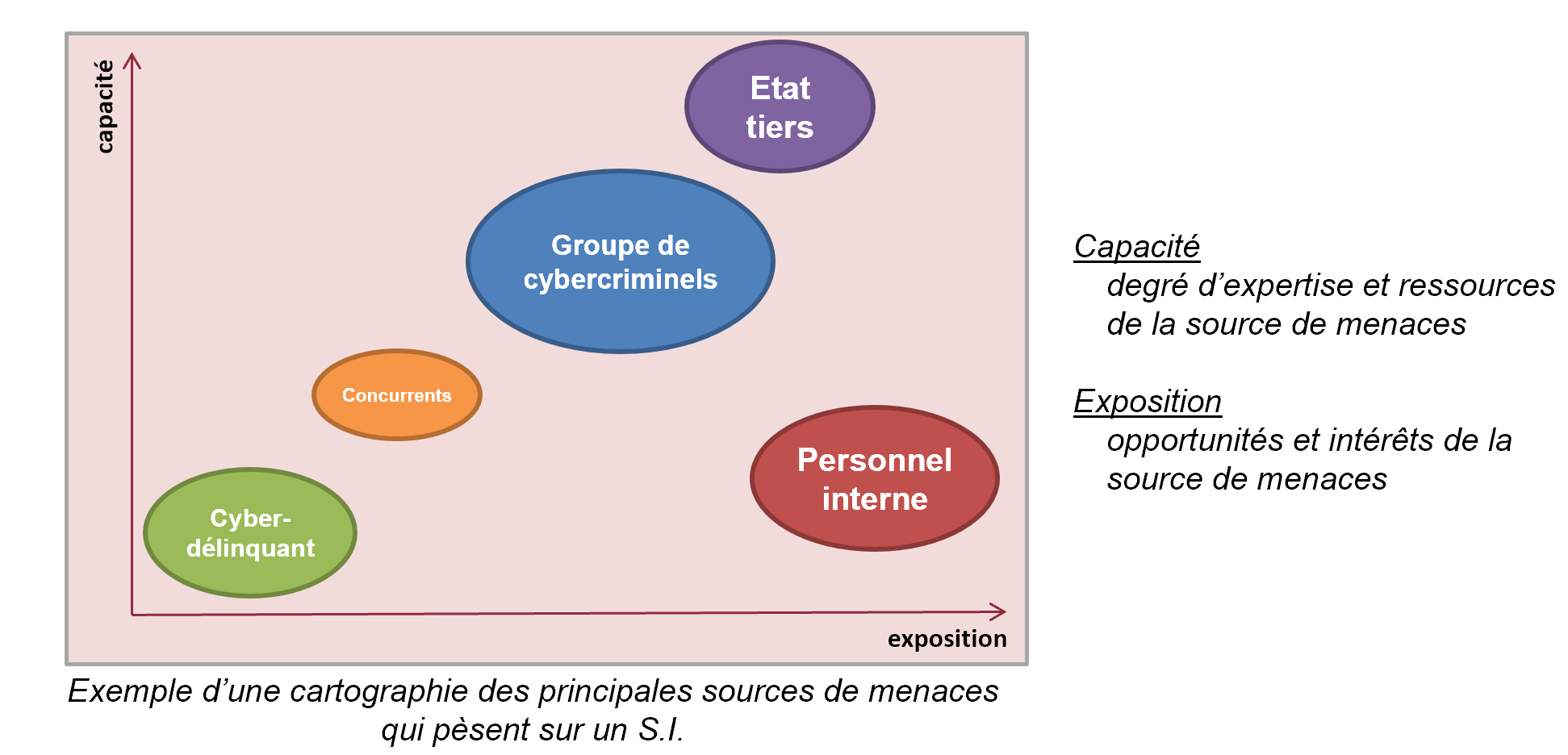
L'ANSSI regroupe les attaquant dans trois catégories : **organisation structurée** avec moyens importants, **groupes** avec motivation **idéologique, attaquants** avec moyens limités mais **spécialisés.**

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.



###### Scenario 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.

###### 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**.

#### 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 irrémédiables parfois insurmontables |  |  |  |

source : [https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-3-fr-basesdeconnaissances.pdf](https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-3-fr-basesdeconnaissances.pdf%20) p. 5

#### 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 systèmes** | 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 :

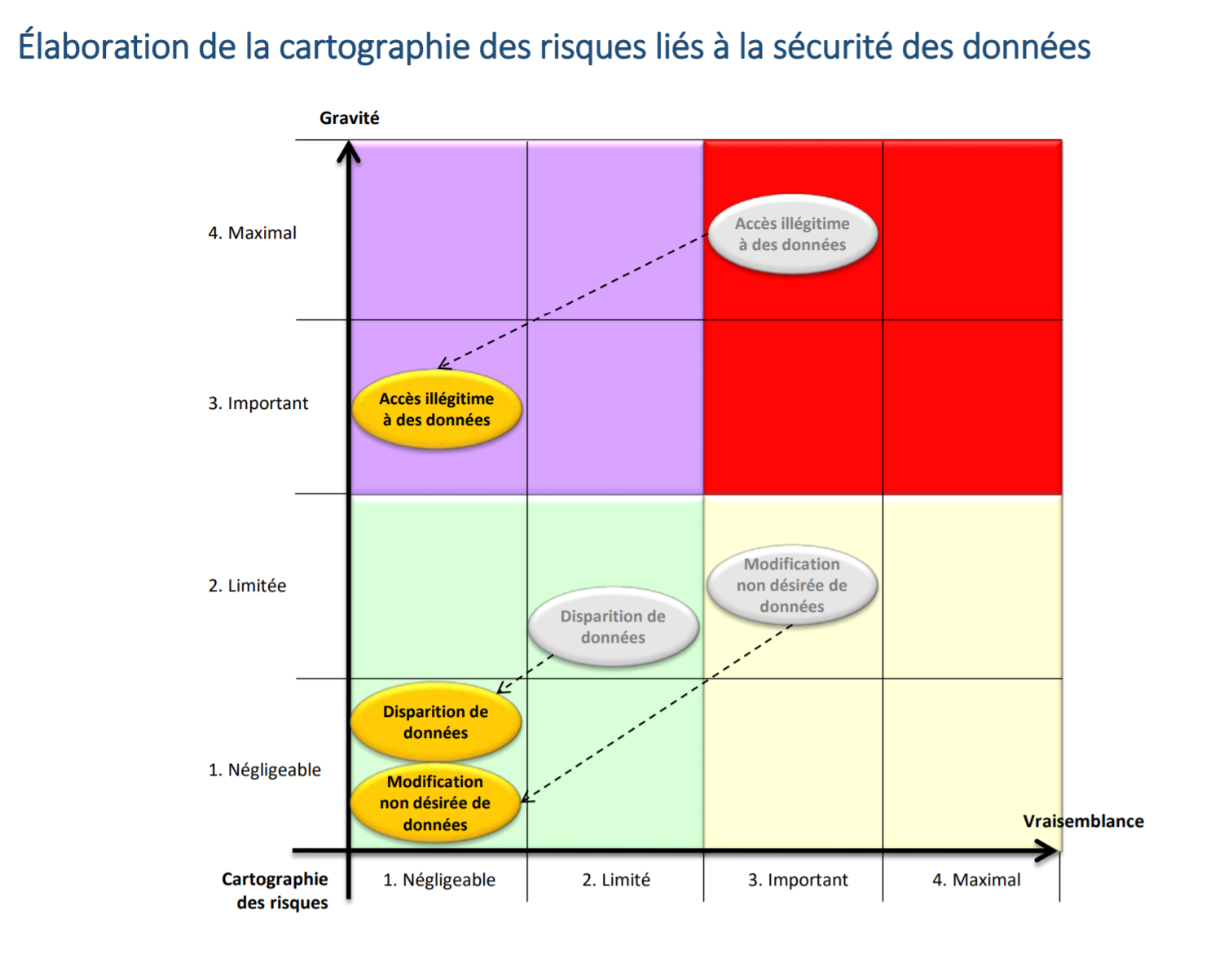
|  |  |
| --- | --- |
| **Gouvernance et anticipation** | gestion continue des risques (PIA par exemple)  gestion des facteurs humains (sensibilisation, formation)  veille |
| **Protection** | voir sécuriser les données dans la FM1 |
| **Défense** | surveillance  détection et classification des incidents  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

#### 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.



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