Les risques en protection des données – L'analyse au pouce levé (ou à la louche) ?

Yvann Barras / Livio di Tria

Table des matières

A. Introduction

La Loi fédérale du 25 septembre 2020 sur la protection des données (LPD) et ses ordonnances d'exécution,[1] entrées en vigueur le 1er septembre 2023, ont marqué un tournant significatif dans le cadre législatif suisse en matière de protection des données. Plus d'une année après son entrée en vigueur, la LPD reste au centre des discussions, tant en raison de son impact sur le secteur privé et public que de la place prépondérante que continue d'occuper la protection des données dans la vie des citoyens.

La LPD occupe également une place importante pour les praticiens du domaine, en raison des nombreuses questions qu'elle soulève et des défis qu'elle impose dans

[1] À savoir l'Ordonnance fédérale du 31 août 2022 sur la protection des données (OPDo ; RS 235.11) et l'Ordonnance fédérale du 31 août 2022 sur les certifications en matière de protection des données (OCPD ; RS 235.13).

sa mise en œuvre. Si, dans sa forme théorique, la LPD peut sembler relativement accessible, sa traduction pratique s'avère souvent complexe pour les entreprises et les administrations cherchant à assurer leur conformité.

Les risques jouent un rôle central dans l'élaboration et la mise en œuvre des mesures de sécurité. Chaque mesure qu'une entreprise prend pour protéger les données doit être fondée sur une analyse des risques. La conformité en matière de protection des données ne se limite pas à l'application mécanique des règles prévues par la LPD : elle exige une approche proactive et systématique pour identifier, apprécier et maîtriser les risques liés aux traitements de données personnelles.

Cet article explore comment les organisations peuvent aborder ces défis en matière de gestion des risques, et propose une approche méthodologique à suivre. Pour ce faire, l'article rappelle l'approche fondée sur les risques qui a guidé le législateur dans le cadre de la révision de la LPD (chapitre B), précise la notion de risque et de ses composantes (chapitre C), aborde la gestion des risques (chapitre D) et présente un panorama non exhaustif des méthodologies les plus connues (chapitre E), propose une méthodologie adaptée au domaine de la protection des données (chapitre F), avant de conclure (chapitre G).

B. Approche fondée sur le risque

Le concept de risque est fréquemment mentionné par la LPD. La fréquence à laquelle la LPD mentionne ce concept s'explique par la place centrale qu'occupe l'approche fondée sur le risque, autour de laquelle les différents concepts en matière de protection des données s'articulent.[2]

L'approche fondée sur le risque met l'accent sur le processus de gestion des risques envers les personnes concernées par le traitement de leurs données personnelles. Selon cette approche, l'État et les organisations doivent déceler à temps les **risques qui pèsent sur la sphère privée** et sur l'**autodétermination informationnelle**. Ils doivent également intégrer les exigences relatives à la protection des données dès la conception de leurs projets, qu'ils soient digitaux ou non.

Cette approche se concentre ainsi sur l'identification des menaces spécifiques qui pourraient affecter la **personnalité** et les **droits fondamentaux des personnes concernées**, en tenant compte des traitements menés par le responsable du traitement ou le sous-traitant. En pratique, cela signifie que les obligations sont proportionnelles au niveau de risque associé aux traitements. Le responsable du traitement dont l'activité principale consiste à traiter des données personnelles sensibles est typiquement soumis à des exigences de sécurité plus strictes que le responsable du traitement qui ne traite pas de données personnelles sensibles. À titre illustratif, nous mentionnerons l'exemple selon lequel les exigences sont plus élevées pour un

[2] Conformément au Message du 15 septembre 2017 concernant la Loi fédérale sur la révision totale de la Loi fédérale sur la protection des données et sur la modification d'autres lois fédérales (FF 2017 6565), le Conseil fédéral souligne que le projet de révision repose sur sept principes. Le premier à être mentionné, et probablement le plus important aux côtés de la neutralité technologique, est l'approche fondée sur le risque (FF 2017 6565, 6593 s.).

hôpital qui traite régulièrement des données personnelles sensibles que pour une boulangerie ou une boucherie qui traite les données de ses clients ou de ses fournisseurs.[3]

L'approche fondée sur le risque est utilisée **au-delà de la protection des données** et n'est pas propre qu'à la Suisse. Nous la retrouvons notamment au sein de diverses législations européennes en lien avec le numérique, telles que le Règlement (UE) 2022/2065 relatif à un marché unique des services numériques, le Règlement (UE) 2022/2554 sur la résilience opérationnelle numérique du secteur financier ou le Règlement (UE) 2024/1689 établissant des règles harmonisées concernant l'intelligence artificielle. L'approche fondée sur le risque se retrouve également au sein d'autres législations spécifiques à certains secteurs, telles que le droit bancaire, le droit de l'environnement ou encore la sécurité de l'information.[4]

L'approche fondée sur le risque permet de créer un cadre flexible et adapté, capable de répondre efficacement aux défis spécifiques de chaque domaine. Elle permet également de respecter le caractère technologiquement neutre des législations touchant au numérique, en traitant les risques de manière indépendante de toute technologie. En matière de protection des données, l'objectif de l'approche fondée sur le risque est de garantir que les mesures prises par le responsable du traitement ou le sous-traitant sont adaptées et proportionnées aux risques, assurant une protection efficace de la personnalité et des droits fondamentaux des personnes concernées. L'approche fondée sur le risque se matérialise comme suit :

– Premièrement, cette approche exige du responsable du traitement et du sous-traitant qu'ils assurent, par des mesures organisationnelles et techniques appropriées, une sécurité adéquate des données personnelles par rapport au risque encouru.[5] Il s'agit ici de l'une des émanations les plus fortes de l'approche fondée sur le risque, dès lors que le principe de sécurité s'applique en toutes circonstances, contrairement à certaines obligations qui ne doivent être mises en œuvre que sous certaines conditions.
– Deuxièmement, le responsable du traitement est tenu de mettre en place des mesures techniques et organisationnelles dès la conception d'un traitement afin que celui-ci respecte les prescriptions de protection des données. Ces mesures doivent être appropriées au regard notamment du risque que le traitement des données présente.[6]
– Troisièmement, l'entreprise qui emploie moins de 250 collaborateurs et dont le traitement des données présente un risque limité d'atteinte à la personnalité des

3 Cet exemple est directement tiré du rapport explicatif du 31 août 2022 de l'OPDo. Cf. Office fédéral de la justice, Rapport explicatif du 31 août 2022 — Ordonnance sur la protection des données (OPDo), 19.

4 L'art. 8 de la Loi fédérale du 18 décembre 2020 sur la sécurité de l'information au sein de la Confédération (LSI ; RS 128) concerne spécifiquement la gestion des risques par les autorités et organisations concernées, qui doivent prendre des mesures nécessaires pour éliminer les risques ou les ramener à un niveau acceptable.

5 Cette exigence découle du principe de sécurité ancré à l'art. 8 LPD (FF 2017 6565, 6650).

6 Cette exigence découle de l'obligation de protection des données dès la conception ancrée à l'art. 7 LPD (FF 2017 6565, 6649).

personnes concernées n'est pas obligée d'établir un registre des activités de traitement.[7]

- Quatrièmement, le responsable du traitement doit procéder à une analyse d'impact relative à la protection des données (AIPD) si le traitement envisagé est susceptible d'entraîner un risque élevé.[8]
- Cinquièmement, le responsable du traitement doit annoncer au Préposé fédéral à la protection des données et à la transparence (PFPDT) les cas de violation de la sécurité des données entraînant vraisemblablement un risque élevé.[9]

L'approche fondée sur le risque se manifeste encore dans le cadre de la distinction entre le profilage (art. 5 let. f LPD)[10] et le profilage à risque élevé (art. 5 let. g LPD), apparaît comme une condition dans le cadre de la désignation – ou non – par le responsable du traitement privé qui a son siège ou son domicile à l'étranger d'un représentant (art. 14 LPD)[11] ou dans le cadre du rang de la base légale en lien avec le traitement de données personnelles par des organes fédéraux (art. 34 LPD).

L'approche fondée sur le risque occupe finalement une place importante dans l'analyse des principes généraux de la protection des données. Le principe d'exactitude (art. 6 al. 5 LPD) souligne par exemple que le caractère approprié d'une mesure permettant de rectifier, d'effacer ou de détruire les données inexactes ou incomplètes au regard des finalités pour lesquelles elles sont collectées ou traitées dépend en partie du risque que le traitement des données en question présente.

Bien que l'approche fondée sur le risque soit théoriquement facile à comprendre dans son acception générale, la concrétiser et l'appliquer dans la pratique s'avère bien plus ardu.[12] Cette complexité réside notamment dans le fait que, même si la notion de risque reste la même, ses émanations varient en fonction de chaque obligation, par exemple :

---

7 Cette exigence découle de l'obligation de tenir un registre des activités de traitement ancrée à l'art. 12 LPD. À noter que si le traitement porte sur des données sensibles à grande échelle ou constitue un profilage à risque élevé, le registre des activités de traitement doit dans tous les cas être établi (art. 24 OPDo).

8 Cette exigence découle de l'obligation de réaliser une AIPD ancrée à l'art. 22 LPD et l'obligation de consulter le PFPDT dans le cas d'un risque résiduel élevé ancrée à l'art. 23 LPD.

9 Cette exigence découle de l'obligation d'annonce des violations de la sécurité des données ancrée à l'art. 24 LPD.

10 L'application de certaines règles dépendent elles-mêmes de savoir si l'on a affaire ou non à un profilage à risque élevé, comme pour la forme que doit revêtir le consentement (art. 6 al. 7 let. b et c LPD) ou dans le cadre du motif justificatif relatif à l'évaluation de la solvabilité de la personne concernée (art. 31 al. 2 let. c ch. 1 LPD).

11 La désignation d'un représentant par le responsable du traitement privé au sens de l'art. 14 LPD n'est nécessaire que dans le cas où celui-ci traite des données personnelles concernant des personnes en Suisse et que le traitement remplit plusieurs conditions, dont notamment celle selon laquelle le traitement présente un risque élevé (art. 14 al. 1 let. d LPD).

12 Dans le même sens, *François Charlet*, Protection des données : enjeux et risques pour les entreprises, in : Défago/Dunand/Mahon et al. (éd.), La protection des données dans les relations de travail à la lumière de la nouvelle loi fédérale sur la protection des données, 2024, 49.

– L'AIPD a pour but de déterminer si un traitement envisagé comporte un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée. L'analyse du risque intervient en amont du traitement envisagé et se concentre uniquement sur celui-ci.
– Le profilage est considéré à risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée lorsqu'il conduit à un appariement de données qui permet d'apprécier les caractéristiques essentielles de la personnalité d'une personne physique. L'analyse du risque se concentre ici sur les données utilisées dans le cadre d'un profilage et les résultats qui peuvent en découler pour les personnes concernées.
– L'annonce des violations de la sécurité des données vise à protéger les personnes concernées lorsqu'une violation s'est produite. L'analyse du risque se focalise ici sur les données qui ont été violées et sur les potentielles conséquences qui découlent de la violation pour les personnes concernées.

En plus de ces variations dans les émanations du risque, il est important de noter que ni les dispositions générales de la protection des données ni celles inscrites dans des lois spéciales n'indiquent de méthodologies précises pour procéder aux analyses de risque.[13] Cette absence laisse ainsi une grande marge d'appréciation aux organisations, tout en ajoutant une couche supplémentaire de complexité dans la mise en œuvre pratique de la LPD.

Parce qu'elle est sujette à interprétation en raison de son caractère indéterminé, l'approche fondée sur le risque[14] utilisée dans la LPD ouvre aux organisations et à la surveillance de la protection des données assurée par le PFPDT un vaste champ d'application. L'approche fondée sur le risque peut être déconcertante pour les juristes, car elle requiert des connaissances au-delà du domaine juridique, avec lesquelles ils peuvent ne pas être familiers ou pour lesquelles ils ne sont – malheureusement – pas formés. On comprend donc bien que la protection des données ne puisse pas être pensée sous le seul prisme juridique, mais doit également intégrer les pratiques issues du prisme normatif, en particulier les normes internationales relatives à la gestion des risques ou à la sécurité de l'information. En fin de compte, la LPD ne peut être appliquée efficacement qu'en intégrant ces différentes perspectives.

C'est pour cette raison que nous avons opté pour une approche plus concrète dans cet article, afin de proposer une approche méthodologique pratique adaptée à la gestion des risques en protection des données. L'objectif est de rendre l'approche fondée sur le risque plus accessible en offrant des outils concrets et opérationnels, permettant aux organisations de mieux gérer la complexité de la protection des données.

---

13 *François Charlet*, Protection des données : enjeux et risques pour les entreprises, in : Défago/Dunand/Mahon et al. (éd.), La protection des données dans les relations de travail à la lumière de la nouvelle loi fédérale sur la protection des données, 2024, 49.

14 Et plus largement la notion de « risque » utilisée au sein de la LPD.

C. Notion de risque

I. Définition

Le concept de risque peut être défini comme la **possibilité que survienne un événement indésirable ou imprévu pouvant avoir un impact sur des objectifs**. Dans la conception générale du risque, l'impact d'un risque peut être neutre, positif ou négatif en fonction du point de vue de l'observateur.[15] Dans le domaine de sécurité de l'information, les risques sont associés à un effet négatif sur les objectifs de sécurité.[16] En revanche, dans le cadre de la protection des données, il est également question des effets négatifs sur la personnalité ou les droits fondamentaux des personnes concernées.[17]

Dans ces domaines, un risque peut être exprimé en termes de sources de risque et d'événements redoutés avec leur gravité et leur vraisemblance.

II. Cadre de référence

En matière de gestion des risques, les **normes internationales** constituent un excellent cadre de référence.

Les normes sont des règles volontaires qui recouvrent pratiquement tous les domaines de la vie économique et de la vie quotidienne modernes. Elles énoncent les meilleures pratiques et décrivent des manières de procéder afin de répondre à une problématique. L'organisation internationale de normalisation (*International Organization for Standardization*, ISO) et les organismes de normalisation nationaux[18] s'efforcent de répondre aux besoins du marché au travers de normes qui sont développées et rédigées par des experts provenant de différents horizons, et qui, pour la plupart, les utiliseront au quotidien dans leurs propres travaux.

La norme ISO 31000[19] (Management du risque) et la norme ISO 27005[20] (Préconisations pour la gestion des risques liés à la sécurité de l'information) s'avèrent particulièrement importantes dans le contexte de la gestion des risques en matière de protection des données.

La norme ISO 27005 fait partie de la famille de normes ISO 27000 qui traite du management de la sécurité de l'information, aux côtés de la norme ISO 27001 (Sys-

15 ISO 31000:2018, Management du risque — Lignes directrices, art. 3.1.

16 ISO 27005:2022, Sécurité de l'information, cybersécurité et protection de la vie privée — Préconisations pour la gestion des risques liés à la sécurité de l'information, art. 3.1.3, note 5.

17 ISO 27701:2019, Techniques de sécurité – Extension d'ISO/IEC 27001 et ISO/IEC 27002 au management de la protection de la vie privée – Exigences et lignes directrices, art. 5.1.

18 P. ex. la *Schweizerische Normen-Vereinigung* (SNV) en Suisse.

19 La norme ISO 31000 fournit des lignes directrices concernant la gestion des risques de manière générale. La norme ISO 31000 s'applique à toute forme de risque, sans être spécifique à un domaine ou à une industrie. Il est ici question de la version 2018 de la norme ISO 31000.

20 La norme ISO 27005 fournit des préconisations spécifiques concernant la gestion des risques liés à la sécurité de l'information. Il est ici question de la version 2022 de la norme ISO 27005.

tème de management de la sécurité de l'information, SMSI) qui permet la certification des personnes et des organisations. La norme ISO 27001 et son SMSI sont, par ailleurs, spécifiquement complétés en matière de protection des données par la norme ISO 27701 (Système de management de la protection de la vie privée, PIMS). Cette dernière permet également la certification des personnes et des organisations. Il convient de noter que la certification du PIMS d'une organisation n'est possible qu'en complément d'un SMSI selon ISO 27001. Il ne s'agit donc pas d'un système de management à part entière, mais d'une extension de celui-ci, et ce pour la protection de la vie privée dans le cadre d'un traitement de données personnelles.

III. Concepts fondamentaux

1. Axes de protection et besoins de protection

La sécurité des données repose sur trois axes de protection :

- la **confidentialité**, qui se définit comme la propriété selon laquelle l'information n'est ni diffusée ni divulguée à des personnes, des entités ou des processus non autorisés ;[21]
- **l'intégrité**, qui se définit comme la propriété selon laquelle l'information est exacte, complète et qu'elle n'est pas altérée de manière non autorisée ;[22] et
- la **disponibilité**, qui se définit comme la propriété selon laquelle l'information est accessible et utilisable par une personne, une entité ou un processus autorisé quand et où il en a besoin.[23]

En matière de protection des données, nous considérons également la **traçabilité** comme un axe de protection.[24] La traçabilité fait référence à la capacité de suivre les actions effectuées sur une information de manière à être notamment auditable.

Le **besoin de protection** détermine quelles mesures doivent être mises en place et à quel degré pour garantir un niveau de sécurité approprié sur un axe de protection spécifique.[25] Les quatre axes de protection ne s'appliquent pas nécessairement à toutes les données de la même manière. Par exemple, pour certaines données, seule la confidentialité peut être requise, avec des niveaux de protection variés selon le contexte. Prenons l'exemple de la classification des documents, qui peuvent être classés selon si le document est public, restreint ou confidentiel. Chaque niveau

---

21 ISO 27000:2018, Technologies de l'information — Techniques de sécurité — Systèmes de management de la sécurité de l'information — Vue d'ensemble et vocabulaire, art. 3.10.

22 ISO 27000:2018, Technologies de l'information — Techniques de sécurité — Systèmes de management de la sécurité de l'information — Vue d'ensemble et vocabulaire, art. 3.36.

23 ISO 27000:2018, Technologies de l'information — Techniques de sécurité — Systèmes de management de la sécurité de l'information — Vue d'ensemble et vocabulaire, art. 3.7.

24 La traçabilité n'est pas explicitement définie comme un axe de protection indépendant dans les normes internationales relatives à la sécurité de l'information. Elle est néanmoins implicitement incluse dans des concepts clés comme la journalisation. Cependant, elle est reconnue comme un élément à part entière par la LPD, mais également par la LSI, qui exigent des mécanismes permettant de retracer les traitements et les accès aux données.

25 Dans le domaine de la protection des données, le besoin de protection est précisé par l'art. 1 al. 2 OPDo (cf. *infra* F. II. 2. b)).

de classification impose des mesures de sécurité plus ou moins strictes. Le besoin de protection détermine ainsi l'intensité des mesures à mettre en place pour assurer un niveau de protection adéquat sur l'axe concerné.

2. Sources de risque et événements redoutés

Un risque peut être exprimé en termes de **sources de risque** et **d'événements redoutés** en relation avec leur **gravité** et leur **vraisemblance**.

Dans le domaine de la sécurité de l'information, le risque est généralement exprimé par la possibilité qu'une menace exploite une vulnérabilité d'un actif informationnel et porte ainsi atteinte à l'organisation.[26] Ces deux expressions du risque sont équivalentes et dépendent essentiellement de la méthodologie utilisée d'un point de vue terminologique.

La **source de risque** correspond à tout élément qui, seul ou combiné à d'autres, est susceptible d'engendrer un risque.[27] Il s'agit donc de la cause d'un risque, c'est-à-dire de la menace. La source de risque peut être de nature environnementale, intentionnelle ou accidentelle.[28]

La norme ISO 27005 propose de séparer la source de risque en 7 catégories :[29]

- les menaces physiques (p. ex. un incendie ou une inondation) ;
- les menaces naturelles (p. ex. un phénomène sismique ou un phénomène météorologique) ;
- les défaillances des infrastructures (p. ex. la défaillance d'un système d'alimentation ou d'un réseau de télécommunication) ;
- les défaillances techniques (p. ex. la saturation d'un système d'information) ;
- les actions humaines (p. ex. l'ingénierie sociale ou le vol de documents) ;
- la compromission de fonctions ou de services (p. ex. une erreur d'utilisation ou le reniement d'action) ; et
- les menaces organisationnelles (p. ex. le manque de personnel ou la défaillance d'un prestataire de services).

L'événement redouté représente la manifestation concrète du risque. Dans le contexte de la sécurité de l'information, un événement redouté survient lorsqu'une source de risque parvient à exploiter une vulnérabilité présente dans un actif informationnel. S'il se produit, l'événement redouté altérera un ou plusieurs axes de protection.

---

26 ISO 27005:2022, Sécurité de l'information, cybersécurité et protection de la vie privée — Préconisations pour la gestion des risques liés à la sécurité de l'information, art. 3.1.3, note 7.

27 ISO 27005:2022, Sécurité de l'information, cybersécurité et protection de la vie privée — Préconisations pour la gestion des risques liés à la sécurité de l'information, art. 3.1.6.

28 Il est intéressant de noter qu'une même source de risque peut être de plusieurs natures. Un incendie peut ainsi être d'origine accidentelle, intentionnelle ou environnementale.

29 ISO 27005:2022, Sécurité de l'information, cybersécurité et protection de la vie privée — Préconisations pour la gestion des risques liés à la sécurité de l'information, annexe A, tableau 10.

La norme ISO 27005 propose de séparer les vulnérabilités types en 6 catégories :[30]

- matériel (p. ex. du stockage non protégé ou un manque de prudence lors de la mise au rebut) ;
- logiciel (p. ex. un logiciel insuffisamment testé ou une interface utilisateur compliquée) ;
- réseau (p. ex. un mauvais câblage ou une connexion au réseau public non protégée) ;
- personnel (p. ex. un niveau de formation insuffisant ou des mécanismes de surveillance absents) ;
- site (p. ex. un emplacement situé en zone inondable) ; et
- organisme (p. ex. une attribution inappropriée des responsabilités).

À titre illustratif, un événement redouté peut être formulé comme une inondation causée par de fortes pluies (la source de risque), qui rend le centre de données indisponible (l'axe de protection qui concerne la disponibilité), car il se situe en zone inondable (la vulnérabilité).

IV. Composantes du risque

En partant du postulat qu'un risque s'exprime en termes de sources de risque et d'événements redoutés, en relation avec leur gravité et leur vraisemblance, l'équation suivante peut être établie pour modéliser l'appréciation du risque :

[Gravité] x [Vraisemblance] = [Niveau de risque]

1. Gravité

La **gravité** correspond à **l'intensité des impacts d'un risque**.[31] En matière de protection des données, l'appréciation de la gravité consiste à mesurer les impacts sur la personnalité ou les droits fondamentaux des personnes concernées dans le cas où le risque se réalise. En matière de sécurité de l'information, l'appréciation de la gravité est plus large dans la mesure où d'autres types d'impacts doivent être pris en compte, comme les impacts financiers (directs ou indirects), les impacts sur l'image et la réputation ou encore les impacts sociétaux. À noter encore que dans le domaine de la sécurité de l'information, les impacts sont mesurés envers l'organisation, et non vis-à-vis des personnes concernées.

---

30 ISO 27005:2022, Sécurité de l'information, cybersécurité et protection de la vie privée — Préconisations pour la gestion des risques liés à la sécurité de l'information, annexe A, tableau 11.

31 La norme ISO 27005 utilise le terme de « conséquences » et non de « gravité ». Selon notre expérience, l'utilisation du terme de « conséquences » dans la gestion des risques engendre souvent la confusion entre, d'une part, les conséquences concrètes si le risque se réalisée et, d'autre part, l'intensité des conséquences qui est une appréciation qualitative ou quantitative qui permet de déterminer le niveau de risque (cf. *infra* C. IV. 3.). Nous recommandons l'usage de la notion de « gravité » pour exprimer l'intensité et « d'impact » pour exprimer les effets concrets du risque.

La gravité s'apprécie généralement de manière qualitative sur la base d'une échelle comportant différents niveaux. Il appartient à chaque organisation de définir cette échelle de manière pertinente avec son propre contexte. L'échelle d'appréciation du niveau de gravité suivante est proposée sur la base de la norme ISO 29134 dans le domaine de la protection des données :[32]

Niveau	Description
Négligeable	Les personnes concernées ne seront pas affectées ou peuvent subir quelques désagréments qu'elles surmonteront sans aucun problème.
Limité	Les personnes concernées peuvent rencontrer d'importants désagréments qu'elles seront en mesure de surmonter au prix de quelques difficultés.
Important	Les personnes concernées peuvent rencontrer d'importants désagréments qu'elles seront en mesure de surmonter au prix de difficultés majeures.
Maximal	Les personnes concernées peuvent subir des conséquences graves, voire irréversibles, qu'elles pourront ne pas être en mesure de surmonter.

Tableau 1 : Échelle d'appréciation du niveau de gravité basée sur la norme ISO 29134

Afin d'illustrer le niveau de gravité, la norme ISO 29134 fournit également des exemples d'impacts :

Niveau	Exemples
Négligeable	Temps passé à saisir de nouveau les informations, gênes, irritations.
Limité	Coûts supplémentaires, refus d'accès aux services métiers, troubles physiques mineurs.
Important	Détournement de fonds, mise sur liste noire par des établissements bancaires, dommages matériels, perte d'emploi, citation à comparaître, aggravation de l'état de santé.
Maximal	Détresse financière telle qu'une dette irrécouvrable ou une incapacité de travail, troubles psychologiques ou physiques de longue durée, décès.

Tableau 2 : Exemples d'impacts selon le niveau de gravité basée sur la norme ISO 29134

2. Vraisemblance

La **vraisemblance** correspond à la **possibilité qu'un risque se produise**.[33] La norme ISO 27005 précise ce qui suit :

« Dans la terminologie de la gestion des risques, le mot "vraisemblance" est utilisé pour indiquer la possibilité que quelque chose se produise, que cette possibilité soit définie, mesurée ou déterminée de façon objective ou subjective, qualitative ou quantitative, et qu'elle soit décrite au

[32] ISO 29134:2023, Technologies de l'information — Techniques de sécurité — Lignes directrices pour l'étude d'impacts sur la vie privée, annexe A, art. 2.

[33] ISO 27005:2022, Sécurité de l'information, cybersécurité et protection de la vie privée — Préconisations pour la gestion des risques liés à la sécurité de l'information, art. 3.1.13.

moyen de termes généraux ou mathématiques (telles une probabilité ou une fréquence sur une période donnée). »[34]

D'un point de vue terminologique, on parle donc de vraisemblance dans la mesure où le terme anglais « *likehood* » utilisé n'a pas d'équivalent français. Si le terme « probabilité » est souvent utilisé, la norme précise toutefois que celui-ci est davantage destiné à une interprétation mathématique.[35] Ainsi le terme « vraisemblance » lui est préféré dans l'intention qu'il fasse l'objet d'une interprétation plus large.

L'appréciation de la vraisemblance est intrinsèquement incertaine, non seulement parce qu'elle tient compte d'éléments qui ne se sont pas encore produits et qui ne sont pas entièrement connus, mais aussi, car la vraisemblance est une mesure statistique et n'est pas directement représentative d'événements isolés.

Toute comme pour la gravité, la vraisemblance s'apprécie sur la base d'une échelle comportant différents niveaux qui doivent être définis par l'organisation. L'échelle d'appréciation proposée ci-après se fonde sur la norme ISO 29134 :[36]

Niveau	**Description**
Invraisemblable	Il ne semble pas possible pour la source de risque d'exécuter une menace en exploitant les propriétés des actifs sous-jacents.
Peu vraisemblable	Il semble difficile pour la source de risque d'exécuter une menace en exploitant les propriétés des actifs à l'appui.
Vraisemblable	Il semble possible pour la source de risque d'exécuter une menace en exploitant les propriétés des actifs sous-jacents.
Quasi certain	Il semble extrêmement facile pour la source de risque d'exécuter une menace en exploitant les propriétés des actifs sous-jacents.

Tableau 3 : Échelle de niveau de vraisemblance basée sur la norme ISO 29134

3. Niveau de risque

Résultat de l'équation utilisée pour modéliser l'appréciation du risque, le **niveau de risque représente l'importance d'un risque exprimée par le produit de sa gravité et de sa vraisemblance**. Au-delà d'exprimer l'importance du risque, le niveau de risque permet d'évaluer le risque, afin de déterminer si celui-ci est par exemple acceptable, tolérable ou inacceptable.

Pour déterminer le niveau de risque, l'organisation doit, d'une part, définir une échelle de niveaux de risque et, d'autre part, définir une matrice déterminant le niveau de risque selon le produit de la gravité et de la vraisemblance. De la même

[34] ISO 27005:2022, Sécurité de l'information, cybersécurité et protection de la vie privée — Préconisations pour la gestion des risques liés à la sécurité de l'information, art. 3.1.13, note 1.

[35] ISO 27005:2022, Sécurité de l'information, cybersécurité et protection de la vie privée — Préconisations pour la gestion des risques liés à la sécurité de l'information, art. 3.1.13, note 2.

[36] ISO 29134:2023, Technologies de l'information — Techniques de sécurité — Lignes directrices pour l'étude d'impacts sur la vie privée, annexe A, art. 3.

manière que pour les précédentes échelles, l'organisation doit déterminer les différents niveaux de risque, mais aussi la position de chaque niveau au sein de la matrice de niveau de risque, et ce en relation avec son appétence aux risques. En règle générale, l'échelle de niveau de risque comprend trois niveaux, à savoir « faible », « modéré » et « élevé ». Pour chacun de ces niveaux, l'organisation détermine par exemple si le risque est évalué comme acceptable, tolérable ou inacceptable. Chaque évaluation donne lieu à différentes possibilités de traitement du risque. La norme ISO 27005 propose l'échelle suivante :[37]

Niveau	**Évaluation**	**Description**
Faible	Acceptable tel quel	Le risque peut être accepté sans autre action.
Modéré	Tolérable si maîtrisé	Il convient de réaliser un suivi en termes de gestion des risques et de mettre en place des actions dans le cadre de l'amélioration continue à moyen et long terme.
Élevé	Inacceptable	Il convient absolument que des mesures de réduction du risque soient prises à court terme. Dans le cas contraire, il convient que tout ou partie de l'activité soit refusé.

Tableau 4 : Échelle de niveau de risque selon la norme ISO 27005

Quant à la matrice d'appréciation du niveau de risque, elle reprend sur un de ses deux axes, les niveaux de gravité, et sur l'autre, les niveaux de vraisemblance. L'organisation détermine ensuite le niveau de risque correspondant pour chaque croisement. L'exemple de matrice d'appréciation du niveau de risque suivant est couramment utilisé en pratique :

Maximal	Modéré	Modéré	Élevé	Élevé
Important	Faible	Modéré	Élevé	Élevé
Limité	Faible	Faible	Modéré	Élevé
Négligeable	Faible	Faible	Modéré	Modéré
Gravité / Vraisemblance	Invraisemblable	Peu vraisemblable	Vraisemblable	Quasi certain

Tableau 5 : Exemple de matrice d'appréciation du niveau de risque

En lieu et place de la matrice d'appréciation du niveau de risque, il est également possible d'utiliser des valeurs seuils en calculant de manière numérique le niveau de risque. Nous ne recommandons toutefois pas cette approche car elle s'avère nettement moins visuelle que la matrice d'appréciation du niveau de risque. La matrice permet de visualiser facilement la position des risques sur un plan quadrillé, facilitant ainsi l'identification des priorités. En revanche, l'approche numérique peut rendre plus complexe l'interprétation des résultats et, par conséquent, la prise de décision, surtout dans des environnements où la communication rapide des risques et des priorités est essentielle pour une gestion efficace.

[37] ISO 27005:2022, Sécurité de l'information, cybersécurité et protection de la vie privée — Préconisations pour la gestion des risques liés à la sécurité de l'information, annexe A, tableau 6.

D. Gestion des risques

I. Processus de gestion des risques

1. Présentation du processus de gestion des risques selon la norme ISO 31000

Au-delà de la seule appréciation du risque, la gestion des risques repose sur un **processus complet et itératif**. Le processus de gestion des risques tel que défini par la norme ISO 31000[38] repose sur la succession structurée des 3 étapes suivantes :

– l'établissement du contexte ;
– l'appréciation des risques ; et
– le traitement des risques.

L'étape relative à l'appréciation des risques est elle-même divisée en 3 sous-processus :

– l'identification des risques ;
– l'analyse des risques ; et
– l'évaluation des risques.

Parallèlement à cela, la norme ISO 31000 préconise les étapes transversales de communication et concertation, de surveillance et revue et d'enregistrement et d'élaboration de rapports.

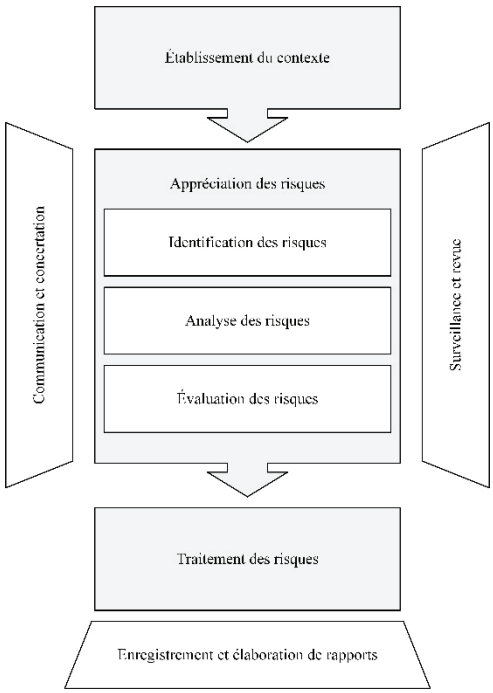

Figure 1 : Processus de gestion des risques basé sur la norme ISO 31000

38 ISO 31000:2018, Management du risque — Lignes directrices, art. 6.1.

2. Première étape : Établissement du contexte

L'établissement du contexte vise à obtenir une vue d'ensemble du contexte interne et externe dans lequel se situe l'objet de l'étude, par exemple une activité de traitement. Pour identifier les risques de manière pertinente, il est important que l'organisation comprenne de manière suffisamment détaillée les circonstances dans lesquelles elle opère.

Le **contexte interne** peut inclure, sans s'y limiter, la mission de l'organisation, ses valeurs, ses objectifs, sa stratégie, mais aussi son fonctionnement, sa gouvernance et sa structure organisationnelle.[39]

Le **contexte externe** inclut les facteurs qui influencent l'environnement dans lequel l'organisation évolue. Ces facteurs peuvent être variés et comprennent notamment les aspects réglementaires, légaux, technologiques, économiques, socioculturels et géopolitiques.[40] L'analyse du contexte externe doit également intégrer les relations avec les parties prenantes externes, telles que les clients, les fournisseurs, les partenaires commerciaux et les autorités.[41]

3. Deuxième étape : Appréciation des risques

a) Identification des risques

L'identification des risques vise à rechercher, reconnaître et décrire les risques qui pèsent sur les axes de protection de l'objet de l'étude en tenant compte des besoins de protection.

Il existe un grand nombre de techniques pour identifier les risques selon le contexte de l'étude. En matière de sécurité de l'information, la norme ISO 27005 préconise deux approches pour identifier les risques :[42]

- **l'approche basée sur les événements** qui vise à identifier des scénarios de niveau stratégique en tenant compte des sources de risque et de comment ils utilisent ou impactent les parties prenantes pour atteindre l'objectif souhaité de ce risque ; et
- **l'approche basée sur les biens** qui vise à identifier des scénarios de niveau opérationnels en tenant compte des biens, des menaces et des vulnérabilités.

b) Analyse des risques

L'analyse des risques vise à déterminer le niveau de risque de chaque risque en appréciant leur gravité et leur vraisemblance au moyen des échelles évoquées.

---

39 ISO 31000:2018, Management du risque — Lignes directrices, art. 5.4.1.
40 ISO 31000:2018, Management du risque — Lignes directrices, art. 5.4.1.
41 ISO 31000:2018, Management du risque — Lignes directrices, art. 5.4.1.
42 ISO 27005:2022, Sécurité de l'information, cybersécurité et protection de la vie privée — Préconisations pour la gestion des risques liés à la sécurité de l'information, art. 7.2.1.

c) Évaluation des risques

L'appréciation des risques implique d'évaluer chaque risque en fonction de son niveau de risque afin de déterminer si celui-ci est acceptable, tolérable ou inacceptable. Cette sous-étape permet de prioriser les risques en vue de leur traitement.

4. Troisième étape : Traitement des risques

La dernière étape du processus de gestion des risques concerne le **traitement des risques** qui ne sont pas jugés acceptables en l'état. La norme ISO 27005 mentionne les 4 options de traitement des risques suivants :[43]

- le **refus du risque**, qui consiste à décider de ne pas commencer ou poursuivre l'activité porteuse du risque ;
- la **modification du risque** (ou **mitigation du risque**), qui consiste à réduire le risque à un niveau acceptable ou tolérable au moyen de mesures ;
- la **prise de risque** (ou **acceptation du risque**), qui consiste par un choix éclairé d'accepter un risque ; ou
- le **partage du risque**, qui consiste à répartir les responsabilités entre différentes parties.[44]

La modification du risque implique de mettre en œuvre des mesures qui exerceront une influence sur sa gravité ou sa vraisemblance de manière à en réduire le niveau. La formation du personnel réduira par exemple la vraisemblance d'un risque de transmission de données non autorisé par erreur.

Lorsque des mesures sont utilisées pour mitiger un risque, il convient de procéder à une nouvelle appréciation du risque afin de déterminer le niveau de « **risque résiduel** » et de procéder à une nouvelle évaluation.[45] Si le risque n'a pas atteint un niveau de risque résiduel acceptable ou tolérable, une nouvelle option de traitement du risque doit être choisie. Ce mécanisme peut être illustré en matière de protection des données par l'AIPD, qui peut conduire le responsable du traitement à refuser un risque s'il n'est pas possible de le réduire à un niveau acceptable ou tolérable, l'empêchant de mettre en œuvre l'activité de traitement en question.

II. Défis

La gestion des risques constitue un enjeu majeur pour les organisations, indépendamment de leur taille ou leur secteur d'activité. Dans un environnement en constante évolution, où les menaces numériques, légales et opérationnelles se multiplient, la capacité à identifier, apprécier et traiter les risques devient cruciale. Cependant, cette démarche soulève de nombreux défis.

---

43 ISO 27005:2022, Sécurité de l'information, cybersécurité et protection de la vie privée — Préconisations pour la gestion des risques liés à la sécurité de l'information, art. 8.2.

44 P. ex. par la conclusion d'une assurance. L'option de traitement du risque consistant à le partager est généralement inapplicable dans un contexte de protection des données, dans la mesure où la responsabilité incombe avant tout au responsable du traitement.

45 ISO 31000:2018, Management du risque — Lignes directrices, art. 6.5.1

L'un des premiers défis de la gestion des risques est la nécessité pour les organisations de **définir des échelles adaptées à leurs propres besoins et contextes**. Ces échelles, telles que celles relatives à la confidentialité, la disponibilité ou l'intégrité des données, jouent un rôle crucial dans l'évaluation des risques. Chaque organisation possède une appétence aux risques qui lui est propre, influencée par sa culture, sa taille, ses objectifs et son secteur d'activité.[46] Par exemple, une *start-up* pourrait être plus tolérante aux risques que ne le serait une administration publique. Il devient alors essentiel de définir des échelles cohérentes qui permettent à l'organisation de s'approprier la démarche de gestion des risques tout en l'intégrant de manière fluide à ses activités.

Un deuxième défi réside dans la **subjectivité inhérente** à l'appréciation des risques, particulièrement en raison des biais cognitifs. Lorsqu'il s'agit d'évaluer des risques, même avec des échelles bien définies, les biais cognitifs peuvent influencer les jugements de manière significative. Le biais de disponibilité, par exemple, peut amener un évaluateur à surestimer certains risques simplement parce qu'ils sont récents ou marquants dans sa mémoire. De même, le biais de confirmation peut conduire à interpréter les données de manière à confirmer des croyances ou des hypothèses préexistantes, réduisant ainsi l'objectivité du processus. Cette subjectivité rend la tâche complexe et peut entraîner des évaluations peu fiables, souvent réalisées « **au pouce levé** » ou « **à la louche** », c'est-à-dire sans bases solides ou avec une trop grande approximation. Pour atténuer ces biais, nous recommandons l'utilisation d'échelles avec un nombre pair de niveaux, car cela oblige l'évaluateur à prendre position, évitant ainsi le choix par défaut d'une valeur moyenne en cas d'incertitude. Cette approche, bien qu'utile, ne garantit pas l'objectivité totale, mais elle permet de limiter les jugements instinctifs et mal fondés.

Un troisième défi en matière de gestion des risques concerne les **exigences légales** qui peuvent exister, particulièrement en ce qui a trait à la protection des données. La LPD impose en effet des obligations dans certaines circonstances, notamment en cas de risques élevés pour la personnalité ou les droits fondamentaux des personnes concernées. Cependant, la LPD laisse une marge d'appréciation aux organisations pour déterminer si un risque est suffisamment élevé pour déclencher des mesures spécifiques, comme la réalisation AIPD ou la notification au PFPDT d'une violation de la sécurité des données. Ce caractère indéterminé ouvre un vaste champ d'interprétation, tant pour les organisations que pour les autorités de surveillance. Si cette flexibilité permet une adaptation aux contextes variés, elle ajoute également une complexité supplémentaire à la gestion des risques. En l'absence de critères précis pour déterminer quand ces obligations s'appliquent, les organisations peuvent être confrontées à des divergences dans l'interprétation de la loi, créant ainsi des zones d'incertitude dans la mise en œuvre des mesures. En outre, la **conformité aux réglementations internationales** vient compliquer encore davantage la gestion des risques pour les organisations opérant à l'échelle mondiale. Chaque juridiction peut imposer des obligations différentes en matière de protection des données. Ces variations législatives exigent des organisations qu'elles

[46] ISO 27005:2022, Sécurité de l'information, cybersécurité et protection de la vie privée — Préconisations pour la gestion des risques liés à la sécurité de l'information, art. 6.4.2

ajustent leurs pratiques et leurs politiques pour respecter les réglementations locales tout en maintenant une cohérence globale.

Un quatrième défi auquel les organisations sont confrontées en matière de gestion des risques est **l'évolution rapide et constante des menaces**. Les cyberattaques et les techniques utilisées par les acteurs malveillants se perfectionnent en permanence, rendant obsolètes certaines mesures de sécurité si elles ne sont pas régulièrement mises à jour. Les organisations doivent ainsi faire face à de nouvelles vulnérabilités qui émergent à mesure que la technologie progresse, et cela exige une adaptation continue des stratégies de gestion des risques. Cela nécessite également de mettre en place des techniques de veille proactives pour surveiller les nouvelles menaces et vulnérabilités.

Un cinquième défi de la gestion des risques réside dans la **complexité technologique**. L'adoption de nouvelles technologies telles que l'intelligence artificielle, le *cloud computing* et la *blockchain* complexifie les environnements technologiques des organisations. Chacune de ces technologies introduit ses propres menaces et nécessite des approches spécifiques pour la gestion des risques. Les organisations doivent non seulement comprendre les technologies qu'elles adoptent, mais aussi anticiper les nouvelles menaces qu'elles pourraient introduire.

Le **manque de ressources humaines, techniques et financières** représente un sixième défi pour de nombreuses organisations, en particulier les petites et moyennes entreprises. Mettre en place une gestion des risques efficace nécessite des ressources spécialisées et du personnel formé, ce qui peut être un luxe pour certaines organisations. Le manque d'expertise interne en matière de gestion des risques et de protection des données complique encore la situation. En l'absence de compétences spécialisées, les organisations peuvent être tentées de sous-évaluer les risques ou de ne pas mettre en place les mesures de sécurité adéquates. Externaliser certaines fonctions de sécurité peut être une solution, mais elle exige également une gestion efficace des prestataires et partenaires.

Le septième défi, et peut-être l'un des plus grands défis en matière de gestion des risques, et plus globalement en matière de sécurité, reste le **facteur humain**. Les collaborateurs sont souvent la première ligne de défense, mais aussi le point de vulnérabilité le plus exposé aux erreurs. Des erreurs comme cliquer sur des liens de *phishing*, utiliser des mots de passe faibles, ou ne pas respecter les procédures internes de sécurité peuvent compromettre tout un système. La sensibilisation et la formation continue des collaborateurs aux bonnes pratiques de sécurité sont donc essentielles. Toutefois, cette formation doit aller au-delà des simples procédures ; elle doit également cultiver une culture de la sécurité et de la protection des données, où chaque collaborateur comprend l'importance de son rôle. Assurer l'engagement des collaborateurs dans la gestion des risques nécessite des efforts de communication et des programmes de formation réguliers.

E. Méthodologies de gestion des risques (panorama non exhaustif)

Dans son approche du SMSI, la norme ISO 27001 indique qu'il convient d'aligner l'approche et la méthodologie de gestion des risques en matière de sécurité de l'information avec celle utilisée pour gérer les autres risques de l'organisation.[47] En cela, la norme ISO 27005 précise que la méthodologie choisie doit assurer :

- la cohérence des appréciations réalisées par plusieurs personnes ou par la même personne à différentes occasions ;
- la comparabilité des appréciations entre différents risques selon les critères déterminés ; et
- la validité des appréciations qui doivent être aussi proche de possible de la réalité.

Il existe ainsi une myriade de méthodologies de gestion des risques. Certaines sont spécifiques à un domaine particulier et d'autres sont plus génériques. Il est d'ailleurs important de préciser qu'il n'est pas impératif de se servir d'une méthodologie existante. Une organisation peut tout à fait développer sa propre méthodologie si cela s'avère plus pertinent dans son contexte, tout en tenant compte toutefois des lignes directrices de la norme ISO 31000.

Dans le cadre de la mise en œuvre d'un SMSI, la norme ISO 27001 prescrit notamment que l'organisation doit veiller à ce que la méthodologie qu'elle utilise réponde aux préconisations de la norme ISO 27005 (compatibilité à la norme). L'utilisation d'une méthodologie reconnue permet de s'assurer de la validité de la démarche.

Parmi les méthodologies couramment utilisées dans le domaine de la sécurité de l'information, nous pouvons citer les méthodologies OCTAVE, MEHARI ou encore EBIOS.

OCTAVE, qui signifie « *Operationally Critical Threat, Asset, and Vulnerability Evaluation* », est une méthodologie d'identification et d'évaluation des risques liés à la sécurité de l'information sur un plan opérationnel développé par le *Software Engineering Institute*. OCTAVE se compose de quatre variantes :

- OCTAVE Original, qui est conçue pour les grandes organisations disposant d'une structure organisationnelle complexe ;
- OCTAVE-S, qui est une version simplifiée pour les petites et moyennes organisations ;
- OCTAVE Allegro, qui est une version plus flexible orientée sur les informations critiques plutôt que sur les actifs technologiques ; et
- OCTAVE FORTE qui est une version destinée aux grandes organisations qui souhaitent aligner leur gestion des risques avec leurs objectifs stratégiques globaux.

47 ISO 27001:2022, Sécurité de l'information, cybersécurité et protection de la vie privée – Systèmes de management de la sécurité de l'information – Exigences, art. 6.1.2.

MEHARI, qui signifie « Méthode Harmonisée d'Analyse de Risques », est une méthodologie d'analyse de risques développée par l'Association française des professionnels de la sécurité de l'information (CLUSIF). Il s'agit d'une méthodologie modulaire basée sur un ensemble de guides, de grilles d'évaluation et de bases de connaissances adaptés à différents types d'organisations.

EBIOS, qui signifie « Expression des besoins et identification des objectifs de sécurité », est la méthodologie d'appréciation et de traitement des risques numériques publiée par l'ANSSI avec le soutien du Club EBIOS. Elle adopte une structure en cinq ateliers et met l'accent sur la compréhension des besoins et objectifs de sécurité spécifiques de l'organisation. Elle aide à définir clairement les niveaux de protection requis pour chaque actif, en fonction de la sensibilité de l'information et des risques associés. EBIOS utilise des scénarios pour illustrer comment les menaces peuvent exploiter des vulnérabilités pour nuire aux objectifs de l'organisation. Cela permet de mieux comprendre le contexte et les conséquences potentielles des incidents de sécurité et ainsi d'impliquer plus facilement des experts métiers dans le processus.

Dans cette diversité de méthodologies de gestion des risques, il est essentiel de sélectionner celle qui correspond le mieux aux besoins et spécificités de l'organisation. Alors que certaines méthodologies, comme OCTAVE ou MEHARI, se concentrent principalement sur des aspects opérationnels ou techniques, d'autres, comme EBIOS, permettent d'adopter une approche plus stratégique et adaptée aux besoins spécifiques de sécurité. Chaque organisation doit choisir sa méthodologie en fonction de ses objectifs et du contexte dans lequel elle opère. Cela étant dit, quelle que soit la méthodologie retenue, il reste impératif de s'assurer qu'elle est en cohérence avec les préconisations de gestion des risques, notamment celles fixées par la norme ISO 27005.

F. Proposition d'une méthodologie

I. Nécessité d'une méthodologie

La gestion du risque nécessite d'adopter et d'utiliser une méthodologie structurée et efficace. À cet égard, nous sommes d'avis que le recours à la méthodologie EBIOS Risk Manager est particulièrement intéressant, notamment en raison de sa capacité à être transposée au domaine de la protection des données, et en particulier à l'esprit de la LPD.

La méthodologie EBIOS Risk Manager propose un cadre flexible et itératif, qui s'adapte aux besoins spécifiques de chaque organisation et de chaque projet. En addition, et sous réserve de certaines adaptations, la combinaison de ses approches permet de couvrir l'ensemble des risques, et ce y compris en matière de protection des données.

La méthodologie EBIOS Risk Manager se distingue par l'appréciation des risques en combinant :[48]

[48] *ANSSI*, La méthode EBIOS Risk Manager — le Guide, 4.

– une **approche par conformité** pour déterminer le socle de sécurité pour les risques les plus communs, y compris ceux liés à des événements accidentels et environnementaux ; et
– une **approche par scénarios** utilisée pour identifier les risques avancés, d'origine intentionnelle, et notamment les attaques particulièrement ciblées ou sophistiquées.

La combinaison des deux approches permet ainsi de couvrir non seulement le principe de sécurité, qui forme le socle de sécurité de toute organisation, mais aussi de traiter les risques les plus élevés ou complexes.

En intégrant ces éléments dans une approche structurée et conforme aux exigences de la LPD, les organisations peuvent s'assurer qu'elles répondent aux obligations légales tout en optimisant leur stratégie de gestion des risques et de conformité globale.

II. Approche par conformité

1. Applicabilité

L'approche par conformité de la méthodologie EBIOS Risk Manager, consiste à déterminer le **socle de sécurité nécessaire pour se prémunir contre les risques les plus courants**. L'approche par conformité s'applique par conséquent davantage à **l'ensemble de l'organisation** plutôt qu'à une **activité de traitement spécifique**. En identifiant et en se préparant à ces types de risques, l'approche par conformité permet aux organisations de mettre en place des mesures de sécurité de base, formant ainsi un socle solide sur lequel elles peuvent bâtir une stratégie de gestion des risques pertinente et efficace.

Appliquée au domaine de la protection des données, cette approche vise à s'assurer du respect du principe de sécurité, en s'assurant que toutes les mesures organisationnelles et techniques adaptées sont en place pour protéger les données en garantissant un niveau adéquat de leurs axes de protection.

2. Socle de sécurité

a) Socle de sécurité

Le socle de sécurité représente l'ensemble des mesures de base destinées à protéger les données contre les risques non délibérés ou non ciblés qui ne nécessitent pas une analyse approfondie conformément à l'approche par scénarios.

Ces risques comprennent les **risques accidentels**, tels que les erreurs humaines lors du traitement des données ou la perte de données causée par une mauvaise opération de maintenance, comme le remplacement d'un support de stockage. Ils comprennent également les **risques environnementaux**, tels que les incendies ou les inondations qui pourraient compromettre l'intégrité physique des systèmes de stockage de données.

Les mesures qui composent le socle de sécurité proviennent principalement de législations dont l'application est obligatoire, ainsi que de normes internationales

qui proposent de larges référentiels. En matière de protection des données, et plus largement de sécurité de l'information, le socle de sécurité doit être envisagé sous le prisme du principe de sécurité inscrit au sein de la LPD et détaillé par l'OPDo, ainsi que des normes ISO 27001 et ISO 27701.

b) Socle de sécurité selon la LPD et l'OPDo

Le principe de sécurité implique que les responsables du traitement et les sous-traitants doivent assurer, par des mesures organisationnelles et techniques appropriées, une sécurité adéquate des données par rapport au risque encouru (art. 8 al. 1 LPD).[49]

Les mesures organisationnelles et techniques représentent le socle de sécurité minimale que chaque responsable de traitement et sous-traitant doit mettre en place sous le prisme de la protection des données. Elles doivent permettre, conformément à l'art. 2 OPDo, de garantir que les données traitées ne soient accessibles qu'aux personnes autorisées (confidentialité), soient disponibles en cas de besoin (disponibilité), ne puissent être modifiées sans droit ou par mégarde (intégrité) et soient traitées de manière à être traçables (traçabilité).

L'art. 1 OPDo établit les bases pour la mise en œuvre du principe de sécurité, en déterminant les critères à prendre en compte pour évaluer le besoin de protection (art. 1 al. 2 OPDo) et le risque pour la personnalité ou les droits fondamentaux de la personne concernée (art. 1 al. 3 OPDo). Le besoin de protection des données est évalué en fonction du type de données traitées, ainsi que de la finalité, de la nature, de l'étendue et des circonstances du traitement. En ce qui concerne le risque pour la personnalité ou les droits fondamentaux de la personne concernée, celui-ci est pour sa part analysé sur la base de critères tels que les causes du risque, les principales menaces, les mesures prévues pour réduire le risque, et la probabilité ainsi que la gravité d'une éventuelle violation de la sécurité des données, même après la mise en place des mesures de protection. À ceci s'ajoute le fait que, lors de la détermination des mesures à adopter, des éléments comme l'état des connaissances et les coûts de mise en œuvre doivent également pris en compte (art. 1 al. 4 OPDo). Il est enfin précisé que le processus doit être continu, avec une réévaluation régulière du besoin de protection, du risque encouru, et des mesures mises en place (art. 1 al. 5 OPDo).

L'art. 3 OPDo détaille une série de mesures techniques et organisationnelles que les responsables du traitement et les sous-traitants peuvent mettre en œuvre pour assurer une sécurité appropriée des données.

Pour chaque axe de protection – la confidentialité, l'intégrité, la disponibilité, et la traçabilité des données – l'art. 3 OPDo propose une liste de mesures.

Confidentialité	**Objectif de la mesure**
Contrôle de l'accès aux données	Seules les personnes autorisées doivent avoir accès aux données personnelles dont elles ont besoin pour accomplir leurs tâches.

[49] Il est en outre précisé que ces mesures doivent notamment permettre d'éviter toute violation de la sécurité des données (art. 8 al. 2 LPD).

Contrôle de l'accès aux locaux et aux installations	Seules les personnes autorisées doivent pouvoir accéder aux locaux et aux installations utilisés pour le traitement de données.
Contrôle d'utilisation	Seules les personnes autorisées doivent pouvoir utiliser les systèmes de traitement automatisé de données personnelles à l'aide d'installations de transmissions.

Tableau 6 : Mesures pour assurer la confidentialité selon l'art. 3 al. 1 OPDo

Disponibilité et intégrité	**Objectif de la mesure**
Contrôle des supports de données	Seules les personnes autorisées doivent pouvoir lire, copier, modifier, déplacer, effacer ou détruire des supports de données.
Contrôle de la mémoire	Seules les personnes autorisées doivent pouvoir enregistrer, lire, modifier, effacer ou détruire des données personnelles dans la mémoire.
Contrôle du transport	Seules les personnes autorisées doivent pouvoir lire, copier, modifier, effacer ou détruire des données personnelles lors de leur communication ou lors du transport de supports de données.
Restauration	La disponibilité et l'accès aux données personnelles doivent pouvoir être rapidement restaurés en cas d'incident physique ou technique.
Disponibilité	Les fonctions du système de traitement automatisé de données personnelles doivent être disponibles.
Fiabilité	Les dysfonctionnements du système de traitement automatisé de données personnelles doivent pouvoir être signalés.
Intégrité des données	Les données personnelles stockées dans le système de traitement automatisé de données personnelles ne doivent pas pouvoir être endommagées en cas de dysfonctionnements.
Sécurité du système	Les systèmes d'exploitation et les logiciels d'application doivent toujours être maintenus à jour en matière de sécurité et les failles critiques connues doivent être corrigées.

Tableau 7 : Mesures pour assurer la disponibilité et l'intégrité selon l'art. 3 al. 2 OPDo

Traçabilité	**Objectif de la mesure**
Contrôle de la saisie	Il doit être possible de vérifier quelles données personnelles sont saisies ou modifiées dans le système de traitement automatisé de données, par quelle personne et à quel moment.
Contrôle de la communication	Il doit être possible de vérifier à qui sont communiquées les données personnelles à l'aide d'installations de transmission.
Détection	Les violations de la sécurité des données doivent pouvoir être rapidement détectées.
Réparation	Les mesures prises en relation avec les violations de la sécurité des données doivent pouvoir atténuer ou éliminer les conséquences.

Tableau 8 : Mesures pour assurer la traçabilité selon l'art. 3 al. 3 OPDo

Les mesures techniques et organisationnelles prévues par la LPD et l'OPDo laissent une certaine flexibilité aux responsables du traitement et aux sous-traitants dans leur mise en œuvre, leur permettant d'adopter des solutions appropriées selon, par exemple, la taille de leur organisation.

c) Socle de sécurité selon la norme ISO 27001

La norme ISO 27001 dépasse largement le cadre de la simple protection des données pour couvrir l'ensemble des enjeux liés à la gestion de la sécurité de l'information, et ce par le biais de l'établissement d'un SMSI. Ce dernier englobe toutes les mesures et contrôles nécessaires pour protéger les actifs informationnels d'une organisation. Par actif organisationnel, il faut comprendre toutes les données qui ont de la valeur pour l'organisation, comme les données stratégiques, les données personnelles, les secrets de fabrication ou les secrets d'affaires.

La norme ISO 27001 propose, dans son annexe A, un **catalogue de 93 mesures de sécurité** destinées à protéger la confidentialité, l'intégrité et la disponibilité des actifs informationnels.[50] Ce catalogue constitue le socle de sécurité selon la norme ISO 27001.

Le catalogue de mesures est cependant plus étendu dans la mesure où il propose une répartition des mesures de sécurité qui couvre une variété de scénarios plus larges. Les mesures prévues sont ainsi catégorisées pour répondre aux différents besoins de la sécurité de l'information, à savoir :

- les mesures de sécurité applicables aux personnes ;[51]
- les mesures de sécurité physique ;[52]
- les mesures de sécurité technologiques ;[53] et

---

50 ISO 27001:2022, Sécurité de l'information, cybersécurité et protection de la vie privée — Systèmes de management de la sécurité de l'information — Exigences, annexe A.

51 Les mesures de sécurité applicables aux personnes impliquent par exemple de procéder aux vérifications des références de tous les candidats à l'embauche avant qu'ils n'intègrent l'organisation (A.6.1 — Sélection des candidats), d'indiquer les responsabilités du personnel et de l'organisation en matière de sécurité de l'information au sein des contrats de travail (A.6.2 — Termes et conditions du contrat de travail), de sensibiliser le personnel et les parties intéressées pertinentes (A.6.3 — Sensibilisation, enseignement et formation en sécurité de l'information) ou de mettre en place un processus disciplinaire permettant de prendre des mesures à l'encontre du personnel et d'autres parties intéressées qui ont commis une violation de la politique de sécurité de l'information (A.6.4 — Processus disciplinaire).

52 Les mesures de sécurité organisationnelles impliquent par exemple de définir des périmètres de sécurité pour protéger les zones qui contiennent les actifs informationnels (A.7.1 — Périmètres de sécurité physique), de protéger par des mesures de sécurité les accès et les points d'accès appropriés (A.7.2 — Entrées physiques) ou d'établir des règles du bureau vide et des règles de l'écran vide (A.7.7 — Bureau propre et écran vide).

53 Les mesures de sécurité technologiques impliquent par exemple de protéger les terminaux utilisateurs (A.8.1 — Terminaux utilisateurs), de limiter et de gérer l'attribution et l'utilisation des droits d'accès privilégiés (A.8.2 — Droits d'accès privilégiés), de mettre en œuvre des technologies et procédures d'authentification sécurisées (A.8.5 — Authentification sécurisée) ou de mettre en œuvre une protection contre les programmes malveillants (A.8.7 — Protection contre les programmes malveillants).

– les mesures de sécurité organisationnelles.[54]

Lorsqu'une organisation souhaite certifier son SMSI selon la norme ISO 27001, elle doit évaluer l'applicabilité de l'ensemble des mesures en relation avec son plan de traitement des risques.[55] En pratique, de nombreuses organisations de petite et moyenne taille se réfèrent aux mesures sans toutefois chercher à obtenir une certification de leur SMSI.

Nous soulignons également que la norme ISO 27701 ajoute et modifie certaines mesures dans la perspective de son extension au SMSI, en les adaptant au contexte spécifique d'un PIMS. La norme ISO 29151 fournit également des recommandations sur un large éventail de mesures de sécurité de l'information et de protection des données personnelles.[56] L'ensemble de ces normes constitue ainsi un référentiel particulièrement large pour constituer le socle de sécurité.

3. Analyse générale

L'approche par conformité doit être réalisée de manière générale à l'organisation, et non à une activité de traitement spécifique. Cette analyse générale permet notamment d'évaluer si le socle de sécurité est suffisant. En même temps, elle aide à identifier les éléments qui nécessitent une analyse plus détaillée à travers l'approche par scénarios.

L'approche par conformité implique notamment pour l'organisation d'avoir une compréhension détaillée de ses systèmes d'information, de ses activités de traitement et de leur contexte. À cet égard, le registre des activités de traitement constitue un élément central permettant d'obtenir un niveau de compréhension suffisant. En pratique, nous recommandons de commencer par l'identification des outils, logiciels et plateforme en ligne utilisés par l'organisation.[57] Cette étape facilite l'identification des acteurs impliqués dans les activités de traitements tels que les éditeurs de logiciels, les hébergeurs de données, ainsi que les autres sous-traitants ou responsables du traitement tiers. Elle facilite également l'identification des ensembles de données personnelles traitées.

---

54 Les mesures de sécurité organisationnelles impliquent par exemple de l'établissement d'une politique de sécurité de l'information (A.5.1 — Politiques de sécurité de l'information), de s'assurer que le personnel et les autres parties intéressées restituent tous les actifs informationnels de l'organisation (A.5.11 — Restitution des actifs), de classifier les actifs informationnels conformément aux besoins de sécurité de l'information de l'organisation (A.5.12 — Classification des informations) ou de contrôler les accès physiques et logiques aux actifs informationnels (A.5.15 — Contrôle d'accès).

55 ISO 27001:2022, Sécurité de l'information, cybersécurité et protection de la vie privée – Systèmes de management de la sécurité de l'information – Exigences, art. 6.1.3.

56 ISO 29151:2017, Technologies de l'information — Techniques de sécurité — Code de bonne pratique pour la protection des données à caractère personnel, Introduction.

57 Il peut s'agir d'un progiciel de gestion (ERP), d'une plateforme en ligne de gestion de la relation client (*Customer Relationship management,* CRM) en ligne, d'un outil en ligne de gestion des salaires ou de l'horaire de travail.

Dans le cadre de l'analyse générale, il est donc essentiel de considérer les données personnelles **sous forme d'ensembles plutôt que de les segmenter individuellement**, comme on pourrait le faire dans le registre des activités de traitement. Prenons l'exemple d'un progiciel de gestion qui regroupe différentes catégories de données personnelles. Un module « ressources humaines » pourrait traiter les données du personnel, tandis qu'un module « ventes » serait dédié aux données des clients. Bien que ces ensembles de données soient différenciés par la catégorie de personnes concernées, l'analyse générale vise à considérer la totalité des données du progiciel comme un tout. En effet, une atteinte à un axe de protection aurait probablement un impact sur l'ensemble des données, et non uniquement sur celles liées à une catégorie spécifique. Cette approche holistique permet de mieux comprendre les risques globaux qui pèsent sur les systèmes d'information et de mettre en place des mesures de sécurité adaptées.

En pratique, la cartographie de l'écosystème de l'organisation, comprenant les parties prenantes externes, les outils et les ensembles de données personnelles, se fait au moyen de schémas visuels permettant d'impliquer les différents métiers. Leur implication permet de s'assurer du caractère exhaustif de la cartographie en tenant compte des aspects opérationnels de l'organisation.

Pour transposer la méthodologie EBIOS Risk Manager au domaine de la protection des données, il est nécessaire de s'adapter à son langage spécifique afin de le rendre pertinent pour cette application.

Ainsi, dans la suite de cet article, nous désignerons les ensembles de données personnelles sous le terme de « **valeur métier** ». Ce terme fait référence à un élément essentiel pour l'organisation dans l'accomplissement de sa mission qui nécessite d'être protégé.[58] Il peut s'agir d'un service, d'une fonction de support, d'informations stratégiques ou d'un savoir-faire associé. Il appartient à l'organisation de déterminer le besoin de protection pour chacune des valeurs métiers.

Une autre notion clé à intégrer est celle de « **bien support** ». Cette notion se définit comme une composante du système d'information sur laquelle repose une ou plusieurs valeurs métier.[59] Un bien support peut être de différentes natures : physique,[60] organisationnelle[61] ou numérique.[62]

Pour reprendre l'exemple du progiciel de gestion, l'ensemble de données constitue la valeur métier et le serveur sur lequel se situe le progiciel en question constitue un des biens supports. Celui-ci peut tout aussi bien être interne à l'organisation qu'externe, ce qui n'influence en rien l'analyse à ce stade. Ainsi, le besoin de protection de la valeur métier peut être reporté sur les biens supports qui lui sont associés.

Si plusieurs valeurs métiers reposent sur un même bien support, le besoin de protection le plus élevé doit être retenu. Il faut dans ce cas imaginer un serveur qui

58 *ANSSI*, La méthode EBIOS Risk Manager — le Guide, 4.

59 *ANSSI*, La méthode EBIOS Risk Manager — le Guide, 86.

60 P. ex. un serveur physique, un local technique ou un dispositif de vidéoprotection.

61 P. ex. un département des ressources humaines, un administrateur système ou une équipe de projet.

62 P. ex. un réseau de téléphonie, une passerelle d'interconnexion ou un serveur virtuel.

héberge le progiciel de gestion ainsi qu'un outil de newsletter. Les données concernant la newsletter n'ont pas le même besoin de protection que les données du progiciel de gestion. Le serveur nécessite dès lors une protection en relation avec le besoin de protection du progiciel de gestion dont les exigences sont plus élevées.

Il est ainsi pertinent d'identifier les mesures provenant de référentiels qui contribuent au besoin de protection. Cette approche permet de justifier d'une part, l'application de certaines mesures et, d'autre part, de justifier l'absence de mise en œuvre d'autres mesures. À titre de comparaison, dans une démarche de système de management de la sécurité de l'information selon la norme ISO 27001, on parle de « déclaration d'applicabilité » qui consiste à justifier la mise en œuvre et l'absence de mise en œuvre des mesures de l'annexe A de ladite norme.

L'organisation peut ainsi évaluer l'état de mise en œuvre des mesures[63] qu'elle a identifié comme pertinent et, le cas échéant, élaborer un plan d'action.

4. Surveillance et revue

Le socle de sécurité doit être **surveillé** et **régulièrement réévalué**, car de nombreux composants de l'écosystème de l'organisation évoluent, tout comme les sources de risque qui y sont associées. La pandémie de COVID-19 en est un exemple frappant : de nombreuses organisations n'avaient pas jugé pertinent d'intégrer le risque pandémique dans leur gestion des risques. Cependant, face aux conséquences majeures de cette crise, elles ont dû revoir leurs stratégies. De même, le réchauffement climatique entraîne des phénomènes météorologiques de plus en plus fréquents et violents, ce qui oblige les organisations à en tenir compte, notamment pour protéger leurs biens supports, comme leurs serveurs. Ces évolutions montrent l'importance d'une gestion des risques adaptable et proactive.

Le processus de surveillance et de révision du socle de sécurité doit permettre à l'organisation de s'assurer que les mesures en place restent pertinentes face aux risques identifiés et qu'elles sont à la fois efficaces et économiquement viables, tant dans leur conception que dans leur fonctionnement.[64] Il est également crucial d'inclure dans cette révision les incidents passés, qu'ils aient été des succès ou des échecs, afin de tirer des leçons et d'alimenter une amélioration continue du socle de sécurité. De plus, il est essentiel d'anticiper et d'identifier suffisamment tôt les risques émergents susceptibles d'affecter ce socle, pour garantir qu'il continue de fournir un niveau de protection adéquat. Dans cette optique, nous recommandons une révision annuelle du socle de sécurité afin de maintenir sa pertinence et son efficacité.

---

63 Il est possible d'évaluer les mesures comme « non mise en œuvre », « partiellement mise en œuvre » ou « totalement mise en œuvre ».

64 ISO 27005:2022, Sécurité de l'information, cybersécurité et protection de la vie privée — Préconisations pour la gestion des risques liés à la sécurité de l'information, art. 10.5.1.

III. Approche par scénarios

1. Applicabilité

L'approche par scénarios de la méthodologie EBIOS Risk Manager, appliquée au domaine de la protection des données, est conçue pour traiter les risques plus avancés d'origine intentionnelle et les risques potentiellement élevés ou particulièrement complexes à aborder. Tout ou partie de l'approche peut ainsi s'appliquer de manière pertinente à l'AIPD, au profilage à risque élevé ainsi qu'à l'analyse des violations de la sécurité des données.

Seules les grandes lignes de l'approche par scénarios seront présentées, car chaque contexte nécessite une analyse détaillée et adaptée. Il serait impraticable de détailler l'approche par scénarios pour chaque obligation spécifique de la LPD, d'autant plus que ces obligations ne s'appliquent pas de manière systématique.[65] Contrairement au principe de sécurité, qui doit toujours être respecté, certaines obligations, comme l'AIPD, ne se déclenchent que sous certaines conditions. Par conséquent, une approche standardisée pour tous les cas ne serait pas appropriée, et il est nécessaire d'adapter l'analyse des scénarios en fonction du risque propre à chaque situation. Néanmoins, il est essentiel de suivre la structure de l'approche par scénarios, telle que définie dans la méthodologie EBIOS Risk Manager, afin de garantir une évaluation cohérente des risques dans chaque contexte spécifique.

2. Structure de l'approche

La méthodologie EBIOS Risk Manager s'articule autour de 5 ateliers :

- le premier atelier, qui traite du cadrage de l'étude et du socle de sécurité ;
- le deuxième atelier, qui traite des sources de risque ;
- le troisième atelier, qui traite des scénarios stratégiques ;
- le quatrième atelier, qui traite des scénarios opérationnels ; et
- le cinquième atelier, qui traite du traitement du risque.

L'approche par conformité précédemment abordée se retrouve au sein du premier et cinquième atelier. L'approche par scénarios se déroule, quant à elle, sur la totalité des 5 ateliers.[66]

---

65 Par exemple, l'AIPD vise à déterminer en amont si un traitement de données envisagé comporte un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée. Ici, l'analyse du risque est focalisée sur le traitement en question avant sa mise en œuvre, permettant d'anticiper les impacts possibles. En revanche, pour le profilage à risque élevé, l'analyse du risque se concentre sur les données utilisées pour établir des profils et les résultats potentiels qui peuvent en découler. Enfin, l'annonce des violations de la sécurité des données cherche à protéger les personnes concernées après qu'une violation se soit produite, en se concentrant sur les données qui ont été compromises et les conséquences potentielles de cette violation.

66 *ANSSI*, La méthode EBIOS Risk Manager — le Guide, 6.

a) Atelier 1 : Cadrage de l'étude

Le premier atelier a pour objectif de définir clairement ce que l'organisation souhaite protéger, en établissant un **cadre précis**. L'approche par scénarios se focalise sur des éléments ciblés, tels qu'une activité de traitement spécifique. Si le cadrage de l'analyse est trop étendu, cela risque de la rendre excessivement complexe et longue à réaliser, diminuant ainsi son efficacité et sa pertinence.[67]

Les questions suivantes permettent d'établir le contexte de manière suffisamment détaillée, permettant ainsi l'identification des valeurs métiers et des biens supports :

- À quoi sert l'activité de traitement ?
- Quelles sont les finalités et les raisons d'être de l'activité de traitement ?
- Quelles sont les données traitées pour atteindre ces finalités ?
- Quels sont les outils, les sous-traitants, les ressources humaines, les infrastructures physiques, etc., impliqués ?

Pour chaque valeur métier, l'organisation doit déterminer le besoin de protection. Pour ce faire, les échelles suivantes peuvent être utilisées.

Niveau de confidentialité	**Description**
Public	La valeur métier est publique.
Limité	La valeur métier ne doit être accessible qu'au personnel et aux partenaires.
Réservé	La valeur métier ne doit être accessible qu'au personnel (interne) impliqué.
Confidentiel	La valeur métier ne doit être accessible qu'à des personnes identifiées et ayant le besoin d'en connaître.

Tableau 9 : Exemple d'échelle de besoin de confidentialité

Niveau de disponibilité	**Description**
Faible	La valeur métier peut être indisponible plus d'une semaine.
Modéré	La valeur métier doit être disponible dans les 7 jours.
Élevé	La valeur métier doit être disponible dans les 3 jours.
Critique	La valeur métier doit être disponible dans les 24 heures.

Tableau 10 : Exemple d'échelle de besoin de disponibilité

Niveau d'intégrité	**Description**
Détectable	La valeur métier peut ne pas être intègre si l'altération est identifiée.
Maîtrisé	La valeur métier peut ne pas être intègre si l'altération est identifiée et l'intégrité de la valeur métier retrouvée.
Intègre	La valeur métier doit être rigoureusement intègre.

Tableau 11 : Exemple d'échelle de besoin d'intégrité

[67] Afin d'éviter que l'analyse ne soit trop étendue, il est conseillé de se limiter à 10 valeurs métiers.

La suite du premier atelier vise à **identifier les événements redoutés** et à les caractériser d'un point de vue des impacts sur la personnalité et les droits fondamentaux des personnes concernées. Les événements redoutés traduisent une altération d'un ou plusieurs axes de protection sur la valeur métier dépassant le besoin de protection. En pratique, les événements redoutés sont décrits sous la forme d'une expression courte permettant une compréhension facile.[68]

Sur la base des événements redoutés, l'organisation peut estimer de manière relativement concrète les impacts sur la personnalité et les droits fondamentaux des personnes concernées afin d'en faire émerger une appréciation de gravité. Le tableau suivant présente plusieurs exemples d'impacts avec, pour chacun, leur niveau de gravité :

Impact	**Niveau de gravité**
Perte de temps pour réitérer des démarches ou pour attendre de les réaliser	Négligeable
Réception de courriers non sollicités (p. ex. spams)	Négligeable
Publicité ciblée pour des produits de consommation courants	Négligeable
Simple contrariété par rapport à l'information reçue ou demandée	Négligeable
Refus d'accès à des services administratifs ou prestations commerciales	Limité
Opportunités de confort perdues (p. ex. annulation de loisirs, d'achats, de vacances, fermeture d'un compte en ligne)	Limité
Données non mises à jour (p. ex. emploi antérieurement occupé)	Limité
Difficultés financières non temporaires (p. ex. obligation de contracter un prêt)	Important
Perte financière à la suite d'une escroquerie (p. ex. après une tentative d'hameçonnage)	Important
Perte de données relatives à des clients	Important
Sentiment d'atteinte aux droits fondamentaux (p. ex. discrimination, liberté d'expression)	Important
Péril financier	Maximal
Perte de preuves dans le cadre d'un contentieux	Maximal
Sanction pénale	Maximal

Tableau 12 : Exemples d'impacts

La norme ISO 29134 qui traite spécifiquement de l'AIPD propose une approche simplifiée pour apprécier le niveau de gravité basé sur la nature des données traitées au moyen de l'échelle suivante :[69]

[68] *ANSSI*, La méthode EBIOS Risk Manager — le Guide, 25.

[69] ISO 29134:2023, Technologies de l'information — Techniques de sécurité — Lignes directrices pour l'étude d'impacts sur la vie privée, annexe A, tableau 1.

Nature des données personnelles	Niveau de gravité
Données personnelles publiquement accessibles (p. ex. dans des annuaires téléphoniques, des carnets d'adresses ou des listes de sélections)	Négligeable
Données personnelles qui exigent un intérêt légitime pour y accéder (p. ex. des fichiers publics à diffusion restreinte ou membres d'une liste de diffusion)	Limité
Données personnelles dont la divulgation non autorisée peut nuire à la réputation des personnes concernées (p. ex. des informations sur les revenus, sur les avantages sociaux ou sur l'impôt foncier)	Important
Données personnelles dont la divulgation, la modification, la perte ou la destruction non autorisée peut affecter l'existence ou la santé, la liberté et la vie de la personne concernée (p. ex. des informations concernant un engagement vis-à-vis d'une institution, une peine, des évaluations du personnel, des données de santé, des dettes irrécouvrables, ou si la personne concernée risque de devenir une victime dans une affaire criminelle)	Maximal

Tableau 13 : Échelle de niveau de gravité selon la nature des données traitées

b) Atelier 2 : Sources de risque

Le second atelier se focalise sur **l'identification des sources de risque** et **leurs objectifs visés**.[70] Le second atelier vise ainsi à répondre aux questions suivantes :

- Quelles sont les sources de risque susceptibles de porter atteinte aux valeurs métiers étudiées ?
- Quels peuvent être les objectifs visés par chaque source de risque en termes d'effets recherchés ?

La norme ISO 27005 propose une liste non exhaustive de sources de risques dans le cadre de cette approche :[71]

- les sources de risque étatique ;[72]
- le crime organisé ;[73]
- le cyberterrorisme ;
- les activistes idéologiques ;[74]
- les officines spécialisées ;
- les amateurs ;
- les vengeurs ; et
- les attaquants pathologiques ou opportunistes.

[70] L'approche par scénarios s'applique uniquement aux risques intentionnels dans ce contexte.

[71] ISO 27005:2022, Sécurité de l'information, cybersécurité et protection de la vie privée — Préconisations pour la gestion des risques liés à la sécurité de l'information, annexe A, tableau 7.

[72] P. ex. les agences de renseignement.

[73] P. ex. les organisations cybercriminelles.

[74] P. ex. les cyberhacktivistes ou les groupements d'intérêts.

La norme ISO 27005 propose également une liste d'objectifs visés :[75]

- l'espionnage ou les opérations de renseignement ;
- le prépositionnement stratégique ;
- l'influence ;
- l'entrave au fonctionnement ;
- les opérations lucratives ; et
- le défi ou l'amusement.

Le second atelier consiste donc à évaluer la pertinence des couples formés par les sources de risque et leurs objectifs visés en tenant compte de leur motivation, de leurs ressources[76] et de leur niveau d'activité.[77]

L'Office fédéral de la cybersécurité (OFCS) propose un état de la menace qui fournit les informations nécessaires pour réaliser cette évaluation.[78] Il est à noter que la méthodologie EBIOS Risk Manager suggère de se limiter à 6 couples et de privilégier ceux qui sont suffisamment distincts les uns des autres.[79]

Dans la précédente version du guide de la méthodologie EBIOS Risk Manager, les profils des sources de risques étaient regroupés en trois catégories principales :[80]

- les organismes structurés, guidés par une logique d'efficacité et de profit, qui disposent de moyens sophistiqués et importants, voire pratiquement illimités (États, crime organisé) ;
- les organismes ou groupes guidés par une motivation idéologique qui disposent de moyens importants mis en œuvre de manière relativement coordonnée (terroristes, activistes) ; et
- les attaquants limités par des moyens spécialisés (individus isolés, groupes d'individus ou d'organismes).

En pratique, cette catégorisation peut s'avérer plus simple à appréhender et constitue ainsi une base intéressante dans le cadre d'une première itération de l'approche par scénarios.

c) Atelier 3 : Scénarios stratégiques

Le troisième atelier vise à **disposer d'une vision claire des parties prenantes** qui interagissent avec les valeurs métiers, comme les sous-traitants et leurs sous-traitants ultérieurs. La méthodologie EBIOS Risk Manager considère particulièrement les parties prenantes externes en partant du constat que de plus en plus de modes

---

75 ISO 27005:2022, Sécurité de l'information, cybersécurité et protection de la vie privée — Préconisations pour la gestion des risques liés à la sécurité de l'information, Annexe A, tableau 9.

76 P. ex. ressources financières, compétences et moyens techniques

77 Par niveau d'activité, on entend le niveau d'activité dans l'écosystème étudié, dans le domaine ou dans l'industrie concernée.

78 *NSCS*, Type de menaces, auteurs et outils, février 2021.

79 *ANSSI*, La méthode EBIOS Risk Manager — le Guide, 38.

80 *ANSSI*, EBIOS Risk Manager, Going Further, version 1.0 – Novembre 2019, 20.

opératoires exploitent les maillons les plus vulnérables de l'écosystème pour atteindre leur objectif (p. ex. atteinte à la disponibilité d'un service en attaquant le fournisseur de service en nuage).[81]

La première partie de cet atelier vise à évaluer la dangerosité des parties prenantes en considérant plusieurs critères tels que :

– le taux de pénétration de la partie prenante dans les données ;
– le niveau de dépendance de l'organisation vis-à-vis de la partie prenante ;
– le niveau de maturité de la partie prenante en matière de protection des données et de sécurité de l'information ; et
– le niveau de confiance que l'organisation accorde à la partie prenante.

La deuxième partie de l'atelier, après avoir identifié les parties prenantes, consiste à **imaginer des scénarios réalistes de haut niveau**, illustrant comment une source de risque pourrait atteindre son objectif.[82] Par exemple, la source de risque pourrait choisir d'exploiter l'écosystème de l'organisation ou de corrompre un collaborateur. En pratique, ces scénarios sont modélisés sous forme graphique, montrant les différents chemins qu'une source de risque pourrait emprunter pour atteindre son objectif sur une valeur métier.

Les scénarios stratégiques, en relation avec les événements redoutés qu'ils engendrent, permettent d'en apprécier la gravité. Par exemple, une source de risque qui agirait dans un objectif d'entrave au fonctionnement engendrerait une indisponibilité des données. La gravité des événements redoutés consistant en l'altération de la disponibilité serait ainsi reprise.

Il s'agit ici d'une appréciation de la gravité dite « initiale » en cela que les mesures de sécurité ne sont pas prises en compte dans le scénario. Il est important de procéder à une seconde appréciation de la gravité du scénario en tenant compte, par exemple, des mesures de sécurité présentée par le sous-traitant. Des mesures de chiffrement au repos pouvant, par exemple, réduire considérablement la gravité d'un scénario.[83] Cette seconde appréciation de la gravité du scénario démontre de l'importance capitale des contrôles envers les sous-traitants s'agissant des mesures de sécurité.

Les éléments abordés lors de ce troisième atelier peuvent être particulièrement utiles pour analyser une violation de la sécurité des données et en déterminer le niveau de risque. En effet, lorsqu'une telle violation se produit, certaines variables issues de l'analyse des scénarios stratégiques, comme la présence d'une source de risque intentionnelle, sont déjà connues. En partant des données altérées et des informations disponibles sur la source de risque, il devient possible d'émettre des hypothèses concernant l'objectif visé. Cet objectif permet souvent d'évaluer les impacts potentiels sur la personnalité et les droits fondamentaux des personnes concernées. Par exemple, dans le cas d'une violation de la sécurité des données visant à entraver le fonctionnement d'un système, les impacts seraient différents de ceux

81 *ANSSI*, La méthode EBIOS Risk Manager — le Guide, 42.
82 *ANSSI*, La méthode EBIOS Risk Manager — le Guide, 38.
83 Par exemple, si la source de risque ne dispose pas de suffisamment de moyens techniques, le déchiffrement des données serait impossible. La gravité du scénario est ainsi réduite par le biais de la mesure de chiffrement.

d'une violation poursuivant un but lucratif. La gravité de la violation, ainsi que le niveau de risque associé, varieraient en fonction de l'objectif poursuivi.

d) Atelier 4 : Scénarios opérationnels

Le quatrième atelier adopte une démarche similaire au précédent au travers des scénarios, mais vise à déterminer la **vraisemblance** liée à chaque chemin qu'une source de risque pourrait emprunter. Ces chemins se nomment des **scénarios opérationnels** dans le cadre de la méthodologie EBIOS Risk Manager. Le quatrième atelier consiste donc à apprécier la vraisemblance que la source de risque puisse exploiter le scénario opérationnel afin d'atteindre l'objectif qu'elle vise.

Les scénarios opérationnels sont généralement analysés au travers d'outils comme la *Cyber Kill Chain* de Lockheed Martin qui découpe le scénario en actions élémentaires dont la vraisemblance est appréciée action par action. En pratique, et particulièrement lors d'une première itération, la vraisemblance est appréciée pour le scénario complet[84] malgré la perte de précision que cela engendre.

e) Atelier 5 : Traitement du risque

Le cinquième atelier concerne le **traitement des risques** basé sur une synthèse des scénarios. À l'issue du troisième et quatrième atelier, les scénarios représentent les risques dont la gravité et la vraisemblance ont été appréciées. Le niveau de risque de chaque scénario peut ainsi être déterminé sur la base de la matrice d'évaluation du risque.

Selon l'échelle de niveau de risque comportant les critères d'évaluation, l'organisation décide de l'option de traitement approprié pour chaque risque. L'organisation établit ainsi à ce moment les mesures spécifiques à prendre pour les risques dont elle décide, par exemple, un traitement par mitigation. Elle formalise les mesures au sein d'un **plan de traitement des risques**.

Dès lors que les mesures sont mises en œuvre, l'organisation apprécie l'impact des mesures sur les scénarios qu'elles impactent afin de déterminer le risque résiduel. Puis elle décide à nouveau d'une option de traitement pour le risque résiduel.

En pratique, l'impact des mesures est apprécié en amont de leur mise en œuvre afin de déterminer si elles seront suffisamment pour le traitement du risque envisagé. Cela peut également permettre de comparer l'efficacité de plusieurs mesures en vue de choisir celle qui présente le meilleur compromis entre mitigation du risque et ressources nécessaires.

Finalement et de la même manière que dans le cadre de l'approche par conformité, l'organisation doit procéder à la surveillance des mesures et à la revue des risques de manière régulière. En pratique, nous recommandons de mener une revue du troisième et quatrième atelier (dit « **cycle opérationnel** ») au moins chaque année et de la totalité des ateliers (dit « **cycle stratégique** ») au moins tous les trois ans.

[84] *ANSSI*, La méthode EBIOS Risk Manager — le Guide, 65.

G. Conclusion

L'approche fondée sur le risque joue un rôle central dans la protection des données et, plus largement, dans le droit du numérique. Elle permet d'adapter les mesures de sécurité à la nature des risques identifiés, assurant ainsi une protection proportionnée et efficace. Il est important de rappeler que la gestion des risques ne se limite pas au domaine juridique, mais relève aussi d'un cadre normatif beaucoup plus vaste. La gestion des risques est en effet une discipline transverse. Pour bien appréhender l'approche fondée sur le risque, il est nécessaire d'adopter une vision globale qui intègre notamment les normes internationales.

La gestion des risques, bien qu'essentielle, n'est cependant pas exempte de défis majeurs. Parmi eux, la constitution d'échelles d'appréciation fiables et la définition précise des risques, notamment lorsqu'il s'agit de risques élevés, posent souvent problème. Le responsable du traitement et le sous-traitant bénéficient d'une marge d'appréciation qui, bien que nécessaire, peut parfois conduire à des analyses bien trop subjectives. Cette flexibilité, si elle est mal maîtrisée, peut entraîner des appréciations imprécises. Il est donc crucial d'adopter une méthodologie éprouvée afin d'éviter des appréciations approximatives, dites également au « pouce levé » ou « à la louche ». La gestion des risques est également essentielle pour déterminer si certaines obligations, comme la réalisation d'une AIPD ou l'annonce des violations de la sécurité des données, doivent être respectées ou non.

Bien que de nombreuses méthodologies existent pour accompagner la gestion des risques, celle que nous présentons, fondée sur l'adaptation d'EBIOS Risk Manager, se distingue par sa flexibilité et sa transposabilité. Elle permet aux organisations d'appliquer une approche structurée, tant pour les risques courants que pour les scénarios plus complexes.

En conclusion, une gestion des risques bien pensée est incontournable pour naviguer efficacement dans le paysage de la protection des données. Aujourd'hui, la protection des données fait selon nous face à un véritable changement de paradigme. Il ne s'agit plus simplement de se conformer au cadre juridique, mais de penser la protection des données dans une perspective plus large, sous la forme d'une gouvernance des données. Cette approche implique de prendre en compte d'autres considérations, telles que l'usage stratégique des données, l'éthique ou la sécurité, le tout sous un prisme transverse. Les organisations doivent adopter une méthodologie qui intègre ces dimensions variées, en dépassant la simple recherche de la conformité légale pour s'engager dans une véritable démarche de gouvernance des données. Grâce à une méthodologie adaptée comme celle que nous proposons, les organisations pourront non seulement respecter leurs obligations, mais aussi renforcer leur résilience face aux menaces croissantes.