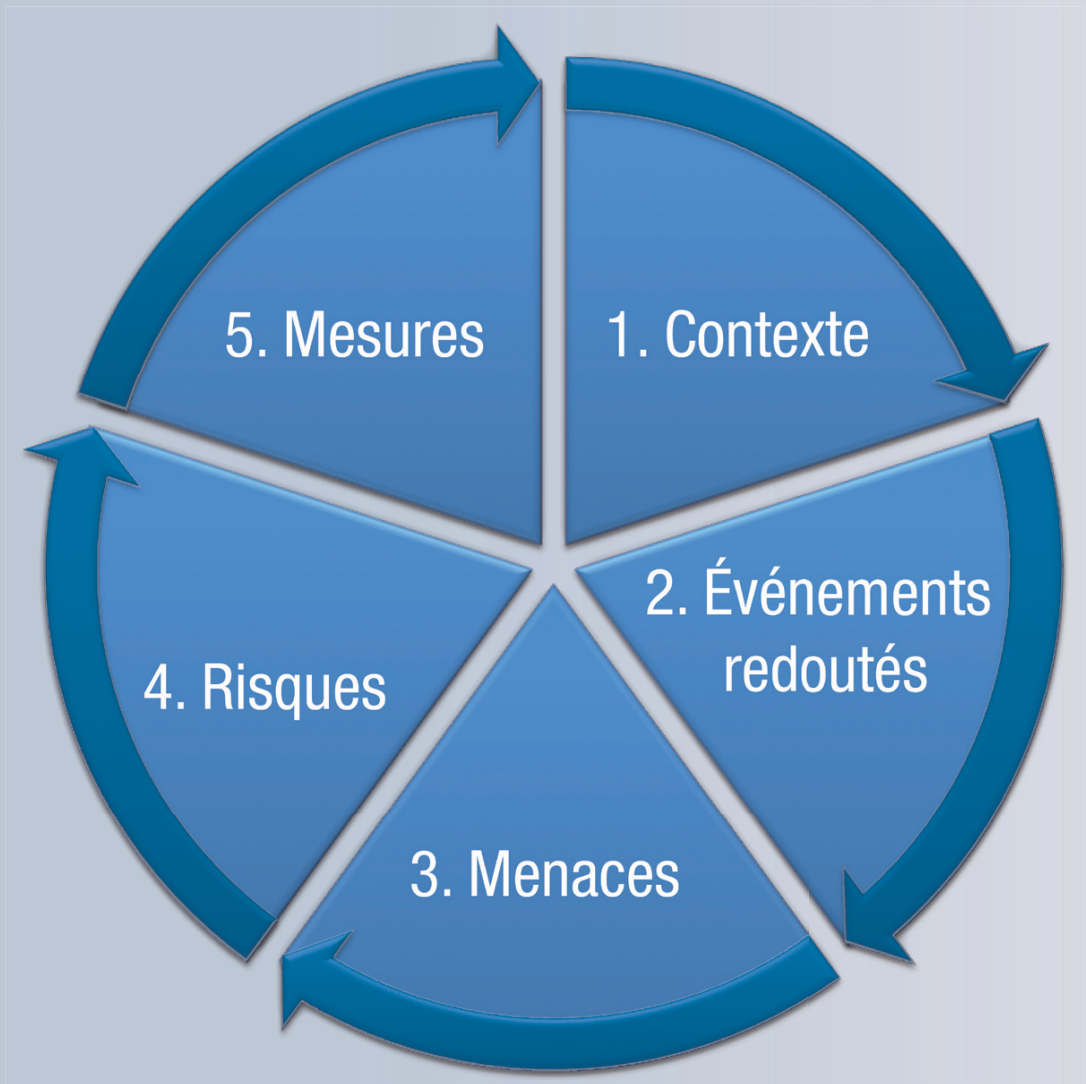
LES GUIDES DE LA CNIL

GUIDE
GÉRER LES RISQUES SUR LES LIBERTÉS ET LA VIE PRIVÉE



Édition 2012

CNIL
Commission Nationale de l'Informatique et des Libertés

Sommaire

AVANT PROPOS 3

INTRODUCTION 4

1. LA THEORIE : LES CONCEPTS DE GESTION DES RISQUES 5

1.1. La notion de risque sur la vie privée 5
Les événements redoutés : ce qu'on veut éviter 5
Les menaces : ce contre quoi on doit se protéger 6
Le niveau des risques : comment les estimer ? 7
1.2. La démarche de gestion des risques sur la vie privée 8

2. LA PRATIQUE : EBIOS DANS LE DOMAINE « INFORMATIQUE ET LIBERTES » . 9

2.1. Étude du contexte : de quoi parle-t-on ? 9
2.2. Étude des événements redoutés : que craint-on qu'il arrive ? 11
2.3. Étude des menaces : comment cela peut-il arriver ? (si besoin) 14
2.4. Étude des risques : quel est le niveau des risques ? (si besoin) 17
2.5. Étude des mesures : que peut-on faire pour traiter les risques ? 19

ANNEXES 23

Menaces génériques 23
Menaces qui peuvent affecter la confidentialité 23
Menaces qui peuvent affecter l'intégrité 24
Menaces qui peuvent affecter la disponibilité 25
Acronymes 27
Définitions 27
Références bibliographiques 29

Tableaux

Tableau 1 - Détermination de la gravité de chaque événement redouté 12
Tableau 2 - Étude des événements redoutés 13
Tableau 3 - Détermination de la vraisemblance de chaque menace 15
Tableau 4 - Étude des menaces 16
Tableau 5 - Mesures choisies pour traiter les risques 22
Tableau 6 - Menaces qui peuvent affecter la confidentialité 23
Tableau 7 - Menaces qui peuvent affecter l'intégrité 24
Tableau 8 - Menaces qui peuvent affecter la disponibilité 26

Figures

Figure 1 - Détermination du niveau de chaque risque 7
Figure 2 - Éléments composant les risques 7
Figure 3 - Les cinq étapes itératives de la démarche 8
Figure 4 - Cartographie des risques 17
Figure 5 - Cartographie des risques résiduels 20

RÉPUBLIQUE FRANÇAISE
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tél. : 01 53 73 22 22 – Fax : 01 53 73 22 00

Avant propos

Ce document a été réalisé par le service de l'expertise de la CNIL avec l'aimable contribution de plusieurs relecteurs[1] et présenté à des groupes de travail[2]. Il présente une méthode pour gérer les risques que les traitements de données à caractère personnel (DCP) peuvent faire peser sur les personnes concernées. Il complète ainsi le guide [CNIL-GuideSécurité] par une démarche d'analyse complète permettant d'améliorer la maîtrise des traitements complexes ou dont les enjeux identifiés sont importants. Il est lié à un catalogue de bonnes pratiques destinées à traiter les risques appréciés avec cette méthode.
L'emploi de cette démarche doit être proportionné aux traitements considérés : il ne sera sans doute pas utile de l'utiliser pour un fichier de DCP créé pour suivre le déroulement d'un projet, alors que cela s'imposera pour un traitement complexe de DCP sensibles.

L'application de la méthode ne se substitue pas aux formalités préalables que les responsables de traitements doivent effectuer auprès de la CNIL. Il s'agit d'une approche rationnelle qui va faciliter leur réalisation.

Ce document s'adresse principalement aux responsables de traitements, et en particulier aux parties prenantes dans la création ou l'amélioration de traitement de DCP :

- les responsables de traitements, qui peuvent avoir à justifier auprès de la CNIL des mesures qu'ils ont choisi de mettre en œuvre dans leurs systèmes ;
- les maîtrises d'ouvrage (MOA), qui doivent apprécier les risques pesant sur leur système et donner des objectifs de sécurité ;
- les maîtrises d'œuvre (MOE), qui doivent proposer des solutions pour traiter les risques conformément aux objectifs identifiés par les MOA ;
- les correspondants « informatique et libertés » (CIL), qui doivent accompagner les MOA dans la protection des DCP ;
- les responsables de la sécurité des systèmes d'information (RSSI), qui doivent accompagner les MOA dans le domaine de la sécurité des systèmes d'information (SSI).

Il a pour but de les aider à appliquer la [Loi-I&L][3] et doit leur permettre :

- d'avoir une vision objective des risques engendrés par leurs traitements ;
- de savoir choisir les mesures de sécurité nécessaires et suffisantes pour « *prendre toute précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès* » (article 34 de la [Loi-I&L]).

Note : les libellés entre crochets ([libellé]) correspondent aux références bibliographiques.

[1] Barbara DASKALA (ENISA), Daniel LE METAYER (INRIA) et d'autres contributeurs anonymes.
[2] Notamment le Club EBIOS (sur la gestion des risques) et NETFOCUS (sur la sécurité des systèmes d'information).
[3] On note que la Délibération de la CNIL n°81-094 du 21 juillet 1981 portant adoption d'une recommandation relative aux mesures générales de sécurité des systèmes informatiques prévoyait déjà « que l'évaluation des risques et l'étude générale de la sécurité soient entreprises systématiquement pour tout nouveau traitement informatique, et réexaminées pour les traitements existants ».

RÉPUBLIQUE FRANÇAISE
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tél. : 01 53 73 22 22 – Fax : 01 53 73 22 00

Introduction

Les données à caractère personnel (DCP) doivent être distinguées des autres informations présentes dans les systèmes d'information.

Elles peuvent représenter une valeur pour l'organisme qui les traite, mais leur traitement engendre également *de facto* une importante responsabilité du fait des risques qu'il fait encourir sur la vie privée[4] des personnes concernées.
Elles ont également une valeur pour les personnes concernées. Si elles peuvent leur être utiles à réaliser des démarches administratives ou commerciales, ou contribuer à leur image, une atteinte à leur sécurité peut leur causer des préjudices corporels, matériels et moraux.
Elles ont enfin une valeur pour autrui. Il peut notamment s'agir d'une valeur marchande dans le cas où elles sont exploitées à des fins commerciales (*spam*, publicité ciblée…), ou bien d'une valeur de nuisance dans le cas d'actions injustes (discrimination, refus d'accès à des prestations, licenciement…) ou malveillantes (usurpation d'identité, diffamation, menaces, chantage, cambriolage, agression…).

Dès lors qu'il traite des DCP, le responsable du traitement doit se conformer à la [Loi-I&L].
D'une part, il doit faire en sorte que la finalité du traitement soit définie et que les DCP collectées soient pertinentes au regard de cette finalité et qu'elles soient supprimées à la fin d'une période déterminée.
D'autre part, il doit s'assurer que les personnes concernées sont informées et peuvent exercer leurs droits (opposition, accès, rectification et suppression). Il convient d'évaluer si ces droits sont pris en considération au niveau de l'organisme et si l'exercice de ces droits est effectif.
En outre, il doit assurer la sécurité des DCP qu'il traite. La [Loi-I&L] dispose dans son article 34 l'obligation pour tout responsable de traitement « *de prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données* ». Il est donc nécessaire d'identifier les risques engendrés par un traitement avant de déterminer les moyens adéquats pour les réduire.
Enfin, il doit respecter les exigences spécifiques qui s'appliquent à ses traitements et aux DCP traités, notamment quand il s'agit de données sensibles, quand des DCP sont transférées en dehors de l'Union européenne, etc.

Pour ce faire, il convient d'adopter une vision globale, qui dépasse le seul cadre des activités de l'organisme et des finalités prévues pour ses traitements, et qui permette d'étudier les impacts sur les personnes que ces données concernent.

[4] Dans l'ensemble de ce document, le terme « vie privée » est utilisé comme raccourci pour évoquer « vie privée, identité humaine, droits de l'homme et libertés individuelles ou publiques ».

RÉPUBLIQUE FRANÇAISE
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tél. : 01 53 73 22 22 – Fax : 01 53 73 22 00

1. La théorie : les concepts de gestion des risques

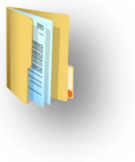
La gestion des risques est utilisée dans de nombreux domaines (sécurité de l'information, protection des personnes, finance, assurances…). Ce chapitre propose une transposition de cette démarche dans le contexte de la protection de la vie privée. La méthodologie présentée ci-après est parfaitement compatible avec les normes internationales relatives à la gestion des risques[5]. Elle s'intègre naturellement dans une logique de gestion globale des risques.

1.1. La notion de risque sur la vie privée

Dans le domaine « Informatique et libertés », seuls les risques que les traitements font peser sur la vie privée des personnes concernées sont considérés. Ces **risques** sont composés d'un événement redouté (que craint-on ?) et de toutes les menaces qui le rendent possible (comment cela peut-il arriver ?).

Les événements redoutés : ce qu'on veut éviter

Pour chaque traitement, les **éléments à protéger** sont les suivants :



- processus : ceux du traitement (ses fonctionnalités en tant que telles, dans la mesure où elles traitent des DCP) et ceux requis par la [Loi-I&L] pour informer les personnes concernées (article 32), obtenir leur consentement (s'il y a lieu, article 7) et permettre l'exercice des droits d'opposition (article 38), d'accès (article 39), de rectification et suppression[6] (article 40) ;
- données à caractère personnel (DCP) : celles directement concernées par le traitement et celles concernées par les processus légaux.

On souhaite éviter les situations suivantes[7] :

- indisponibilité des processus légaux : ils n'existent ou ne fonctionnent pas ou plus ;
- modification du traitement : il dévie de ce qui était initialement prévu (détournement de la finalité, collecte excessive ou déloyale…) ;
- accès illégitime aux DCP : elles sont connues de personnes non autorisées ;
- modification non désirée des DCP : elles ne sont plus intègres ou sont changées ;
- disparition des DCP : elles ne sont pas ou plus disponibles.

[5] Notamment la norme internationale [ISO31000].

[6] La personne concernée peut demander que les « *données inexactes, incomplètes, équivoques, périmées* » ou dont « *la collecte, l'utilisation, la communication ou la conservation est interdite* » soient supprimées.

[7] Si besoin, on peut également traiter de :

- la « compromission du traitement ». En effet, certains traitements, par exemple des traitements intéressant la sûreté de l'État, peuvent devoir être tenus secrets du fait que la connaissance de leur existence peut générer ou aggraver les risques sur les personnes concernées ;
- l' « indisponibilité du traitement », en plus de la « disparition des DCP ». Il est parfois utile de distinguer les DCP de leur traitement, qui serait indispensable aux personnes concernées, comme dans le cas de certaines prestations (de santé, administratives…) ;
- la « modification des processus légaux ». Bien que cela soit peu courant et difficile à étudier, il est possible d'apprécier les risques liés au fait qu'un processus légal, par l'exemple celui permettant aux personnes concernées d'exercer leur droit d'accès, puisse changer et leur porter préjudice.

RÉPUBLIQUE FRANÇAISE
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tél. : 01 53 73 22 22 – Fax : 01 53 73 22 00

En effet, si elles ont lieu, elles peuvent avoir des **impacts** sur la vie privée des personnes concernées, l'identité humaine, les droits de l'homme ou les libertés publiques.

L'**événement redouté** décrit la situation et ses impacts potentiels dans le contexte considéré.

Exemples d'événements redoutés

Des données sur les habitudes d'employés sont illégalement collectées et utilisées par leur hiérarchie pour orienter la recherche d'éléments permettant de les licencier.
Des coordonnées sont récupérées et utilisées à des fins commerciales (spam, publicité ciblée…).
Des identités sont usurpées afin de réaliser des activités illégales au nom des personnes concernées, ces dernières risquant des poursuites pénales.
Suite à la modification non désirée de données de santé, des patients sont pris en charge de manière inadaptée, ce qui aggrave leur état de santé et cause même des invalidités ou décès.
Des demandes de prestations sociales disparaissent, empêchant ainsi les bénéficiaires de les toucher et les obligeant à relancer leurs démarches administratives.

Les menaces : ce contre quoi on doit se protéger

Pour qu'un événement redouté ait lieu, il faut qu'une ou plusieurs **sources de risques** le provoquent, de manière accidentelle ou délibérée. Il peut s'agir de :

- personnes internes à l'organisme : utilisateur, informaticien…
- personnes externes à l'organisme : destinataire, prestataire, concurrent, tiers autorisé, militant, organisation gouvernementale, activité humaine environnante…
- sources non humaines : virus informatique, catastrophe naturelle, matières inflammables, épidémie, rongeurs…

Les sources de risques vont agir, de manière accidentelle ou délibérée, sur les composants du système d'information (informatique et organisation) sur lesquels reposent les éléments à protéger. Ces **supports** peuvent être des :

- matériels : ordinateurs, relais de communication, clés USB, disques durs…
- logiciels : systèmes d'exploitation, messagerie, bases de données, applications métier…
- canaux informatiques : câbles, WiFi, fibre optique…
- personnes : utilisateurs, administrateurs informatiques, décideurs…
- supports papier : impressions, photocopies…
- canaux de transmission papier : envoi postal, circuit de validation…

L'action des sources de risques sur les supports peut prendre la forme de différentes **menaces** :

- détournements d'usage : les supports sont détournés de leur cadre d'utilisation prévu sans être modifiés ni endommagés ;
- espionnage : les supports sont observés sans être endommagés ;
- dépassements de limites de fonctionnement : les supports sont surchargés, surexploités ou utilisés dans des conditions ne leur permettant pas de fonctionner correctement ;
- détériorations : les supports sont endommagés, partiellement ou totalement ;

RÉPUBLIQUE FRANÇAISE
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tél. : 01 53 73 22 22 – Fax : 01 53 73 22 00

- modifications : les supports sont transformés ;
- pertes de propriété : les supports sont perdus, volés, vendus ou donnés, de telle sorte qu'il n'est plus possible d'exercer les droits de propriété.

Exemples de menaces

Un individu malveillant injecte des requêtes non prévues dans le formulaire d'un site web.
Un concurrent, en visite incognito, vole un disque dur portable.
Un membre du personnel supprime des tables d'une base de données par inadvertance.
Un dégât des eaux détruit les serveurs informatiques et de télécommunications.

Le niveau des risques : comment les estimer ?

Un risque est donc un scénario qui décrit comment des sources de risques pourraient exploiter les vulnérabilités des supports jusqu'à provoquer un incident sur les éléments à protéger et des impacts sur la vie privée.

Le **niveau d'un risque** est estimé en termes de gravité et de vraisemblance.
La **gravité** représente l'ampleur d'un risque. Elle dépend essentiellement du caractère identifiant des DCP et du caractère préjudiciable des impacts potentiels.
La **vraisemblance** traduit la faisabilité d'un risque. Elle dépend essentiellement des vulnérabilités des supports face aux menaces et des capacités[8] des sources de risques à les exploiter.

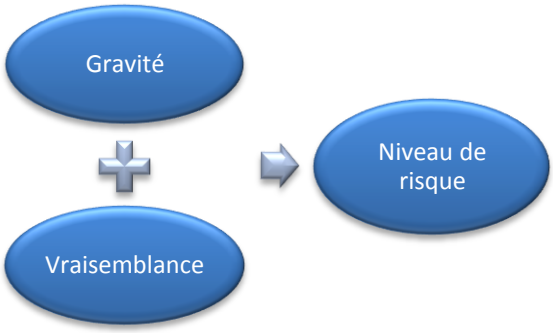


Figure 1 – Détermination du niveau de chaque risque

Le schéma suivant synthétise l'ensemble des notions présentées :

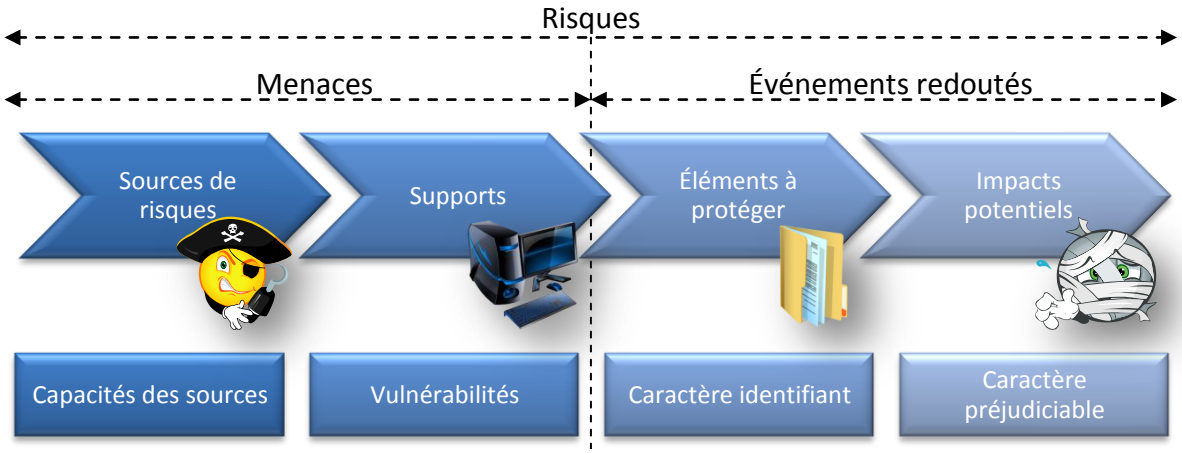


Figure 2– Éléments composant les risques

[8] Les capacités de sources de risques dépendent de leurs compétences, temps disponible, ressources financières, proximité du système, motivations, sentiment d'impunité…

RÉPUBLIQUE FRANÇAISE
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tél. : 01 53 73 22 22 – Fax : 01 53 73 22 00

La démarche de gestion des risques sur la vie privée

Du besoin de gérer les risques

« Le responsable du traitement est tenu de prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès »

(article 34 de la [Loi-I&L])

Employer une démarche de gestion des risques est la manière la plus sûre de garantir l'objectivité et la pertinence des choix à effectuer lors de la mise en place d'un traitement.

Pour apprécier les risques, il convient de commencer par identifier les événements redoutés et les estimer en termes de gravité.
Ensuite, il est seulement nécessaire d'identifier les menaces et d'estimer leur vraisemblance si elles permettent la réalisation des événements redoutés dont la gravité est élevée.
Les risques ainsi appréciés peuvent alors être traités par des mesures proportionnées.

La démarche consiste à étudier :

1. le contexte du traitement considéré,
2. les événements redoutés dans ce contexte,
3. les menaces envisageables (si besoin),
4. les risques qui en découlent (si besoin),
5. les mesures appropriées pour les traiter.

En outre, il s'agit d'un processus d'amélioration continue. Il requiert donc une surveillance des évolutions dans le temps (du contexte, des risques, des mesures…) et des mises à jour dès qu'une évolution significative a lieu.

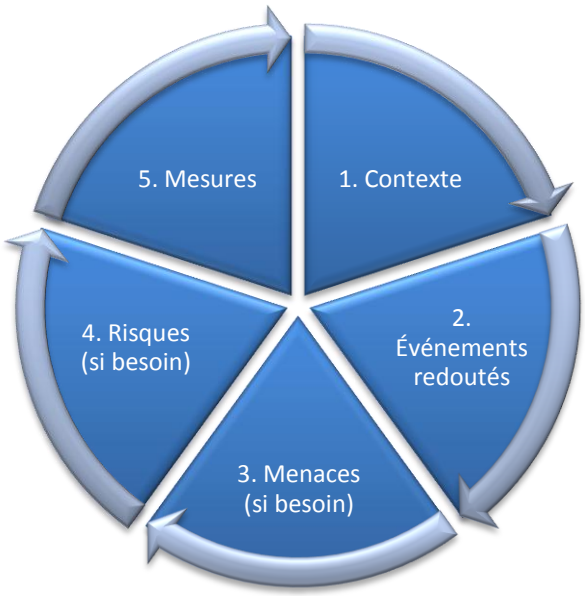


Figure 3 – Les cinq étapes itératives de la démarche

Notes

La validation de la manière dont les risques ont été traités, ainsi que l'acceptation des risques résiduels (qui subsistent après application de mesures), relèvent de la responsabilité du responsable de traitement.
Certains risques ne peuvent être ni réduits ni pris, notamment lorsque des données sensibles sont traitées ou quand les préjudices dont peuvent être victimes les personnes concernées sont très importants. Dans de tels cas, il pourra s'avérer nécessaire de choisir de les éviter, par exemple en ne mettant pas en œuvre tout ou partie d'un traitement.
Cela ne préjuge en rien de l'évaluation de conformité qui peut être faite le cas échéant par la CNIL dans le cadre des formalités préalables.

RÉPUBLIQUE FRANÇAISE
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tél. : 01 53 73 22 22 – Fax : 01 53 73 22 00

2. La pratique : EBIOS dans le domaine « Informatique et libertés »

Ce chapitre décrit les étapes de la démarche à appliquer pour réaliser une étude des risques qu'un traitement de DCP fait peser sur la vie privée. Elle décrit la manière d'employer la méthode [EBIOS][9] dans le contexte spécifique « informatique et libertés ».

Notes

La démarche devrait être employée dès la conception d'un nouveau traitement. En effet, une application en amont permet de déterminer les mesures nécessaires et suffisantes, et donc d'optimiser les coûts. A contrario, une application tardive, alors que le système est déjà créé et les mesures en place, peut remettre en question les choix effectués.
Du fait de sa compatibilité avec les normes internationales relatives à la gestion des risques, cette démarche s'inscrit aisément dans une gestion globale des risques.

2.1. Étude du contexte : de quoi parle-t-on ?

Rôles	Parties prenantes
Responsable[10]	MOA[11]
Approbateur[12]	Responsable de traitement
Consulté[13]	CIL[14] et/ou RSSI
Informé[15]	-

Le but de cette étape est d'obtenir une vision claire du périmètre considéré en identifiant tous les éléments utiles à la gestion des risques, en répondant aux questions suivantes :

- Quels sont les **éléments à protéger** ?
  - Quel est le traitement concerné ?
  - Quelle est sa finalité (voir les articles 6[16] et 9 de la [Loi-I&L]) ?
  - Quels sont ses destinataires ?
  - Quel est le processus métier que le traitement permet de réaliser ?
  - Quelles sont les personnes concernées par le traitement[17] ?

[9] EBIOS – Expression des Besoins et Identification des Objectifs de Sécurité – est la méthode de gestion des risques publiée par l'Agence nationale de la sécurité des systèmes d'information (ANSSI). Cette boîte à outils méthodologiques, reconnue et éprouvée, est largement utilisée dans le secteur public (ministères, organismes sous tutelle, collectivités…) et dans le secteur privé (industriels, grands comptes, consultants…), en France et à l'international (Québec, Belgique, Luxembourg, Union européenne, OTAN…), pour gérer les risques de sécurité des systèmes d'information. Elle est facilement adaptable à d'autres usages tels que la protection de la vie privée, du fait de sa grande souplesse et de sa compatibilité avec les normes internationales relatives à la gestion des risques.
[10] Personne(s) responsable(s) de la mise en œuvre de l'action.
[11] Elle peut être déléguée, représentée ou sous-traitée.
[12] Personne légitime pour approuver l'action.
[13] Personne(s) consultée(s) pour obtenir les informations utiles à l'action.
[14] Ou la personne en charge des aspects « Informatique et libertés ».
[15] Personne(s) informée(s) des résultats de l'action.
[16] Il est rappelé que les DCP sont collectées pour des finalités déterminées, explicites et légitimes.

RÉPUBLIQUE FRANÇAISE
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tél. : 01 53 73 22 22 – Fax : 01 53 73 22 00

- Comment les processus légaux vont-ils être mis en œuvre ?
- Quelles sont les DCP du traitement considéré ?
- Quelles sont les DCP utilisées par les processus légaux ?

Note

Le recensement des DCP doit être l'occasion de vérifier que chacune d'entre elles est indispensable au traitement et que les durées de conservations sont prévues et pertinentes[18].

- Quels sont les **supports**[19] des éléments à protéger ?
  - Quels sont les matériels (ordinateurs, routeurs, supports électroniques…) ?
  - Quels sont les logiciels (systèmes d'exploitation, messagerie, base de données, applications métier…) ?
  - Quels sont les canaux informatiques (câbles, WiFi, fibre optique…) ?
  - Quelles sont les personnes impliquées?
  - Quels sont les supports papier (impressions, photocopies…) ?
  - Quels sont les canaux de transmission papier (envoi postal, circuit de validation…) ?

- Quels sont les principaux **bénéfices du traitement** pour les personnes concernées ou la société en général ?

- Quelles sont les principales **références à respecter** (réglementaires, sectorielles…) ?

- Quelles sont les **sources de risques** pertinentes qui peuvent être à l'origine de risques[20] dans le contexte particulier du traitement considéré ?
  - Quelles sont les personnes internes à considérer (utilisateur, administrateur, développeur, décideur…) ?
  - Quelles sont les personnes externes à considérer (client, destinataire, prestataire, concurrent, militant, curieux, individu malveillant, organisation gouvernementale, activité humaine environnante…) ?
  - Quelles sont les sources non humaines à considérer (sinistre, code malveillant d'origine inconnue, phénomène naturel, catastrophe naturelle ou sanitaire…) ?

[17] Salariés, usagers, adhérents, clients (actuels ou potentiels), visiteurs, patients, étudiants/élèves…

[18] Une durée « *qui n'excède pas la durée nécessaire aux finalités pour lesquelles elles sont collectées et traitées* » (article 6 de la [Loi-I&L]), à défaut d'une autre obligation légale imposant une conservation plus longue.

[19] Les solutions de sécurité (produits, procédures, mesures…) ne sont pas des supports. Il s'agit de mesures destinées à traiter les risques, qui sont déterminées en fin d'étude (chiffrer, réaliser des sauvegardes, journaliser les actions, utiliser un pare-feu, mettre en place un réseau privé virtuel, sensibiliser les acteurs…).

[20] Elles peuvent agir de manière accidentelle (maladresse, inconscience, faible conscience d'engagement, peu motivé dans sa relation avec l'organisme…) ou délibérée (jeu, égo, vengeance, appât du gain…).

RÉPUBLIQUE FRANÇAISE
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tél. : 01 53 73 22 22 – Fax : 01 53 73 22 00

2.2. Étude des événements redoutés : que craint-on qu'il arrive ?

Rôles	Parties prenantes
Responsable	MOA
Approbateur	Responsable de traitement
Consulté	CIL et/ou RSSI
Informé	-

Le but de cette étape est d'obtenir une liste explicite et hiérarchisée de tous les événements redoutés dans le cadre du traitement considéré. Un exemple est fourni dans le tableau page 13.

Pour expliciter les événements redoutés, leurs **impacts potentiels** doivent être identifiés : quelles pourraient être les conséquences sur l'identité des personnes concernées, leur vie privée, les droits de l'homme ou les libertés publiques pour chacun des événements redoutés, c'est-à-dire si :

- les processus légaux n'étaient pas disponibles ?
- le traitement était modifié ?
- une personne non autorisée accédait aux DCP ?
- les DCP étaient modifiées ?
- les DCP disparaissaient ?

Afin de hiérarchiser les événements redoutés, la gravité est déterminée en fonction du caractère identifiant des DCP et du caractère préjudiciable de ces impacts potentiels.

Tout d'abord, le **caractère identifiant** de l'ensemble des DCP (précédemment identifiées) doit donc être estimé : avec quelle facilité peut-on identifier les personnes concernées[21] ?

1. Négligeable : il semble quasiment impossible d'identifier les personnes à l'aide des DCP les concernant (ex. : prénom seul à l'échelle de la population française).
2. Limité : il semble difficile d'identifier les personnes à l'aide des DCP les concernant, bien que cela soit possible dans certains cas (ex. : nom et prénom à l'échelle de la population française).
3. Important : il semble relativement facile d'identifier les personnes à l'aide des DCP les concernant (ex. : nom, prénom et date de naissance, à l'échelle de la population française).
4. Maximal : il semble extrêmement facile d'identifier les personnes à l'aide des DCP les concernant (ex. : nom, prénom, date de naissance et adresse postale, à l'échelle de la population française).

On retient la valeur dont la description correspond le mieux aux DCP identifiées. Des mesures existantes ou prévues peuvent avoir pour effet de réduire le caractère identifiant. Il convient alors de les mentionner en tant que **justification**, comme présenté dans le tableau page 13.

[21] « *Pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens en vue de permettre son identification dont dispose ou auxquels peut avoir accès le responsable de traitement ou toute autre personne* » (article 2 de la [Loi-I&L]), y compris les informations publiques, détenues ou obtenues par ailleurs, notamment sur Internet.

RÉPUBLIQUE FRANÇAISE
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tél. : 01 53 73 22 22 – Fax : 01 53 73 22 00

Ensuite, leur **caractère préjudiciable** doit être estimé pour chaque événement redouté : quelle serait l'importance des dommages[22] correspondant à l'ensemble des impacts potentiels ?

1. Négligeable : les personnes concernées ne seront pas impactées ou pourraient connaître quelques désagréments, qu'elles surmonteront sans difficulté (perte de temps pour réitérer des démarches ou pour attendre de les réaliser, agacement, énervement…).
2. Limité : les personnes concernées pourraient connaître des désagréments significatifs, qu'elles pourront surmonter malgré quelques difficultés (frais supplémentaires, refus d'accès à des prestations commerciales, peur, incompréhension, stress, affection physique mineure…).
3. Important : les personnes concernées pourraient connaître des conséquences significatives, qu'elles devraient pouvoir surmonter, mais avec de sérieuses difficultés (détournements d'argent, interdiction bancaire, dégradation de biens, perte d'emploi, assignation en justice, aggravation de l'état de santé…).
4. Maximal : les personnes concernées pourraient connaître des conséquences significatives, voire irrémédiables, qu'elles pourraient ne pas surmonter (péril financier tel que des dettes importantes ou une impossibilité de travailler, affection psychologique ou physique de longue durée, décès…).

On retient la valeur dont la description correspond le mieux aux impacts potentiels identifiés.
Des mesures existantes ou prévues peuvent avoir pour effet de réduire le caractère préjudiciable. Il convient alors de les mentionner en tant que **justification**, comme présenté dans le tableau figurant page 13.

Enfin, la **gravité** est déduite en fonction des valeurs retenues pour le caractère identifiant des DCP et le caractère préjudiciable des impacts. Elle se détermine en additionnant les deux valeurs et en identifiant la gravité correspondante dans le tableau suivant :

Caractère identifiant + caractère préjudiciable	Gravité correspondante
< 5	1. Négligeable
= 5	2. Limité
= 6	3. Important
> 6	4. Maximal

Tableau 1 - Détermination de la gravité de chaque événement redouté

Optionnel : il est possible d'augmenter ou de diminuer la gravité ainsi déduite en tenant compte d'autres facteurs. Par exemple, un grand nombre de personnes concernées (ce qui peut favoriser un sinistre massif) pourrait augmenter la gravité d'un niveau. Un grand nombre d'interconnexions (notamment avec l'étranger) ou de destinataires (ce qui facilite la corrélation de DCP initialement séparées) pourrait également être considéré comme un facteur aggravant. A contrario, très peu de personnes concernées, pas ou très peu d'interconnexions ou de destinataires, pourraient diminuer la gravité d'un niveau.

[22] Les dommages sur les personnes concernées peuvent être :
- corporels (préjudice d'agrément, d'esthétique ou économique lié à l'intégrité physique),
- matériels (perte subie ou gain manqué concernant le patrimoine des personnes),
- moraux (souffrance physique ou morale, préjudice esthétique ou d'agrément…).

RÉPUBLIQUE FRANÇAISE
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tél. : 01 53 73 22 22 – Fax : 01 53 73 22 00

Outillage

Le résultat de cette étape peut être formalisé dans un tableau tel que le suivant :

Événements redoutés	Caractère identifiant des DCP[23]	Impacts potentiels les plus graves	Caractère préjudiciable des impacts potentiels	Mesures existantes ou prévues	Gravité maximum
1. Indisponibilité des processus légaux	*4. Maximal*	✓ *Diffusion non maîtrisée de DCP* ✓ *Impossibilité d'exercer ses droits* ✓ *Blocage de procédures d'achats*	*2. Limité*	*Aucune mesure prévue pour réduire la gravité*	*3. Important*
2. Modification du traitement	*4. Maximal*	✓ *Propositions commerciales non sollicitées*	*1. Négligeable*	*Aucune mesure prévue pour réduire la gravité*	*2. Limitée*
3. Accès illégitime aux DCP	*4. Maximal*	✓ *Usurpation de compte* ✓ *Exploitation à des fins commerciales*	*3. Important*	*Toutes les données sont nécessaires*	*4. Maximal*
4. Modification non désirées des DCP	*4. Maximal*	✓ *Commandes non satisfaites*	*1. Négligeable*	*Sauvegardes et récupération dans la journée*	*2. Limitée*
5. Disparition des DCP	*4. Maximal*	✓ *Obligation de se réinscrire* ✓ *Perte d'avantages*	*1. Négligeable*	*Sauvegardes et récupération dans la journée*	*2. Limitée*

Tableau 2 - Étude des événements redoutés

[23] Dans cet exemple, les principales DCP sont l'état civil de clients, leur adresse, leurs coordonnées bancaires, les produits achetés par le client et l'identifiant de connexion au service.

RÉPUBLIQUE FRANÇAISE
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tél. : 01 53 73 22 22 – Fax : 01 53 73 22 00

2.3. Étude des menaces : comment cela peut-il arriver ? (si besoin)

Cette étape est optionnelle si la gravité est négligeable (1) ou limitée (2).

Rôles	Parties prenantes
Responsable	MOE[24]
Approbateur	Responsable de traitement
Consulté	CIL et/ou RSSI
Informé	-

Le but de cette étape est d'obtenir une liste explicite et hiérarchisée de toutes les menaces[25] qui permettraient aux événements redoutés de survenir. Il est possible de ne pas étudier celles qui concernent les événements redoutés dont la gravité est négligeable (1) ou limitée (2). Un exemple est fourni dans le tableau page 16.

Une menace étant une action possible des sources de risques sur les supports, il convient d'identifier et d'estimer ces éléments pour chaque menace.

Tout d'abord, les **vulnérabilités des supports** sont estimées pour chaque menace : dans quelle mesure les caractéristiques des supports sont-elles exploitables pour réaliser la menace ?

1. Négligeable : il ne semble pas possible de réaliser la menace en s'appuyant sur les caractéristiques des supports (ex. : vol de supports papiers stockés dans un local de l'organisme dont l'accès est contrôlé par badge et code d'accès).
2. Limité : il semble difficile de réaliser la menace en s'appuyant sur les caractéristiques des supports (ex. : vol de supports papiers stockés dans un local de l'organisme dont l'accès est contrôlé par badge).
3. Important : il semble possible de réaliser la menace en s'appuyant sur les caractéristiques des supports (ex. : vol de supports papiers stockés dans les bureaux d'un organisme dont l'accès est contrôlé par une personne à l'accueil).
4. Maximal : il semble extrêmement facile de réaliser la menace en s'appuyant sur les caractéristiques des supports (ex. : vol de supports papier stockés dans le hall public de l'organisme).

On retient la valeur dont la description correspond le mieux aux vulnérabilités des supports identifiés.
Des mesures existantes ou prévues peuvent avoir pour effet de réduire les vulnérabilités des supports. Il convient dans ce cas de les mentionner en tant que **justification**, comme présenté dans le tableau page 16.

[24] Elle peut également être déléguée, représentée ou sous-traitée.
[25] Une liste de 45 menaces génériques est fournie en annexe. Issues des bases de connaissances d'[EBIOS], elles sont conçues pour être exhaustives, indépendantes et appliquées aux spécificités de la protection de la vie privée.

RÉPUBLIQUE FRANÇAISE
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tél. : 01 53 73 22 22 – Fax : 01 53 73 22 00

Ensuite, les **capacités des sources de risques** sont estimées pour chaque menace : quelles sont leurs capacités à exploiter les vulnérabilités (compétences, temps disponible, ressources financières, proximité du système, motivation, sentiment d'impunité…) ?

1. Négligeable : les sources de risques ne semblent pas avoir de capacités particulières pour réaliser la menace (ex. : détournement d'usage de logiciels par une personne sans mauvaises intentions ayant des privilèges restreints).
2. Limité : les sources de risques ont quelques capacités, mais jugées peu importantes, pour réaliser la menace (ex. : détournement d'usage de logiciels par une personne mal intentionnée ayant des privilèges restreints).
3. Important : les sources de risques ont des capacités réelles, jugées importantes, pour réaliser la menace (ex. : détournement d'usage de logiciels par une personne sans mauvaises intentions ayant des privilèges d'administration illimités).
4. Maximal : les sources de risques ont des capacités certaines, jugées illimitées, pour réaliser la menace (ex. : détournement d'usage de logiciels par une personne mal intentionnée ayant des privilèges d'administration illimités).

On retient la valeur dont la description correspond le mieux aux sources de risques identifiées.
Des mesures existantes ou prévues peuvent avoir pour effet de réduire les capacités des sources de risques. Il convient alors de les mentionner en tant que **justification**, comme présenté dans le tableau page 16.

Enfin, la **vraisemblance** des menaces est déduite, en fonction des valeurs retenues pour les vulnérabilités des supports et les capacités des sources de risques. Elle se détermine en additionnant les deux valeurs et en identifiant la vraisemblance correspondante en se reportant au tableau suivant :

Vulnérabilités des supports + capacités des sources de risques	Vraisemblance correspondante
< 5	1. Négligeable
= 5	2. Limité
= 6	3. Important
> 6	4. Maximal

Tableau 3 - Détermination de la vraisemblance de chaque menace

Optionnel : il est possible d'augmenter ou de diminuer la vraisemblance ainsi déduite en tenant compte d'autres facteurs. Par exemple, une ouverture sur Internet, des échanges de données avec l'étranger, des interconnexions avec d'autres systèmes ou une grande hétérogénéité ou variabilité du système, pourraient augmenter la vraisemblance d'un niveau. A contrario, un système fermé, sans interconnexion, homogène et stable pourraient la diminuer d'un niveau.

RÉPUBLIQUE FRANÇAISE
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tél. : 01 53 73 22 22 – Fax : 01 53 73 22 00

Outillage

Le résultat de cette étape peut être formalisé en complétant le tableau précédemment utilisé pour présenter les événements redoutés :

Événements redoutés	Menaces les plus vraisemblables	Vulnérabilités des supports	Capacités des sources de risques	Mesures existantes ou prévues	Vraisemblance maximum[26]
1. Indisponibilité des processus légaux	✓ *Détérioration d'un matériel (ex. : destruction d'un serveur)* ✓ *Usage anormal d'un logiciel (ex. : maladresse en manipulant les fichiers)* ✓ *Départ d'une personne (ex. : démission de celui qui connait les procédures)* ✓ *Disparition d'un canal papier (ex. : changement de procédures)*	*4. Maximal*	*3. Important*	*Aucune mesure prévue pour réduire la vraisemblance*	*4. Maximal*
2. Modification du traitement	*[sans objet]*	*[sans objet]*	*[sans objet]*	*[sans objet]*	*[sans objet]*
3. Accès illégitime aux DCP	✓ *Vol d'un matériel (ex. : vol d'un PC portable dans le train)* ✓ *Détournement d'usage d'un logiciel (ex. : usage à titre personnel)* ✓ *Modification d'un logiciel (ex. : propagation d'un virus)*	*3. Important*	*3. Important*	*Aucune mesure prévue pour réduire la vraisemblance*	*3. Important*
4. Modification non désirées des DCP	*[sans objet]*	*[sans objet]*	*[sans objet]*	*[sans objet]*	*[sans objet]*
5. Disparition des DCP	*[sans objet]*	*[sans objet]*	*[sans objet]*	*[sans objet]*	*[sans objet]*

Tableau 4 - Étude des menaces

[26] La vraisemblance est théoriquement déterminée pour chaque menace. On ne garde que la valeur la plus élevée.

RÉPUBLIQUE FRANÇAISE
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tél. : 01 53 73 22 22 – Fax : 01 53 73 22 00

2.4. Étude des risques : quel est le niveau des risques ? (si besoin)

Cette étape est optionnelle si la gravité est négligeable (1) ou limitée (2).

Rôles	Parties prenantes
Responsable	MOA
Approbateur	Responsable de traitement
Consulté	CIL et/ou RSSI
Informé	MOE

Le but de cette étape est d'obtenir une cartographie des risques permettant de décider de la priorité de traitement.
Puisqu'un risque est composé d'un événement redouté et de toutes les menaces qui permettraient qu'il survienne :

- sa **gravité** est égale à celle de l'événement redouté,
- sa **vraisemblance** est égale à la valeur la plus élevée de la vraisemblance des menaces associées à l'événement redouté.

On peut dès lors positionner les risques sur une **cartographie** :

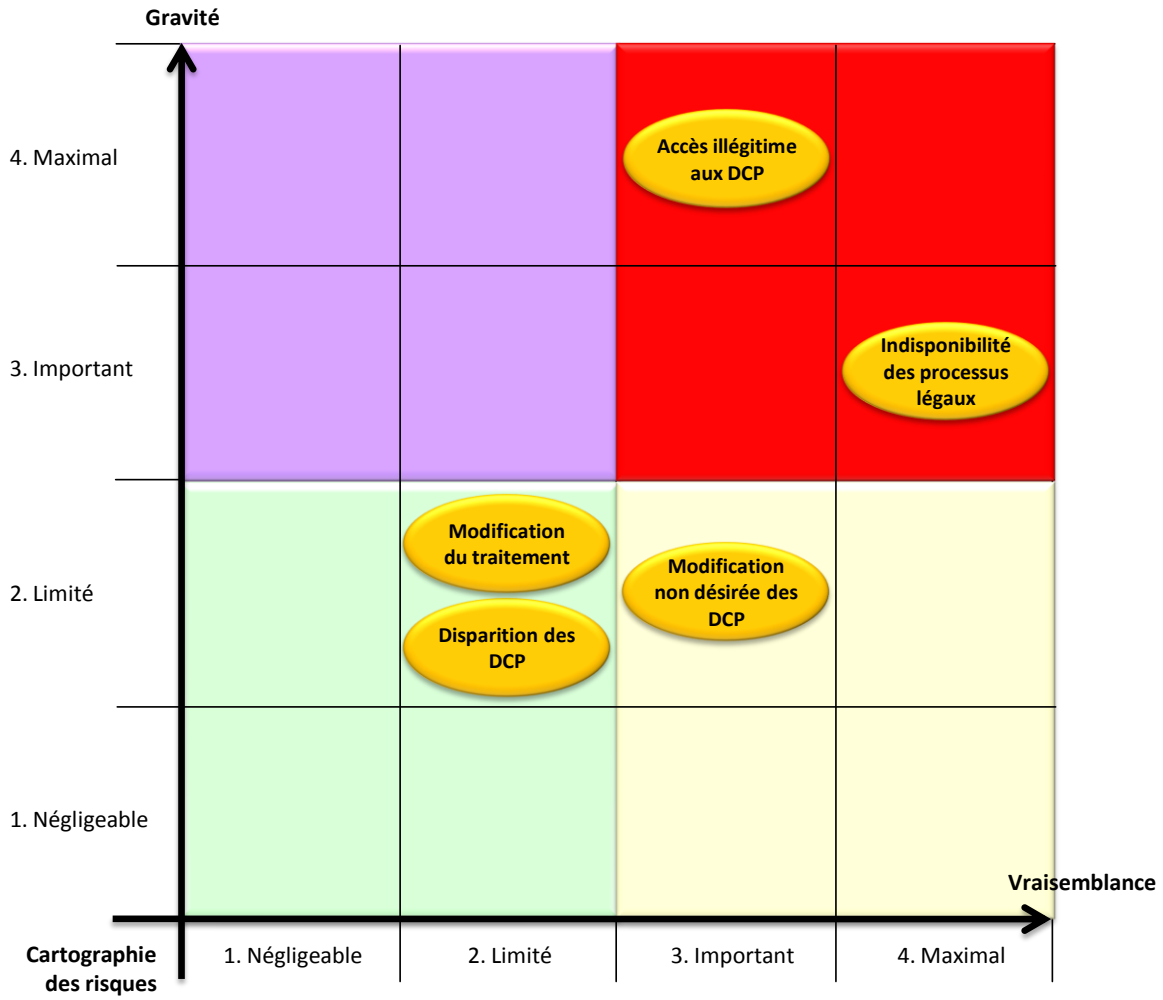


Figure 4 - Cartographie des risques

RÉPUBLIQUE FRANÇAISE
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tél. : 01 53 73 22 22 – Fax : 01 53 73 22 00

Optionnel : des **objectifs** peuvent être fixés en fonction du positionnement des risques au sein de la cartographie (par ordre de priorité) :

1. pour les risques dont la gravité et la vraisemblance sont élevées[27] : ces risques doivent absolument être évités ou réduits par l'application de mesures de sécurité diminuant leur gravité et leur vraisemblance. Dans l'idéal, il conviendrait même de s'assurer qu'ils sont traités à la fois par des mesures indépendantes de prévention (actions avant le sinistre), de protection (actions pendant le sinistre) et de récupération (actions après le sinistre) ;

2. pour les risques dont la gravité est élevée, mais la vraisemblance faible[28] : ces risques doivent être évités ou réduits, par l'application de mesures de sécurité diminuant leur gravité ou leur vraisemblance. Les mesures de prévention devront être privilégiées ;

3. pour les risques dont la gravité est faible mais la vraisemblance élevée : ces risques doivent être réduits par l'application de mesures de sécurité diminuant leur vraisemblance. Les mesures de récupération devront être privilégiées ;

4. pour les risques dont la gravité et la vraisemblance sont faibles : ces risques peuvent être pris, d'autant plus que le traitement des autres risques devrait également contribuer à leur traitement.

[27] Niveaux 3. Important et 4. Maximal.
[28] Niveaux 1. Négligeable et 2. Limité.

RÉPUBLIQUE FRANÇAISE
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tél. : 01 53 73 22 22 – Fax : 01 53 73 22 00

2.5. Étude des mesures : que peut-on faire pour traiter les risques ?

Rôles	Parties prenantes
Responsable	MOE ou MOA
Approbateur	Responsable de traitement ou CNIL[29]
Consulté	CIL et/ou RSSI
Informé	MOA ou MOE, CNIL

Le but de cette étape est de bâtir un dispositif de protection qui permette de traiter les risques de manière proportionnée, qui soit conforme à la [Loi-I&L], et qui tienne compte des contraintes du responsable de traitement (légales, financières, techniques…).

Tout d'abord, il convient de **déterminer les mesures** pour traiter les risques. Pour ce faire, il convient de relier les mesures existantes ou prévues (identifiées précédemment dans l'étude ou dans les références applicables) au(x) risque(s) qu'elles contribuent à traiter. Des mesures sont ensuite ajoutées tant que le niveau des risques n'est pas jugé acceptable.

Outillage

Ces mesures complémentaires peuvent être créées de toute pièce, ou bien issues de bonnes pratiques diffusées par des institutions reconnues ou de normes internationales. Elles doivent généralement être adaptées au contexte spécifique du traitement considéré.

Cette action consiste à déterminer des mesures complémentaires qui vont porter :

1. sur les éléments à protéger : mesures destinées à empêcher que leur sécurité ne puisse être atteinte, à détecter leur atteinte ou à recouvrer la sécurité (informer les personnes concernées, minimiser les DCP, anonymiser les DCP…) ;
2. puis, si ce n'est pas suffisant, sur les impacts potentiels : mesures destinées à empêcher que les conséquences du risque ne puissent se déclarer, à identifier et limiter leurs effets ou à les résorber (sauvegarder, contrôler l'intégrité, gérer les violations de DCP…) ;
3. ensuite, si ce n'est pas suffisant, sur les sources de risques : mesures destinées à les empêcher d'agir ou de concrétiser le risque, à identifier et limiter leur action ou à se retourner contre elles (contrôler les accès physiques et logiques, tracer l'activité, gérer les tiers, lutter contre les codes malveillants…) ;
4. enfin, si ce n'est pas suffisant, sur les supports : mesures destinées à empêcher que les vulnérabilités puissent être exploitées, à détecter et limiter les menaces qui surviennent tout de même ou à retourner à l'état de fonctionnement normal (réduire les vulnérabilités des logiciels, des matériels, des personnes, des documents papiers…).

Optionnel : afin d'améliorer la maturité de la protection des DCP, il est utile de compléter le dispositif par des mesures transverses, globales à l'organisme (organisation, politique, supervision…). Par ailleurs, pour vérifier la fiabilité des mesures, il peut être utile de déterminer les actions entreprises en cas d'ineffectivité de ces mesures (si elles ne fonctionnent plus).

[29] Selon les obligations légales relatives aux formalités préalables.

RÉPUBLIQUE FRANÇAISE
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tél. : 01 53 73 22 22 – Fax : 01 53 73 22 00

Notes

Plus les capacités des sources de risques sont importantes, plus les mesures doivent être robustes pour y résister.
Par ailleurs, les éventuels incidents qui auraient déjà eu lieu, notamment les violations de DCP, ainsi que les difficultés rencontrées pour mettre en œuvre certaines mesures, peuvent servir à améliorer le dispositif de sécurité.
Les mesures spécifiées devraient être formalisées, mises en place, auditées de manière régulière et améliorées de manière continue.

Il convient ensuite de **ré-estimer la gravité et la vraisemblance des risques résiduels** (c'est-à-dire les risques qui subsistent après application des mesures choisies) en tenant compte de ces mesures complémentaires. Il est alors possible de les repositionner sur la cartographie :

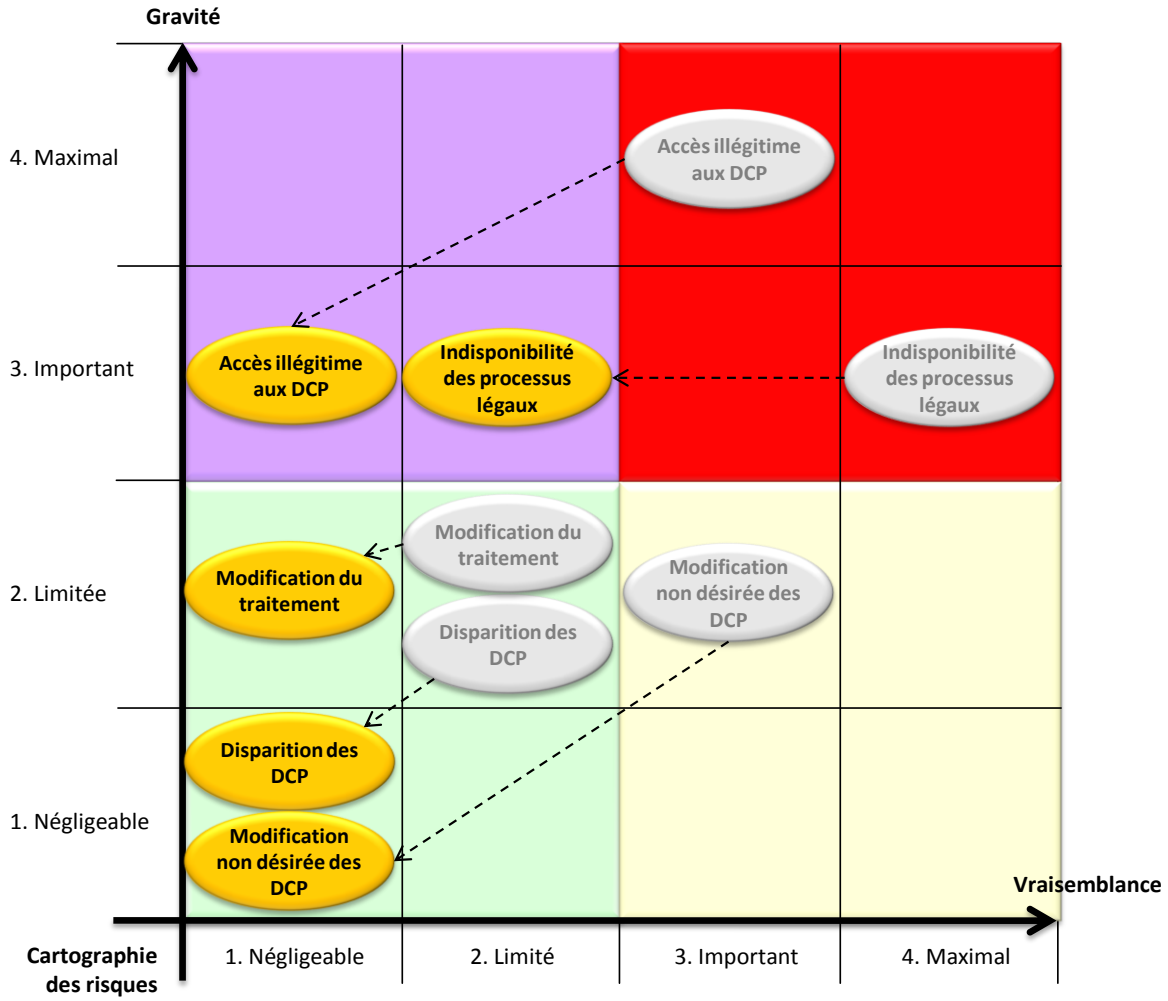


Figure 5 - Cartographie des risques résiduels

RÉPUBLIQUE FRANÇAISE
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tél. : 01 53 73 22 22 – Fax : 01 53 73 22 00

Enfin, il convient d'**expliquer pourquoi les risques résiduels peuvent être acceptés**. Cette justification peut s'appuyer sur les nouveaux niveaux de gravité et de vraisemblance et sur les bénéfices du traitement identifiés précédemment (prise de risques au regard des bénéfices attendus) en appliquant les règles suivantes :

1. pour les risques dont la gravité et la vraisemblance sont élevées[30] : ces risques ne doivent pas être pris ;

2. pour les risques dont la gravité est élevée mais la vraisemblance faible[31] : ces risques peuvent être pris, mais uniquement s'il est démontré qu'il n'est pas possible de réduire leur gravité et si leur vraisemblance est négligeable ;

3. pour les risques dont la gravité est faible mais la vraisemblance élevée : ces risques peuvent être pris, mais uniquement s'il est démontré qu'il n'est pas possible de réduire leur vraisemblance et si leur gravité est négligeable ;

4. pour les risques dont la gravité et la vraisemblance sont faibles : ces risques peuvent être pris.

Il peut être acceptable de déroger à ces règles, mais uniquement s'il est démontré que les bénéfices du traitement sont largement supérieurs aux risques.

Note

On peut ainsi prendre des risques graves si leur vraisemblance est suffisamment réduite. On peut également prendre certains risques si le traitement permet de sauver des vies humaines.

[30] Niveaux 3. Important et 4. Maximal.
[31] Niveaux 1. Négligeable et 2. Limité.

RÉPUBLIQUE FRANÇAISE
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tél. : 01 53 73 22 22 – Fax : 01 53 73 22 00

Outillage

Le résultat de cette étape, qui consiste à présenter les mesures choisies pour traiter chaque risque et à ré-estimer sa gravité et sa vraisemblance, peut être formalisé dans un tableau tel que le suivant[32] :

	Risques				
Mesures[33] choisies pour traiter les risques	**1. Modification du traitement**	**2. Indisponibilité des processus légaux**	**3. Accès illégitime aux DCP**	**4. Modification non désirée des DCP**	**5. Disparition des DCP**
1. Minimiser les DCP	*X*		*X*	*X*	*X*
2. Informer les personnes concernées		*X*			
3. Sauvegarder les DCP	*X*	*X*		*X*	*X*
…	*…*	*…*	*…*	*…*	*…*
Gravité résiduelle	*2. Limité*	*3. Important*	*3. Important*	*1. Négligeable*	*1. Négligeable*
Vraisemblance résiduelle	*1. Négligeable*	*2. Limité*	*1. Négligeable*	*1. Négligeable*	*1. Négligeable*

Tableau 5- Mesures choisies pour traiter les risques

La description des mesures peut être présentée de la manière suivante :

Description des mesures choisies pour traiter les risques

1. Minimiser les DCP
Les DCP nécessaires à la finalité du traitement sont identifiées. Il est démontré pour chacune d'elles qu'elles sont indispensables.

2. Informer les personnes concernées
Les internautes sont informés via le formulaire de commande du site internet avec une typographie identique au reste du texte, de l'identité du responsable de traitement, de la finalité du traitement, du caractère obligatoire ou facultatif des informations collectées, des conséquences en cas de défaut de réponse, des destinataires de ces informations, des droits et de la personne auprès de qui les faire valoir, et des transmissions envisagées.

3. Sauvegarder les DCP
Les données du serveur sont sauvegardées tous les jours de manière incrémentale et toutes les semaines de manière complète. Les supports de sauvegarde sont chiffrés et stockés dans une armoire ignifugée. Un test de récupération des sauvegardes est effectué une fois par an.

[…]

[32] Il convient d'identifier les mesures (une par ligne) et d'indiquer le(s) risque(s) qu'elles traitent (un par colonne).
[33] Les mesures citées correspondent aux bonnes pratiques.

RÉPUBLIQUE FRANÇAISE
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tél. : 01 53 73 22 22 – Fax : 01 53 73 22 00

Annexes

Menaces génériques

Menaces qui peuvent affecter la confidentialité

Le tableau suivant présente les menaces génériques qui peuvent mener à :

- un accès illégitime aux DCP,
- une compromission du traitement (si cet événement redouté est considéré).

Menaces génériques	Exemples de menaces	Exemples de vulnérabilités des supports
C01. Usage anormal d'un matériel	Utilisation de clefs USB ou disques inappropriés à la sensibilité des informations, utilisation ou transport d'un matériel sensible à des fins personnelles…	Utilisable en dehors de l'usage prévu…
C02. Espionnage d'un matériel	Observation d'un écran à l'insu de son utilisateur dans un train, photographie d'un écran, géolocalisation d'un matériel, captation de signaux électromagnétiques à distance…	Permet d'observer des données interprétables, émet des signaux compromettants…
C03. Modification d'un matériel	Piégeage par un keylogger, retrait d'un composant matériel, branchement d'un appareil (ex. : clé USB) pour lancer un système d'exploitation ou récupérer des données…	Permet d'ajouter, retirer ou substituer des éléments (cartes, extensions…) via des connecteurs (ports, slots…), permet de désactiver des éléments (port USB…)…
C04. Perte d'un matériel	Vol d'un ordinateur portable dans une chambre d'hôtel, vol d'un téléphone portable professionnel par un pickpocket, récupération d'un matériel ou d'un support mis au rebut, perte d'un support de stockage électronique…	Petite taille, attractif (valeur marchande)…
C05. Détournement d'usage d'un logiciel	Fouille de contenu, croisement illégitime de données, élévation de privilèges, effacement de traces, envoi de *spams* depuis la messagerie, détournement de fonctions réseaux…	Donne accès à des données, permet de les manipuler (supprimer, modifier, déplacer…), peut être détourné de son usage nominal, permet d'utiliser des fonctionnalités avancées…
C06. Analyse d'un logiciel	Balayage d'adresses et ports réseau, collecte de données de configuration, étude d'un code source pour déterminer les défauts exploitables, test des réponses d'une base de données à des requêtes malveillantes…	Possibilité d'observer le fonctionnement du logiciel, accessibilité et intelligibilité du code source…
C07. Modification d'un logiciel	Piégeage par un keylogger logiciel, contagion par un code malveillant, installation d'un outil de prise de contrôle à distance, substitution d'un composant par un autre…	Modifiable (améliorable, paramétrable…), maîtrise insuffisante par les développeurs ou les mainteneurs (spécifications incomplètes, peu de compétences internes…), ne fonctionne pas correctement ou conformément aux attentes…
C08. Écoute passive d'un canal informatique	Interception de flux sur le réseau Ethernet, acquisition de données sur un réseau wifi…	Perméable (émission de rayonnements parasites ou non), permet d'observer des données interprétables…
C09. Espionnage d'une personne à distance	Divulgation involontaire en conversant, écoute d'une salle de réunion avec un matériel d'amplification sensorielle…	Peu discret (loquace, sans réserve…), routinier (habitudes facilitant l'espionnage récurrent)…
C10. Manipulation d'une personne	Influence (hameçonnage, filoutage, ingénierie sociale, corruption…), pression (chantage, harcèlement moral…)…	Influençable (naïf, crédule, obtus, faible estime de soi, faible loyauté…), manipulable (vulnérable aux pressions sur soi ou son entourage)…
C11. Récupération d'une personne	Débauchage d'un employé, changement d'affectation, rachat de tout ou partie de l'organisation…	Faible loyauté vis-à-vis de l'organisme, faible satisfaction des besoins personnels, facilité de rupture du lien contractuel…
C12. Visualisation d'un document papier	Lecture, photocopie, photographie…	Permet d'observer des données interprétables…
C13. Vol d'un document papier	Vol de dossiers dans les bureaux, vol de courriers dans la boîte aux lettres, récupération de documents mis au rebut…	Portable…
C14. Espionnage d'un canal papier	Lecture de parapheurs en circulation, reproduction de documents en transit…	Observable…

Tableau 6 - Menaces qui peuvent affecter la confidentialité

RÉPUBLIQUE FRANÇAISE
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tél. : 01 53 73 22 22 – Fax : 01 53 73 22 00

Menaces qui peuvent affecter l'intégrité

Le tableau suivant présente les menaces génériques qui peuvent mener à :

- une modification du traitement,
- une modification non désirée des DCP,
- une modification des processus légaux (si cet événement redouté est considéré).

Menaces génériques	Exemples de menaces	Exemples de vulnérabilités des supports
I01. Modification d'un matériel	Ajout d'un matériel incompatible menant à un dysfonctionnement, retrait d'un matériel indispensable au fonctionnement correct d'une application…	Permet d'ajouter, retirer ou substituer des éléments (cartes, extensions…) via des connecteurs (ports, slots…), permet de désactiver des éléments (port USB…)…
I02. Usage anormal d'un logiciel	Modifications inopportunes dans une base de données, effacement de fichiers utiles au bon fonctionnement, erreur de manipulation menant à la modification de données…	Donne accès à des données, permet de les manipuler (supprimer, modifier, déplacer…), peut être détourné de son usage nominal, permet d'utiliser des fonctionnalités avancées…
I03. Modification d'un logiciel	Manipulation inopportune lors de la mise à jour, configuration ou maintenance, contagion par un code malveillant, substitution d'un composant par un autre…	Modifiable (améliorable, paramétrable…), maîtrise insuffisante par les développeurs ou les mainteneurs (spécifications incomplètes, peu de compétences internes…), ne fonctionne pas correctement ou conformément aux attentes…
I04. Attaque du milieu via un canal informatique	*Man in the middle* pour modifier ou ajouter des données à un flux réseau, rejeu (réémission d'un flux intercepté)…	Permet d'altérer les flux communiqués (interception puis réémission, éventuellement après altération…), seule ressource de transmission pour le flux, permet de modifier les règles de partage du canal informatique (protocole de transmission qui autorise l'ajout de nœuds…)…
I05. Surcharge des capacités d'une personne	Charge de travail importante, stress ou perturbation des conditions de travail, emploi d'un personnel à une tâche non maîtrisée ou mauvaise utilisation des compétences…	Ressources insuffisantes pour les tâches assignées, capacités inappropriées aux conditions de travail, compétences inappropriées à la fonction Incapacité à s'adapter au changement…
I06. Manipulation d'une personne	Influence (rumeur, désinformation…)…	Influençable (naïf, crédule, obtus…)…
I07. Falsification d'un document papier	Modification de chiffres dans un dossier, remplacement d'un document par un faux…	Falsifiable (support papier au contenu modifiable)…
I08. Manipulation d'un canal papier	Modification d'une note à l'insu du rédacteur, changement d'un parapheur par un autre, envoi multiple de courriers contradictoires…	Permet d'altérer les documents communiqués, seule ressource de transmission pour le canal, permet la modification du circuit papier …

Tableau 7 - Menaces qui peuvent affecter l'intégrité

RÉPUBLIQUE FRANÇAISE
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tél. : 01 53 73 22 22 – Fax : 01 53 73 22 00

Menaces qui peuvent affecter la disponibilité

Le tableau suivant présente les menaces génériques qui peuvent mener à :

- une indisponibilité des processus légaux,
- une disparition des DCP
- une indisponibilité du traitement (si cet événement redouté est considéré).

Menaces génériques	Exemples de menaces	Exemples de vulnérabilités des supports
D01. Détournement d'usage d'un matériel	Stockage de fichiers personnels, utilisation à des fins personnelles…	Utilisable en dehors de l'usage prévu…
D02. Dépassement des limites de fonctionnement d'un matériel	Unité de stockage pleine, panne de courant, surexploitation des capacités de traitement, échauffement, température excessive…	Dimensionnement inapproprié des capacités de stockage, dimensionnement inapproprié des capacités de traitement, n'est pas approprié aux conditions d'utilisation, requiert en permanence de l'électricité pour fonctionner, sensible aux variations de tension…
D03. Modification d'un matériel	Ajout d'un matériel incompatible menant à une panne, retrait d'un matériel indispensable au fonctionnement du système…	Permet d'ajouter, retirer ou substituer des éléments (cartes, extensions…) via des connecteurs (ports, slots…), permet de désactiver des éléments (port USB…)…
D04. Détérioration d'un matériel	Inondation, incendie, vandalisme, dégradation du fait de l'usure naturelle, dysfonctionnement d'un dispositif de stockage…	Composants de mauvaise facture (fragile, facilement inflammable, sujet au vieillissement…) ; n'est pas approprié aux conditions d'utilisation ; effaçable (vulnérable aux effets magnétiques ou vibratoires…)…
D05. Perte d'un matériel	Vol d'un ordinateur portable, perte d'un téléphone portable, mise au rebut d'un support ou d'un matériel…	Portable, attractif (valeur marchande)…
D06. Usage anormal d'un logiciel	Effacement de données, utilisation de logiciels contrefaits ou copiés, erreur de manipulation menant à la suppression de données…	Donne accès à des données, permet de les manipuler (supprimer, modifier, déplacer…), peut être détourné de son usage nominal, permet d'utiliser des fonctionnalités avancées…
D07. Dépassement des limites d'un logiciel	Dépassement du dimensionnement d'une base de données, injection de données en dehors des valeurs prévues…	Permet de saisir n'importe quelle donnée, permet de saisir n'importe quel volume de données, permet d'exécuter des actions avec les données entrantes, peu interopérable…
D08. Modification d'un logiciel	Manipulation inopportune lors de la mise à jour, configuration ou maintenance, contagion par un code malveillant, substitution d'un composant par un autre…	Modifiable (améliorable, paramétrable…), maîtrise insuffisante par les développeurs ou les mainteneurs (spécifications incomplètes, peu de compétences internes…), ne fonctionne pas correctement ou conformément aux attentes…
D09. Suppression de tout ou partie d'un logiciel	Effacement d'un exécutable en production ou de code sources, bombe logique…	Possibilité d'effacer ou de supprimer des programmes, exemplaire unique, utilisation complexe (mauvaise ergonomie, peu d'explications…)…
D10. Perte d'un logiciel	Non renouvellement de la licence d'un logiciel utilisé pour accéder aux données…	Exemplaire unique (des contrats de licence ou du logiciel, développé en interne…), attractif (rare, novateur, grande valeur commerciale…), cessible (clause de cessibilité totale dans la licence…)…
D11. Saturation d'un canal informatique	Détournement de la bande passante, téléchargement non autorisé, coupure d'accès Internet…	Dimensionnement fixe des capacités de transmission (dimensionnement insuffisant de la bande passante, plage de numéros téléphoniques limitée…)…
D12. Dégradation d'un canal informatique	Sectionnement de câblage, mauvaise réception du réseau wifi…	Altérable (fragile, cassable, câble de faible structure, à nu, gainage disproportionné…), unique…
D13. Disparition d'un canal informatique	Vol de câbles de transmission en cuivre…	Attractif (valeur marchande des câbles…), transportable (léger, dissimulable…), peu visible (oubliable, insignifiant, peu remarquable…)…

RÉPUBLIQUE FRANÇAISE
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tél. : 01 53 73 22 22 – Fax : 01 53 73 22 00

Menaces génériques	Exemples de menaces	Exemples de vulnérabilités des supports
D14. Surcharge des capacités d'une personne	Charge de travail importante, stress ou perturbation des conditions de travail, emploi d'un personnel à une tâche non maîtrisée ou mauvaise utilisation des compétences…	Ressources insuffisantes pour les tâches assignées, capacités inappropriées aux conditions de travail, compétences inappropriées aux conditions d'exercice de ses fonctions, incapacité à s'adapter au changement…
D15. Atteinte d'une personne	Accident du travail, maladie professionnelle, autre blessure ou maladie, décès, affection neurologique, psychologique ou psychiatrique…	Limites physiques, psychologiques ou mentales…
D16. Départ d'une personne	Changement d'affectation, fin de contrat ou licenciement, rachat de tout ou partie de l'organisation…	Faible loyauté vis-à-vis de l'organisme, faible satisfaction des besoins personnels, facilité de rupture du lien contractuel…
D17. Effacement d'un document papier	Effacement progressif avec le temps, effacement volontaire de parties d'un texte…	Modifiable (support papier au contenu effaçable)…
D18. Dégradation d'un document papier	Vieillissement de documents archivés, embrasement des dossiers lors d'un incendie…	Composants de mauvaise facture (fragile, facilement inflammable, sujet au vieillissement…), n'est pas approprié aux conditions d'utilisation…
D19. Disparition d'un document papier	Vol de documents, perte de dossiers lors d'un déménagement, mise au rebut…	Portable…
D20. Saturation d'un canal papier	Surcharge de courriers, surcharge d'un processus de validation…	Existence de limites quantitatives ou qualitatives…
D21. Dégradation d'un canal papier	Coupure du flux suite à une réorganisation, blocage du courrier du fait d'une grève…	Instable, unique…
D22. Modification d'un canal papier	Modification dans l'expédition des courriers Réorganisation de circuits papier, changement de langue professionnelle…	Modifiable (remplaçable…)…
D23. Disparition d'un canal papier	Réorganisation supprimant un processus, disparition d'un transporteur de documents…	Utilité non reconnue…

Tableau 8 - Menaces qui peuvent affecter la disponibilité

RÉPUBLIQUE FRANÇAISE
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tél. : 01 53 73 22 22 – Fax : 01 53 73 22 00

Acronymes

CIL	Correspondant Informatique et Libertés
CNIL	Commission Nationale de l'Informatique et des Libertés
DCP	Donnée à Caractère Personnel
EBIOS	Expression des Besoins et Identification des Objectifs de Sécurité
MOA	Maîtrise d'OuvrAge
MOE	Maîtrise d'Œuvre
RSSI	Responsable de la Sécurité des Systèmes d'Information
SSI	Sécurité des Systèmes d'Information

Définitions

(les libellés entre parenthèses correspondent aux libellés courts employés dans ce document)

Donnée à caractère personnel (DCP)	Constitue une donnée à caractère personnel toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres. Pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens en vue de permettre son identification dont dispose ou auxquels peut avoir accès le responsable du traitement ou toute autre personne. [Loi-I&L]
Élément à protéger	Processus (ceux du traitement, dans la mesure où des DCP sont traitées, et ceux requis par la [Loi-I&L]) ou DCP (d'un traitement ou utilisé par les processus légaux) dont on veut préserver la disponibilité, l'intégrité ou la confidentialité.
Événement redouté	Incident qui affecte la disponibilité, l'intégrité ou la confidentialité des éléments à protéger.
Gestion des risques	Processus itératif permettant de maîtriser objectivement les risques qui pèsent sur la vie privée des personnes concernées par un traitement de DCP. Il consiste essentiellement à les apprécier (identification, estimation en termes de gravité et de vraisemblance, et évaluation comparative), les traiter (détermination et mise en place de mesures proportionnées), accepter les risques résiduels, communiquer (consultation des parties prenantes, présentation de résultats…), et surveiller les évolutions dans le temps (du contexte, des risques, des mesures…).

RÉPUBLIQUE FRANÇAISE
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tél. : 01 53 73 22 22 – Fax : 01 53 73 22 00

Gravité	Estimation de l'ampleur des impacts potentiels sur la vie privée des personnes concernées. Elle dépend essentiellement du caractère identifiant des DCP et du caractère préjudiciable des impacts potentiels.
Menace	Mode opératoire type utilisé par des sources de risques et pouvant provoquer un événement redouté.
Mesure	Action à entreprendre pour traiter des risques. Elle peut consister à les éviter, les réduire, les transférer ou les prendre.
Personnes concernées	Les personnes concernées par un traitement de données à caractère personnel sont celles auxquelles se rapportent les données qui font l'objet du traitement. [Loi-I&L]
Responsable de traitement	Le responsable d'un traitement de données à caractère personnel est, sauf désignation expresse par les dispositions législatives ou réglementaires relatives à ce traitement, la personne, l'autorité publique, le service ou l'organisme qui détermine ses finalités et ses moyens. [Loi-I&L]
Risque	Scénario décrivant un événement redouté et toutes les menaces qui le rendent possibles. Il est estimé en termes de gravité et de vraisemblance.
Source de risque	Personne ou source non humaine qui peut être à l'origine d'un risque, de manière accidentelle ou délibérée.
Support	Bien sur lequel reposent des éléments à protéger. Il peut s'agir de matériels, de logiciels, de canaux informatiques, de personnes, de supports papier ou de canaux de transmission papier.
Traitement de données à caractère personnel (traitement)	Constitue un traitement de données à caractère personnel toute opération ou tout ensemble d'opérations portant sur de telles données, quel que soit le procédé utilisé, et notamment la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction. [Loi-I&L]
Vraisemblance	Estimation de la possibilité qu'un risque se réalise. Elle dépend essentiellement des vulnérabilités exploitables et des capacités des sources de risques à les exploiter.
Vulnérabilité	Caractéristique d'un support, exploitable par des sources de risques et permettant à des menaces de se réaliser.

RÉPUBLIQUE FRANÇAISE
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tél. : 01 53 73 22 22 – Fax : 01 53 73 22 00

Violation de données à caractère personnel (violation de DCP)	Une violation de la sécurité entraînant accidentellement ou de manière illicite la destruction, la perte, l'altération, la divulgation ou l'accès non autorisés de données à caractère personnel transmises, stockées ou traitées d'une autre manière en relation avec la fourniture de services de communications électroniques accessibles au public dans la Communauté. [Ordonnance-2011-1012]

Textes et références bibliographiques

[Directive-1995-46]	Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.
[Directive-2002-58]	Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques modifiée[34].
[Ordonnance-2011-1012]	Ordonnance 2011 1012 relative aux communications électroniques transposant notamment la directive 2009/136/CE introduisant l'obligation de notification des violations de données à caractère personnel collectées dans le cadre de traitement mis en œuvre par des fournisseurs de services de télécommunication ouverts au public.
[Loi-I&L]	Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés modifiée[35].
[ISO31000]	ISO 31000:2009, Management du risque – Principes et lignes directrices, ISO.
[EBIOS]	*Expression des Besoins et Identification des Objectifs de Sécurité – EBIOS – Méthode de gestion des risques*, 25 janvier 2010, ANSSI.
[CNIL-GuideSécurité]	Guide *« La sécurité des données personnelles »*, édition 2010, CNIL.

[34] Modifiée par la Directive 2009/136/CE du Parlement européen et du Conseil du 25 novembre 2009.
[35] Modifiée par la loi n°2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et par la loi n° 2009-526 du 12 mai 2009 de simplification et de clarification du droit et d'allègement des procédures.

RÉPUBLIQUE FRANÇAISE
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tél. : 01 53 73 22 22 – Fax : 01 53 73 22 00