|  |
| --- |
|  |
| **Guide de rédaction d’un Plan d’Assurance de la Sécurité des Informations (PASI)** |
| Edition 5.0 du 6 février 2025 |
| d:\utilisateurs\m.thomas14.DR-CPT\Desktop\Sans titre.jpg |

# Sommaire

[Sommaire 2](#_Toc189729584)

[Introduction générale 3](#_Toc189729585)

[Conseils de rédaction du PASI 4](#_Toc189729586)

[Exigences concernant le formalisme d’un PASI 6](#_Toc189729587)

[Trame d’un plan d’assurance de la sécurité des informations (PASI) 8](#_Toc189729588)

[Page de garde 9](#_Toc189729589)

[Introduction : Le PASI 9](#_Toc189729590)

[Chapitre 1 : L’opération 10](#_Toc189729591)

[Chapitre 2 : Organisation de l’entreprise 12](#_Toc189729592)

[Chapitre 3 : Organisation de l’opération 14](#_Toc189729593)

[Chapitre 4 : Analyse des risques 21](#_Toc189729594)

[Chapitre 5 : Dispositions de réduction de risque 25](#_Toc189729595)

[Chapitre 6 : Suivi de l’application du PASI 28](#_Toc189729596)

[Annexe : Fiches d’analyse de risque 29](#_Toc189729597)

[Note sur l’évaluation des probabilités 31](#_Toc189729598)

# Introduction générale

Le domaine de l’armement est fortement réglementé, et toute activité y est généralement interdite, sauf autorisation. Sur le territoire français, toute activité de commerce, de fabrication ou d’intermédiation de matériel de guerre, d’armes, d’éléments d’armes et de munitions est soumise à une autorisation préalable de l’Etat[[1]](#footnote-1). De même, toute manipulation d’information classifiée est soumise à la fois à l’habilitation du personnel et au besoin d’en connaître[[2]](#footnote-2). À l’exportation, une procédure spécifique s’applique non seulement aux matériels de guerre, armes, éléments d’armes et munitions mais aussi aux matériels dits « assimilés ». L’exportation de ces biens ne peut se faire que suite à l’obtention d’une licence autorisée par la Commission Interministérielle pour l’Étude des Exportations de Matériels de Guerre[[3]](#footnote-3).

Les informations sensibles sont celles dont la divulgation ou l'altération peut porter atteinte aux intérêts de l'État ou à ceux de l'organisme, pour lequel un préjudice financier pourrait, par exemple, le conduire à la faillite. Il faut par conséquent assurer principalement leur confidentialité, et assez souvent répondre à un besoin important d'intégrité.

Depuis 2010, les exportations[[4]](#footnote-4) de technologies prennent une part croissante des opérations soumises à contrôle des exportations. Ces informations sensibles sont contrôlées au titre des catégories ML21, ML22, AMA3 et AMA4[[5]](#footnote-5). Ce type d’exportation est susceptible de s’effectuer par des voies dites « intangibles » ou « dématérialisées ».

Pour toute opération d’exportation présentant des risques significatifs de transferts non autorisés de technologies, de savoir-faire ou d’information sensible, l’administration peut exiger de l’industriel exportateur, en application des articles R2335-12 et -24 du code de la défense, l’élaboration et la mise en œuvre d’un Plan d’Assurance de la Sécurité des Informations (PASI) comme condition préalable sur la réalisation de l’opération, afin d’y apporter des garanties complémentaires. Il appartient alors à l’industriel exportateur de mettre en place une organisation et des moyens adéquats[[6]](#footnote-6) pour assurer la maîtrise de la sécurité des informations sensibles, et le respect de ses obligations, à la fois vis à vis des procédures d’exportations et du contenu de la licence, et vis-à-vis des règles de protection du secret.

Il est rappelé qu’aucune exportation d’information sensible ne peut alors avoir lieu tant que le PASI n’a pas été accepté, et que les dispositions listées ne sont pas mises en œuvre. Il est également rappelé que l’élaboration et la mise en œuvre d’un PASI étant une condition sur la réalisation de l’opération, sa non-application expose le responsable aux sanctions prévues par le code de la défense[[7]](#footnote-7).

# Conseils de rédaction du PASI

**Pourquoi un PASI ?**

D’une manière générale, le PASI (Plan d’Assurance de la Sécurité des Informations) a pour objet de fournir à la DGA et à la CIEEMG l’assurance que des informations jugées sensibles seront en sécurité par rapport aux activités liées à l’opération, grâce (si nécessaire) aux dispositions décrites dans le plan.

Un PASI est demandé lorsque les échanges d’informations envisagés dans l’opération apparaissent plus complexes que ceux pouvant être directement autorisés par une simple licence, pour lesquels un produit défini est vérifié au titre du contrôle export puis transmis à un client identifié.

Ce peut être parce que l’élaboration du produit nécessite des échanges complexes et multiples avec le client, ou implique des travaux collectifs dans des locaux communs, ou passe par des moyens informatiques partagés, ou toute autre forme d’interaction où des informations peuvent être échangées.

Ce peut être aussi, plus simplement, parce que rien ne permet à l’administration de s’assurer qu’il n’est en réalité pas nécessaire de faire une analyse de risque détaillée, ou de prendre des dispositions complémentaires pour réduire encore des risques en réalité déjà négligeables. De ce point de vue, il faut échanger le plus en amont possible dans la formalisation du PASI, afin d’éviter du travail inutile.

* Le PASI peut montrer que les échanges de l’opération portent sur des produits simples couramment traités par le contrôle export. Dans ce cas, un PASI décrivant ces échanges et ce contrôle (y compris le cas échéant sur un plan de soumission des livrables documentaires) est suffisant.
* Si c’est insuffisant, le PASI peut montrer que les dispositions générales applicables dans l’entreprise suffisent à maîtriser tous les risques sur les échanges envisagés. Dans ce cas, il faudra de plus décrire ces dispositions.
* Si c’est encore insuffisant, le PASI peut montrer qu’un risque spécifique de l’opération est couvert de manière satisfaisante par des dispositions adaptées. Dans ce cas, il faudra détailler le risque envisagé, et montrer qualitativement en quoi les dispositions permettent de le maîtriser largement.
* Dans des cas plus complexes, au-delà de ces descriptions qualitatives, une analyse quantitative des risques associés à l’interaction avec des partenaires étrangers peut être nécessaire. Une première évaluation peut alors montrer que les différents risques envisagés sont d’un niveau mesurable mais acceptable. Dans ce cas, il est inutile de rechercher des dispositions complémentaires pour réduire ces risques acceptables.
* Ce n’est que lorsque l’analyse montre que certains niveaux de risque restent inacceptables, qu’il faudra affiner et évaluer des dispositions complémentaires de réduction de risque.

**Guide de rédaction**

Le présent guide a pour objectif d’assister l’industriel exportateur dans la rédaction d’un plan d’assurance de la sécurité des informations (PASI), afin que son contenu soit en phase avec les exigences de l’administration.

Pour faciliter la rédaction et le contrôle du document, et dans la mesure où une section est pertinente par rapport à l’opération et doit être développée :

* Le présent guide signale les analyses que l’industriel ☞ doit effectuer ;
* Les éléments ou points attendus dans une section (et à vérifier en relecture) sont présentés sous forme de « case à cocher ».

Il est important de considérer tous les aspects et de se poser toutes les questions nécessaires lors de sa rédaction et dans l’analyse des risques. Toutefois, chaque question ne se traduit pas nécessairement par une disposition de maîtrise, lorsque le risque évoqué est négligeable ou sans objet. Si l’examen des risques ne conduit pas à prendre une disposition de réduction d’un type particulier, il n’est pas nécessaire de s’imposer une telle disposition pour « cocher la case ». Il suffit de mentionner simplement que ce type de disposition n’apparaît pas nécessaire.

**Démarche itérative**

Une démarche itérative est attendue dans la rédaction du document :

* Décrire la nature de l’opération (§1), les participants et le planning envisagés, et les informations sensibles impliquées.
* Décrire succinctement l’organisation de l’entreprise (§2, en principe commune pour toutes les opérations).
* Décrire l’organisation de l’opération (§3).
* Proposer un processus de gestion des risques (§4) et de suivi du PASI (§6).

L’analyse des risques et l’approfondissement du PASI peuvent ensuite se conduire itérativement :

* Examiner (cf. §4.2) les évènements redoutés associés à la nature de l’opération, la nature des données sensibles, et l’organisation de l’opération. Initier les fiches de risques annexes associées.
* Discuter dans le scénario du risque quels sont les facteurs de risques et les spécificités de tel ou tel élément qui ont une pertinence dimensionnante.
* Vérifier que les éléments dimensionnants sont introduits dans la description de l’opération ou celle de l’organisation de l’entreprise ou de l’opération.
* En parallèle, identifier les dispositions permettant de maîtriser le risque, et les décrire dans l’organisation de l’entreprise (§2) pour les dispositions permanentes, ou dans l’organisation de l’opération (§3) pour les compléments nécessaires.

À chaque étape, il est possible d’échanger avec la DGA, qui peut valider le caractère suffisant ou demander à ce que tel point susceptible de présenter un risque soit éclairci ou approfondi.

**Documentation de la maîtrise des informations sensibles**

Le PASI ***doit*** examiner la protection de ***toutes*** les informations à risque impliquées dans l’opération, qu’elles soient soumises à contrôle des exportations ou classifiées au titre de la protection du secret, qu’elles soient ou non destinées à être transmises à des partenaires, qu’ils soient étrangers ou nationaux. L’objet du PASI est de démontrer que l’entreprise maîtrise le risque d’exporter ou de compromettre accidentellement ces informations soumises à réglementation, compte tenu des ***échanges***, des ***traitements*** ou des ***présences étrangères*** prévus ou rendus possibles par l’opération.

En complément, en tant que « Plan d’Assurance de la Sécurité des Informations », le PASI ***peut*** examiner la protection d’informations ou de technologies sensibles d’autres natures (propriété intellectuelle, etc.).

**Rester à la fois concis et précis**

Le niveau de détail est celui nécessaire et suffisant pour une bonne compréhension des dispositions issues de l’analyse des risques (§5), par rapport aux risques sur les informations sensibles découlant de l’organisation de l’opération (§3) et de son environnement (§2).

Il faut éviter de diluer le document par des descriptions détaillées qui sont sans incidence pour ce qui est de l’exposé sur la maîtrise des risques. Le rédacteur devra se poser en permanence la question « en quoi cet élément est-il pertinent pour la bonne compréhension de la maîtrise de la sécurité des informations sensibles ? » Les éléments à présenter sont ceux qui sont nécessaires et suffisants pour atteindre ce but.

# Exigences concernant le formalisme d’un PASI

**Présentation**

La présentation d’un PASI peut respecter le formalisme imposé au sein d’une société, à condition de comporter une référence et une date ainsi qu’un indice de révision permettant son suivi dans le temps.

Il est important de trouver un titre permettant une identification aisée[[8]](#footnote-8) du plan d’assurance de la sécurité des informations, par exemple en indiquant en complément le nom de l’opération s’il existe.

Le PASI doit être signé au minimum par les personnes responsables des services devant avoir une part dans sa rédaction et sa mise en œuvre ultérieure, à savoir :

* Le responsable de l’opération ;
* Le responsable de la sécurité de défense de la société ;
* Le responsable de la sécurité des systèmes d’information de la société ;
* Le responsable du contrôle des exportations de la société.

La participation de ces services est un prérequis indispensable permettant d’obtenir un document le plus complet possible, et connu des différents acteurs impliqués. Un point de contact privilégié avec l’administration peut bien entendu être défini par la société.

Les risques identifiés doivent être numérotés individuellement (R01 par exemple) ainsi que les dispositions prescrites (M01 par exemple) afin de faciliter leur identification.

**Références à des documents externes**

Le PASI ne doit pas constituer une énumération de procédures, bien qu’il soit admis que certaines procédures existantes au sein du référentiel qualité de l’industriel exportateur peuvent être réutilisées dans le cadre de l’opération. Dans ce cas, leur apport (à quel élément s’appliquent-elles et en quoi contribuent-elles à réduire un risque) doit faire l’objet d’une description suffisante : le PASI doit être autoporteur.

Les données susceptibles d’évoluer régulièrement (liste des personnels autorisés à transmettre de l’information, liste des responsables du programme ou de l’entreprise, etc.) devraient faire l’objet de notes particulières afin d’éviter des mises à jour répétitives du PASI. Ces notes seront alors appelées par le PASI.

**Diffusion des dispositions**

Le plan d’assurance de la sécurité des informations (PASI) est un document dont la diffusion est de niveau restreinte et spéciale à la France[[9]](#footnote-9). Cette disposition a pour but de protéger les éventuels risques sur les informations sensibles, et les dispositions prises pour y remédier.

Le PASI prévoit que certaines de ses dispositions doivent être communiquées aux personnes concernées, y compris à des personnes n’ayant pas nécessairement la nationalité française (personnels de l’industriel exportateur, personnels du client, sous-traitant, etc.) ; il précise dans ce cas les modalités de cette communication (par exemple par un support de sensibilisation dédié, ou un jeu de règles applicables dans le cadre de l’opération).

**Acceptation du PASI**

En amont, il est recommandé que l’industriel transmette[[10]](#footnote-10) au préalable, pour observation, le projet de PASI, au fur et à mesure de l’avancement de la description de l’opération, de l’organisation qui l’accompagne, et en tant que de besoin de sa démarche d’analyse des risques (cf. §4.1). Dans ce cas, les sections non achevées sont simplement marquées comme telles (rédaction réservée, ou toute formule équivalente).

Les PASI en projet ou achevés sont à transmettre au bureau des licences générales et du contrôle sur place, sous-direction de la gestion des procédures de contrôle, direction internationale de la direction générale de l’armement (DGA/DI/SPEM/SDCE/BLGC).

Si le programme est suivi par un directeur d’opération export, celui-ci doit être mis en copie lors de tout échange relatif au plan d’assurance de la sécurité des informations.

**Tenue à jour**

Toute évolution du PASI accepté devra également faire l’objet d’une acceptation avant d’être mise en œuvre. Les évolutions apportées doivent être clairement identifiées dans le corps du document.

Les services de la direction générale de l’armement sont susceptibles d’auditer la stricte application du PASI par l’industriel exportateur. En particulier, ces services sont susceptibles de demander les preuves et enregistrement démontrant que ces dispositions ont bien été respectées[[11]](#footnote-11). L’industriel ☞ doit s’assurer de sa capacité à ***démontrer qu’il respecte les dispositions du PASI*** qui a été accepté.

# Trame d’un plan d’assurance de la sécurité des informations (PASI)

La trame générique d’un plan d’assurance de la sécurité des informations (PASI) est présentée ci-après. Elle est constituée de six chapitres principaux, divisés en sections. Chaque section est ensuite détaillée (en bleu) afin de préciser ce qui en est attendu, et orienter le rédacteur.

Cette trame générique doit permettre de situer rapidement dans le document les différents thèmes que doit aborder un PASI, et faciliter le contrôle de la bonne prise en compte des exigences attachées aux différentes sections.

Introduction : Le PASI

Chapitre 1 : L’opération

1.1 Objet et description de l’opération

1.2 Participants

1.3 Planning général de l’opération

1.4 Articulation administrative

1.5 Enjeu du PASI

Chapitre 2 : Organisation de l’entreprise

2.1 Présentation de l’entreprise

2.2 Organisation générale

2.3 Organisation du contrôle des exportations

2.4 Organisation de la sécurité de défense

2.5 Systèmes d’information communs

2.6 Organisation pour la sécurité des systèmes d’information

Chapitre 3 : Organisation de l’opération

3.1 Cadre géographique

3.2 Cadre informationnel

3.3 Cadre organisationnel de l’opération

3.4 Cadre humain

Chapitre 4 : Analyse des risques

4.1 Processus de gestion des risques

4.2 Identification des risques liés à l’opération

4.3 Analyse des risques

4.4 Tableau de synthèse

Chapitre 5 : Dispositions de réduction de risque

5.1 Sensibilisation et formation du personnel

5.2 Eléments matériels

5.3 Dispositions spécifiques concernant la reproduction, l’enregistrement, le stockage, l’archivage ou la destruction des données

5.4 Mesures de surveillance

5.5 Dispositions pour lutter contre certaines catégories particulières de risques techniques

Chapitre 6 : Suivi de l’application du PASI

6.1 Contrôles internes

6.2 Réévaluation des risques

6.3 Comptes rendus

Annexe : Fiches d’analyse de risque

Description du scénario

Caractérisation du scénario

Analyse du risque

Disposition de réduction

# Page de garde

* La référence du document doit être clairement indiquée.
* La version du document et la date de cette version doivent être indiqués.
* Le PASI doit être signé en principe par le responsable de l’opération, le responsable de la sécurité de défense de la société, le responsable de la sécurité des systèmes d’informations, et le responsable du contrôle des exportations de la société.

Par cette signature, les responsables ☞ doivent assurer :

* Que le PASI reflète la réalité de l’opération et des risques identifiés ;
* Que les dispositions identifiées permettent une maîtrise satisfaisante de la sécurité des informations sensibles impliquées dans l’opération.

# Introduction : Le PASI

L’industriel peut rédiger une introduction (chapitre zéro) présentant le PASI aux personnes qui seront amenées à le lire.

Le contenu de cette introduction est à usage interne, et ne fait en principe pas partie du PASI à proprement parler. Peuvent y figurer :

* Objet du PASI : organisation et dispositions de la société pour maîtriser le risque de compromission sur les informations sensibles dans le cadre de l’opération.
* Périmètre d’application : tous membres du programme, participants au contrôle export, à la SSI, à la sécurité de défense ; auditeurs et contrôle interne,…
* Textes de référence
* Acronymes et abréviations

# L’opération

L’industriel ☞ doit décrire précisément l’objet de l’opération concernée, en faisant ressortir les domaines concernés par le PASI.

* La description doit permettre de situer l’organisation de l’opération (§3), l’analyse des risques (§4), et la description des mesures prises pour y faire face (§5). Inversement, il est inutile de faire des descriptions détaillées si ses éléments ne font pas l’objet de mesures différenciées par la suite.

Il est indispensable, afin de garantir une bonne compréhension de l’opération par l’administration, que le périmètre de l’opération présente les points suivants :

## Objet et description de l’opération

* Présenter le ***contexte*** dans lequel se place l’opération dans son ensemble (historique, besoin, enjeu, …).
* Présenter ***l’objet*** de l’opération dans son ensemble, et ***comment*** cet objet va être atteint.
* Présenter la ***finalité*** industrielle et technique de la part réalisée par l’entreprise (formations prévues, assistance à la conception, transfert de fabrication, etc.).

Le « comment » devra permettre d’identifier ici les principales activités à réaliser.

* Vérifier que la description peut être lue et comprise par des personnes ne connaissant rien du contexte, de la finalité de l’opération et de l’approche de résolution.

Note : Si tout ou partie des éléments demandés dans cette sous-section font l’objet d’un document de présentation de l’opération, la sous-section peut renvoyer à ladite note, à joindre en annexe, et se limiter à présenter les éventuels compléments.

## Participants

Cette présentation doit permettre d’identifier les acteurs ou types d’acteurs concernés par les flux d’informations de l’opération (données techniques, assistance technique, réunions, etc.).

* Présenter le schéma commercial et contractuel complet de l’opération.
* Présenter les différents acteurs (client final, partenaire industriel, sous-traitant[[12]](#footnote-12), etc.).
* Indiquer la répartition des rôles, qui doit réaliser quoi.

## Planning général de l’opération

Présenter une chronologie de l’opération en prenant soin de bien faire figurer :

* La date de lancement prévisionnelle ;
* Les différentes phases de l’opération ;
* La date de fin estimée de l’opération visée par le PASI.

## Articulation administrative

### Historique des contrats de l’opération

* L’industriel peut indiquer, le cas échéant, le cadre historique dans lequel cette opération s’inscrit. Cette rubrique s’adresse tout particulièrement aux PASI destinés à couvrir des opérations de modernisation.

### Périmètre du PASI

* Donner le périmètre exact couvert par le PASI (notamment pour les programmes complexes avec plusieurs PASI).
* Dans ce périmètre, préciser les activités ou phases qui doivent être traitées par le PASI.

### Licences délivrées

* L’industriel ☞ doit identifier puis lister et décrire ici succinctement les licences qu’il a obtenues et le cas échéant, celles qui ont eu pour conséquence la rédaction du PASI dans ses versions successives.

Pour les programmes complexes, titulaires d’un nombre important de licences, indiquer uniquement les licences principales dans le PASI et tenir à jour un fichier de suivi de l’ensemble des licences au niveau de l’équipe programme. Les conditions des licences ne doivent pas être listées, celles-ci pouvant être amenées à évoluer.

## Enjeu du PASI

Cette section doit présenter en quoi un « plan d’assurance de la sécurité des informations » est utile : quelles sont les informations dont la sécurité peut être compromise, et qu’est-ce qui peut compromettre cette sécurité dans l’opération envisagée ?

L’industriel ☞ doit inventorier ici les informations (ou classes d’informations) sensibles qui seront utilisées ou échangées, feront l’objet de traitement, ou seront exposées à l’occasion de présences étrangères, de collaborations, d’accès temporaire ou durable à des locaux ou à des réseaux sensibles à partager, etc.

* Vérifier que toutes les informations à risque identifiées et faisant l’objet de dispositions dans les sections ultérieures sont introduites ici.
* Vérifier pour chaque information que la description expose qu’est-ce qui est à protéger, par rapport à quelles activités, et vis-à-vis de quel risque.
* Le cas échéant, préciser les « points durs » en terme de sécurité des informations (dimensionnant pour l’analyse des risques).

# Organisation de l’entreprise

Les « dispositions » (mesures et règles de maîtrise des risques pour la sécurité des informations) prises au titre de l’organisation générale de l’entreprise et donc applicables *a priori* à l’opération, ne sont pas décrites ici mais sont regroupées dans le chapitre §3 suivant. Les dispositions spécifiques à l’opération sont décrites au titre de la réduction complémentaire des risques, dans le chapitre §5.

* Décrire ici l’organisation de l’entreprise, et le cas échéant, l’organisation au niveau des établissements. Si les fonctions de contrôle sont assurées au niveau du groupe, l’organisation devra également être décrite à ce niveau.

Dans le cas d’une organisation à plusieurs niveaux (groupe / société / établissement), si l’opération concerne plusieurs éléments et si la rédaction doit conduire à la fois à des éléments communs et des parties différenciées, il peut être souhaitable de regrouper les éléments communs dans un PASI « chapeau », et présenter les éléments complémentaires suivant le même plan, dans des documents complémentaires annexes propres aux différents composants.

Note : Si les éléments demandés dans les sous-sections suivantes font l’objet d’une fiche ou note de présentation ou d’organisation préexistante, la sous-section peut se limiter à renvoyer à ladite note, à joindre en annexe.

## Présentation de l’entreprise

* Situer les sociétés du groupe le cas échéant, en particulier les sociétés étrangères et celles susceptibles d’intervenir dans l’opération.
* Situer l’entreprise en quelques éléments clefs : secteur d’activité, taille, part de l’activité défense et part de l’activité export, principales implantations, etc.

## Organisation générale

* Donner un organigramme permettant de retracer les rattachements hiérarchiques et fonctionnels qui sont évoqués dans le reste du document.
* Préciser en tant que de besoin les principes généraux d’organisation (responsabilité d’un directeur de site, d’un chef de projet, organisation matricielle, …) dans lesquels l’opération s’insèrera, et dont la mention est pertinente par rapport à l’analyse des risques ou aux dispositions prises pour y faire face.

## Organisation du contrôle des exportations

* L’industriel doit décrire ici son organisation générale en terme de contrôle des exportations, notamment :
* La place du contrôle des exportations au sein de l’entreprise ;
* Les directions ou services concernés ;
* Ses missions et les fonctions exercées ;
* Ses liens hiérarchiques et fonctionnels avec d’autres services.
* Vérifier que les liens hiérarchiques et fonctionnels indiqués peuvent être rattachés à des éléments présentés dans l’organisation générale.

## Organisation de la sécurité de défense

* L’industriel doit décrire ici son organisation générale en terme de sécurité de défense, notamment :
* La place de la sécurité de défense au sein de l’entreprise ;
* Les directions ou services concernés ;
* Ses missions et les fonctions exercées ;
* Ses liens hiérarchiques et fonctionnels avec d’autres services.
* Vérifier que les liens hiérarchiques et fonctionnels indiqués peuvent être rattachés à des éléments présentés dans l’organisation générale.

## Systèmes d’information communs

* Préciser ici en tant que de besoin les moyens (messageries, réseaux dédiés, applicatifs) qui font partie du fonctionnement courant de l’entreprise et seront susceptibles d’être utilisés par les participants à l’opération.

## Organisation pour la sécurité des systèmes d’information

* L’industriel doit décrire ici son organisation générale en terme de sécurité des systèmes d’information, notamment :
* La place de la sécurité des systèmes d’information au sein de l’entreprise ;
* Les directions ou services concernés ;
* Ses missions et les fonctions exercées ;
* Ses liens hiérarchiques et fonctionnels avec d’autres services.
* Vérifier que les liens hiérarchiques et fonctionnels indiqués peuvent être rattachés à des éléments présentés dans l’organisation générale.

# Organisation de l’opération

Ce chapitre a pour objet de décrire le cadre spécifique dans lequel se déroulera l’opération, les risques que l’opération présente vis-à-vis de la protection d’informations sensible, et la protection apportée par les dispositions générales de l’entreprise ou du site.

Les « dispositions » (mesures et règles de maîtrise des risques pour la sécurité des informations) éventuellement décrites ici se limitent aux dispositions habituellement retenues au titre de l’organisation générale de l’entreprise ou du site, et donc applicables *a priori* à l’opération (hors aspects formation, regroupés en §5.1). Les dispositions spécifiques à l’opération sont décrites au titre de la réduction des risques, dans le chapitre §5.

* Vérifier que les enregistrements disponibles permettront d’apporter les éléments justifiant le respect des dispositions applicables.

Ce chapitre est la première étape de l’analyse des risques.

* En regard de chaque disposition applicable à l’opération, le rédacteur ☞ doit se demander si elle est de nature à limiter un risque de compromission, et par rapport à quelle donnée sensible.
* En regard de chaque élément de l’organisation de l’opération, le rédacteur ☞ doit se demander si cet élément est porteur d’un risque particulier pour les informations, technologies ou savoir-faire impliqués, et si ce risque est maîtrisé.
* Le résultat de cette analyse primaire doit se retrouver dans le document :

|  |  |
| --- | --- |
| **Estimation qualitative du scénario de risque** | **Niveau de description requis** |
| Scénario de type « mission impossible » ? | Ne pas mentionner de risque. |
| Les multiples dispositions couvrent de manière évidemment satisfaisante et redondante un des risques de com–promission d’une information sensible? | Mentionner à propos de l’élément d’information sensible que tel risque est maîtrisé (ce qui montre que le risque a été examiné). |
| Une disposition (ou deux) couvre spécifiquement un risque de manière évidemment satisfaisante ? | Mentionner en regard de la disposition en question (laquelle est donc à documenter dans le chapitre) qu’elle permet de maîtriser tel risque (ce qui signale que la disposition peut utilement figurer dans un plan d’audit). |
| Une disposition est peut-être insuffisante dans certains cas pour couvrir le risque ? | Identifier un risque (§4.4) et renvoyer à une analyse ultérieure. |

* Les informations à risque identifiées ici doivent être introduites en §1.5.
* S’il faut mentionner une procédure, il n’est pas souhaitable d’en préciser ici le détail, mais (au titre de l’assurance de la sécurité des informations) son objet et son but. S’il paraît nécessaire d’en donner le détail, le faire sur une fiche annexe.
* Pour la bonne lecture des fiches d’analyse de risque, les dispositions éventuellement présentées ici doivent être numérotées de manière cohérente (section, sous-section et numéro à suivre) et clairement délimitées dans le document.
* Les dispositions précisent en tant que de besoin leur cadre d’application (géographique, informationnel et humain).

Le niveau de description ☞ doit être maintenu en cohérence avec l’analyse des risques ultérieure (fiches en annexe), et la description des dispositions prises pour y faire face (§5) ; le chapitre ☞ doit être mis à jour, en tant que de besoin, au fur et à mesure de la progression de cette analyse. Les points abordés dans ces chapitres ultérieurs doivent être présentés sommairement ici. Inversement, il est inutile de faire des descriptions détaillées si ses éléments ne font pas l’objet de dispositions différenciées par la suite.

## Cadre géographique

### Identification et présentation des sites opérationnels en France

L’industriel ☞ doit préciser ici quels sont les sites situés sur le territoire français qui seront impactés par l’opération. Pour chacun des sites identifiés :

* Préciser les raisons sociales et adresses des sites concernés.
* Indiquer leur niveau de protection : niveau d’habilitation, qualité de point d’importance vitale (PIV), présence de zone à régime restrictif (ZRR), Zone d'Importance Vitale (ZIV), etc.
* Indiquer quel type de personnel y sera résident (§3.4).
* Indiquer également, pour chacun des sites relevés, le type d’activité qui y sera réalisé et les conséquences vis à vis du PASI.
* Préciser les modalités d’accès aux différents locaux (badges, plage horaire, circuit de notoriété, accompagnement, etc.) pour les différentes catégories de personnes identifiées.

### Identification et présentation des sites opérationnels à l’étranger

L’industriel doit préciser ici les sites situés à l’étranger sur lesquels son personnel participera à l’opération. Pour chacun des sites identifiés :

* Préciser les raisons sociales et adresses des sites concernés.
* Indiquer quel type de personnel y sera résident ou visiteur (§3.4).
* Préciser les modalités d’accès par les différents types de personnel (badges, plage horaire, etc.).
* Préciser les modalités d’accès par le client (badges, plage horaire, circuit de notoriété, accompagnement, etc.).
* Indiquer le type d’activité qui y sera réalisé, et les conséquences vis à vis du PASI.

### Locaux dédiés à l’opération

S’il y a des locaux dédiés à l’opération sur l’un ou l’autre des sites (état néant sinon), l’industriel doit détailler ici les locaux utilisés dans le cadre de l’opération, à la fois en France et à l’étranger.

Note : Les mesures applicables à des locaux dédiés peuvent aussi bien être considérées comme des mesures d’organisation de l’opération (relevant du §3) que comme des mesures structurelles de réduction de risque (relevant du §5). L’industriel peut choisir de décrire ici toutes les mesures et dispositions relatives aux locaux, y compris celles qui auraient éventuellement été ajoutées à la suite de l’analyse des risques. Alternativement, il peut considérer que toutes les dispositions relatives aux locaux dédiés sont des mesures de réduction de risque, par rapport à l’hypothèse de locaux non cloisonnés et de libre circulation, et présenter l’ensemble des dispositions en §5.2. Dans ce dernier cas, la section présente se limitera à la description topographique.

* Décrire en premier lieu les éventuelles dispositions qui seront applicables à l’ensemble des sites, ou à toute une catégorie de sites.
* Décrire ensuite, site par site, la situation topographique et les dispositions spécifiques applicables.

Si la description des locaux et des dispositions associées est complexe (plus de deux pages), cette section peut se limiter à en donner la liste, et renvoyer en annexe pour une description détaillée (une fiche par locaux).

Description topographique :

Décrire les locaux en tenant compte de l’aspect sûreté, et le cas échéant, les situer dans le bâtiment ou le site. Joindre un plan si la configuration du bâtiment ou du site est complexe.

Dispositions pour les locaux dédiés en France :

En France, préciser les locaux utilisés par les équipes projet et ceux fréquentés ou susceptibles d’être fréquentés par le client :

* Préciser les modalités d’accès aux différents locaux par les équipes projet (badges, plage horaire, circuit de notoriété, accompagnement, etc.).
* Préciser les modalités d’accès aux différents locaux par le client (badges, plage horaire, circuit de notoriété, accompagnement, etc.).
* Préciser les caractéristiques des locaux utilisés par le client (capacité d’accéder aux réseaux, interdiction de tout appareil permettant une prise de vue, etc.).

Dispositions pour les détachements ou missions à l’étranger :

À l’étranger,

* Indiquer les modalités d’accueil des équipes et le degré d’autonomie sur chacun des sites.
* Préciser les caractéristiques des locaux utilisés par les missionnaires (capacité d’accéder aux réseaux, capacité d’accéder aux outils et systèmes, etc.).

Il est généralement convenu qu’un hébergement longue durée chez le client ne présente pas les mêmes garanties d’intégrité des locaux comparé à la location d’un local et sa mise à hauteur à un standard de sécurité maitrisé.

Tenant compte de ces environnements, l’industriel ☞ doit lister les dispositions prises *a priori* afin d’assurer la sécurité de ses personnels et des informations détenues.

## Cadre informationnel

Note : les dispositions associées aux échanges verbaux (réunions, courriers électroniques, téléphone, …) sont décrites au titre du cadre humain (§3.4).

### Identification des outils et systèmes d’information (software)

L’industriel ☞ doit répertorier et présenter ici les outils et systèmes d’information déployés dans le cadre de l’opération, et pouvant supporter des informations sensibles.

* Indiquer pour chacun d’entre eux leurs caractéristiques (responsabilités, règles d’accès, etc.).
* Préciser la nature des informations sensibles qui y sont gérées (en lien avec §3.2.3).
* Préciser si l’outil est normalement accessible au client, ou à telle ou telle catégorie de personnel (§3.4) ; le cas échéant, préciser les règles d’accès spécifique à telle ou telle catégorie de personnel.
* Préciser le cas échéant les dispositions interdisant l’accès aux catégories de personnel non autorisées.
* Préciser le cas échéant la localisation des postes (§3.1.3) permettant l’accès à ces outils.

### Identification des infrastructures informatiques (hardware)

L’industriel doit présenter ici les réseaux accessibles dans le cadre de l’opération.

* Indiquer pour chacun d’entre eux leurs caractéristiques (architecture, responsabilités, règles d’accès, etc.).
* Préciser la nature des informations sensibles qui y sont disponibles (en lien avec §3.2.3).
* Préciser la localisation des postes permettant l’accès aux réseaux (en lien avec §3.1).
* Préciser le pays de localisation des serveurs.

L’industriel doit également décrire les matériels informatiques utilisés dans le cadre de l’opération, en indiquant pour chacun d’entre eux leurs caractéristiques. Il présentera notamment :

* Les ordinateurs particuliers (postes blanchis mis à disposition des missionnaires, postes spécifiquement configurés pour le client, etc.) ;
* Les ressources spécifiques (clé USB nominative, disque dur externe sécurisé, téléphones chiffrés, etc.).

### Identification des informations manipulées dans le cadre de l’opération

En cohérence avec l’identification des moyens informatiques, des outils et des canaux de transmission de l’information, l’industriel ☞ doit répertorier par nature et support les types d’informations soumises à contrôle réglementaire (ou sensible) qui seront manipulées ou accessibles dans le cadre de l’opération[[13]](#footnote-13).

Par manipulation, il est entendu les informations soumises à contrôle (ou sensibles) qui seront :

* Exportées vers les partenaires de l’opération, qu’ils soient nationaux ou étrangers ;
* Utilisées ou potentiellement utilisables par l’équipe programme dans son environnement[[14]](#footnote-14).
* Par nature, doit être précisé la forme sous laquelle se présente les informations à protéger : connaissance ou savoir-faire, base de données, logiciel, caractéristiques technique, données d’essai et de performance, procédé, etc.
* Par support, doit être précisé la forme sous laquelle se présente l’information : informatique, document imprimé, assistance et savoir-faire, exposé et réunion, etc.
* Par type d’informations soumises à contrôle, doivent être précisés la catégorie de contrôle (ML21, ML22, AMA3 et AMA4, ou non contrôlée) les niveaux de protection et de confidentialité des informations manipulées ainsi que la présence de marquage particulier.

Note : les règles de classification à l’usage des rédacteurs sont précisées en tant que de besoin au titre de l’organisation de l’opération (§3.3).

### Processus de transmission des informations sensibles

L’industriel ☞ doit identifier les canaux de transmission des informations sensibles prévus dans le cadre de l’opération, que ceux-ci utilisent une voie dématérialisée ou matérielle. Les situations suivantes seront ainsi décrites dès lors qu’elles sont autorisées :

* Transmission papier ou sur support numérique (clé USB, CD-ROM, etc.) ;
* Outil de partage de données ;
* Système d’information ;
* Formation ;
* Plateau de travail collaboratif ;
* Etc., liste non exhaustive, répertoriant les principaux canaux actuellement utilisés.

Pour chacun des canaux,

* Préciser les informations sensibles (§3.2.3) susceptibles d’y être échangées.

Pour chacun des canaux, préciser les dispositions retenues permettant :

* Une approbation préalable des documents par des personnels compétents ;
* Un marquage des documents comme contenant des informations soumises à contrôle ;
* Une traçabilité complète des échanges ;
* Une sécurisation forte des échanges.

Aucune dérogation aux canaux identifiés dans le PASI ne peut être tolérée pour la transmission d’informations soumises à contrôle.

Note : les échanges associés aux messageries, communications téléphoniques ou réunions, sont décrits ci-après avec le cadre humain (§3.4).

## Cadre organisationnel de l’opération

### Organisation de l’opération

Décrire ici l’organisation générale de l’opération :

* Composition de l’équipe projet de l’industriel ;
* Interactions avec les partenaires étrangers ;
* Gouvernance de l’opération ;
* Réunions techniques.

### Identification des profils spécifiques PASI mis en place pour l’opération

L’industriel ☞ doit définir et introduire ici les fonctions spécifiques créées au sein de l’équipe programme en conséquence de la mise en place du PASI (le cas échéant, les dispositions d’organisation les concernant sont décrites dans les sections suivantes).

* Donner la liste des fonctions spécifiques ;
* Indiquer leurs liens hiérarchiques et fonctionnels.

Quelques profils spécifiques, donnés à titre d’exemple :

* Un responsable d’assurance de la sécurité des informations, dédié à l’application et au suivi du PASI ;
* Un responsable de la sensibilisation des équipes au PASI ;
* Un vérificateur technique, chargé d’approuver la sortie des documents contenant des informations soumises à contrôle.

### Organisation pour le contrôle des exportations

L’industriel doit préciser ici les arrangements spécifiques pris afin de pouvoir assurer un soutien de proximité dans le cadre de l’opération objet du PASI. Ce soutien peut revêtir différentes formes, comme la nomination d’un point de contact privilégié.

* L’articulation du soutien spécifique avec l’organisation globale de l’entreprise et l’organisation de l’opération doit être précisée.
* Les responsabilités en terme de sensibilisation et de formation doivent être listées.
* Préciser le référent pour le classement vis-à-vis du contrôle des exportations.
* Préciser les règles de vérification et d’approbation pour le classement vis-à-vis du contrôle des exportations.

### Organisation de la sécurité de défense

L’industriel doit préciser ici les arrangements spécifiques pris afin de pouvoir assurer un soutien de proximité dans le cadre de l’opération objet du PASI. Ce soutien peut revêtir différentes formes, comme la nomination d’un point de contact privilégié.

* L’articulation du soutien spécifique avec l’organisation globale de l’entreprise doit être précisée.
* Les responsabilités en terme de sensibilisation et de formation doivent être listées.
* Préciser le référent pour la classification vis-à-vis de la protection du secret.
* Préciser les règles de vérification et d’approbation pour la classification vis-à-vis de la protection du secret.

### Organisation de la sécurité des systèmes d’informations

L’industriel doit préciser ici les arrangements spécifiques pris afin de pouvoir assurer le contrôle nécessaire dans le cadre de l’opération objet du PASI.

* Les responsabilités en terme de sensibilisation et de formation doivent être listées.
* L’administration des autorisations d’accès sur les outils et systèmes identifiés doit être précisée, pour les différentes catégories de profils utilisateurs.
* L’articulation du soutien spécifique avec l’organisation globale de l’entreprise doit être précisée.
* Préciser en tant que de besoin le référent pour le classement des informations sensibles, en particulier l’information propriétaire (hors protection réglementaire).

### Gestion des incidents

L’industriel doit développer ici son processus de gestion des incidents dédié à l’opération objet du PASI. Il y détaille tout particulièrement :

* Les responsables du processus et les acteurs ;
* Les outils utilisés pour assurer la remontée des incidents et leur traitement ;
* Les outils utilisés afin de garantir la prise en compte des incidents par le ou les services concernés (par exemple, un incident relatif au contrôle des exportations doit bien remonter au service en charge du contrôle des exportations) ;
* Les règles d’information de l’administration en fonction de la gravité des incidents traités ;
* La prise en compte du retour d’expérience lors de la revue des risques.

## Cadre humain

### Catégories de personnels

* L’industriel ☞ doit identifier et lister ici les différentes catégories de personnels impliqués dans l’opération ou présents sur les lieux, et susceptibles d’être un facteur de risque différencié, soit par exemple :
* Les personnels du programme ;
* Les autres personnels de la société ;
* Les stagiaires, nationaux et étrangers ;
* Le personnel d’entretien ;
* Le personnel d’audit ;
* Les personnels du client ou du partenaire industriel ;
* Les personnels d’éventuels sous-traitants ;
* … etc.

Pour ces différentes catégories de personnel, décrire en quelques mots leur rôle, leur interaction possible avec les autres personnels, les locaux ou les éléments d’information.

### Gestion des réunions

L’industriel ☞ doit identifier ici les réunions ou types de réunion susceptibles de mettre en œuvre de l’information sensible et nécessitant des mesures de protection.

* Préciser la nature des informations (§3.2.3) susceptibles d’être abordées dans ces réunions.
* Préciser les catégories de personnel concernées (§3.4.1) et/ou leur place dans l’organisation de l’opération (§3.3).

Préciser les dispositions (générales, ou spécifiques à tel type de réunion) permettant d’assurer, en tant que de besoin :

* En amont, que les informations qui seront échangées en réunion sont autorisées.
* La légitimité de l’accès des participants aux informations échangées.
* La maîtrise de la confidentialité des échanges.
* En aval, la traçabilité de la réunion, en particulier la conservation d’un compte-rendu.

### Communications interpersonnelles

L’industriel ☞ doit identifier ici les différents types d’échanges (courrier électronique, téléphone, smartphone et portable, …) susceptibles de mettre en œuvre de l’information sensible et nécessitant des mesures de protection.

* Préciser la nature des informations susceptibles d’être discutées.
* Préciser les catégories de personnel concernées et leur place dans l’organisation de l’opération.
* Préciser en tant que de besoin les dispositions permettant d’assurer la confidentialité des échanges.
* Préciser en tant que de besoin les dispositions permettant d’assurer la traçabilité des échanges.

### Reprographie, stockage, archivage ou destruction

* En complément à la description du traitement des informations (§3.3), préciser ici les autres dispositions applicables aux documents manipulés dans l’opération, en particulier les dispositions applicables aux impressions d’exemplaires de travail, etc.

# Analyse des risques

Un risque est l’occurrence potentielle d’un « événement » (danger, scénario) futur, incertain, ne dépendant pas exclusivement de la volonté des parties, et dont la manifestation est susceptible d’engendrer des dommages. Dans le cadre du PASI, il faut entendre par danger tout événement dont la survenance est susceptible d’entrainer ou faciliter l’obtention par un tiers d’informations ou de capacités soumises à contrôle, ou d’informations sensibles, autres que celles autorisées.

Les dispositions discutées sont identifiées dans le chapitre suivant (§5) ; et le suivi de l’application est décrit dans le dernier chapitre (§6).

L’industriel est responsable de sa méthode d’analyse des risques, les exemples ci-après ne sont donnés qu’à titre indicatif.

Pour mémoire, le chapitre §3 ☞ doit documenter une analyse de risque primaire sur l’organisation de l’opération. Si cette analyse primaire et l’éventuelle identification des risques décrite en §4.2 permettent de constater que les scénarios redoutés peuvent être considérés comme suffisamment maîtrisés, l’analyse des risques (§4.3) est sans objet. Dans ce cas, il n’est demandé ni tableau de synthèse (§4.4 sans objet), ni de décrire les dispositions de réduction des risques (§5) en dehors des éventuelles dispositions relatives à la sensibilisation et à la formation (§5.1).

## Processus de gestion des risques

L’industriel ☞ doit définir et exposer ici l’organisation de son ***processus de gestion*** des risques (identification, analyse, réduction et maîtrise) dédié à l’opération, en précisant notamment :

* Le responsable du processus ;
* Les acteurs impliqués ;
* Le déroulement des différentes étapes du processus, et le calendrier associé.
* Distinguer s’il y a lieu entre l’organisation initiale adoptée pour la rédaction du PASI et l’organisation applicable pendant la durée de l’opération. Alternativement, si les organisations sont très différentes, la réévaluation des risques en cours d’opération peut être fait dans le chapitre sur le suivi (§6).

## Identification des menaces liés à l’opération

L’industriel doit décrire ici la ***méthode*** utilisée pour identifier les menaces propres à l’opération (non pas les risques eux-mêmes, qui seront en résultat listés en §4.4).

A/ Comme signalé dans le chapitre §3, la rédaction même de ce chapitre ☞ doit être faite dans une optique d’analyse systématique visant à identifier les menaces les plus évidentes et celles nécessitant une analyse plus approfondie ; la méthode retenue peut doubler cet examen obligatoire par un balayage plus approfondi.

B/ En analyse systématique, il est recommandé de mener l’analyse des risques au niveau de chaque type d’activité de l’opération susceptible de produire, échanger ou accéder à des informations soumises à contrôle (décrites en §3.2) ; et d’une manière générale de questionner chaque élément de l’organisation de l’opération (cadre géographique, informationnel et humain du chapitre §3, entités participantes, etc.) susceptible d’introduire un danger particulier.

C/ Les grandes familles de menaces identifiables *a priori* sont par exemple :

* L’espionnage, la collecte d’informations par des personnes non autorisées ;
* La transmission non autorisée d’information soumise à contrôle ou sensible ;
* La compromission technique ;
* La rétro-ingénierie ;
* Le détournement de matériel ;
* La contamination d’information par la législation ITAR.

… Liste non exhaustive. La veille, le retour d’expérience, l’audit de contrôle interne et le *benchmarking* permettent l’identification de nouvelles menaces.

D/ Préciser le cas échéant les *benchmarking* et retours d’expérience disponibles.

## Analyse des risques

La criticité d’un risque résulte de sa probabilité et de la gravité de l’évènement redouté (c’est une « espérance » au sens mathématique du terme). La criticité n’est quantifiable que par rapport à un ***scénario*** spécifique, réalisant une menace générale, scénario qui ☞ doit être précisé dans la fiche d’analyse du risque.

Quatre niveaux au minimum ☞ doivent être retenus afin de quantifier l’ordre de grandeur de la probabilité et la gravité.

* L’industriel doit préciser ici quels sont les critères retenus pour caractériser chaque niveau.

### Probabilité

La **probabilité** d’occurrence d’un risque est celle d’apparition du scénario à risque, compte tenu de la présence d’éventuels facteurs de risque.

* Préciser les critères qualitatifs ou quantitatifs conduisant à affecter une classe de probabilité et une cotation à un scénario.
* La probabilité doit être définie par rapport à une durée à préciser, qui peut être une année, la durée d’une phase, ou celle de l’opération.

Par exemple, une approche semi-quantitative pourra décider que les classes de probabilités prises en compte seront par convention les suivantes :

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Classe** | **Impossible** | **Improbable** | **Possible** | **Incertain** | **Probable** |
| **Probabilité** | <0.2 % | 0.2 à 1 % | 1 à 5% | 5 à 20 % | >20 % |
| **Cotation** | 0 | 1 | 2 | 3 | 4 |

### Gravité

La **gravité** d’un risque doit pour le PASI être évaluée en raison de la perte de maîtrise des informations qu’il représenterait, si l’évènement redouté se produit.

* Préciser les critères qualitatifs ou quantitatifs conduisant à affecter une classe de gravité et une cotation au résultat d’un scénario.

On aura par exemple (exemple à adapter en fonction de l’objet propre de l’opération) :

| **Gravité :** Obtention par une personne physique ou morale non autorisée, de… | **Qualification** | **Cotation** |
| --- | --- | --- |
| Connaissances ou informations clefs autorisant la mise en œuvre de la technologie (développement, production, réparation ou rénovation) associée à un matériel de guerre ou assimilé. | Inacceptable | 4 |
| Connaissances ou informations clefs autorisant la mise en œuvre (assemblage, exploitation, installation, entretien ou révision) d’un matériel de guerre. | Grave | 3 |
| Connaissances ou informations qui, combinées à d’autres, autoriseraient les mises en œuvre précédentes. | Problématique | 2 |
| Connaissances ou informations de nature à faciliter l’obtention des connaissances ou informations de la catégorie précédentes. | Gênant | 1 |
| Connaissances ou informations n’entrant pas dans la catégorie précédente. | Regrettable | 0 |

La protection d’informations classifiées repose sur le principe d’une protection « en profondeur ». La gravité d’une défaillance peut s’apprécier également en fonction de la détérioration plus ou moins profonde d’une telle protection.

On aura par exemple :

| **Critère de Gravité :** | **Qualification** | **Cotation** |
| --- | --- | --- |
| Accès non autorisé à une information protégée | Inacceptable | 3 |
| Défaillance permanente ou contournement usuel d’une mesure de protection | Grave | 2 |
| Affaiblissement d’une mesure de protection | Problématique | 1 |
| Dispositions de protection conformes | Sans conséquence | 0 |

De même, la gravité peut être fonction de la nature de la protection formelle, une compromission par rapport aux règles de protection du secret étant d’autant plus grave que la protection est élevée.

La gravité peut dans ce cas être la somme des différents critères, lorsque ces critères se superposent, ou être la plus élevée des valeurs, lorsque l’évaluation se fait suivant des critères indépendants.

D’une manière générale, la gravité s’apprécie par le degré de compromission d’un des objectifs de l’entreprise, et par l’importance que l’entreprise accorde à cet objectif. Ici l’objectif du PASI se limite à la non-compromission des informations et technologies sensibles.

### Criticité

La **criticité** est typiquement déterminée à partir de la gravité et de la probabilité.

* L’industriel doit préciser la méthode employée pour caractériser la criticité.

Par exemple, si ces deux éléments sont donnés par les tableaux ci-dessus, la criticité pourra être évaluée par la somme des cotations.

### Critères d’acceptation

* L’industriel doit ensuite indiquer ici la logique utilisée pour le traitement ultérieur des risques (risque toléré, surveillé, à réduire…) sous la forme d’une matrice croisant la probabilité et la gravité.

On aura par exemple :

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Inacceptable : 4** | | | 4 | | | 5 | 6 | | 7 | | 8 |
| **Grave : 3** | | | 3 | | | 4 | 5 | | 6 | | 7 |
| **Problématique : 2** | | | 2 | | | 3 | 4 | | 5 | | 6 |
| **Gênant : 1** | | | 1 | | | 2 | 3 | | 4 | | 5 |
| **Regrettable : 0** | | | 0 | | | 1 | 2 | | 3 | | 4 |
| ↑ Gravité | | Probabilité → | **0 : Impossible** | | | **1 : improbable** | **2 : Possible** | | **3 : Incertain** | | **4 : Probable** |
| <4 | Négligeable | | | 4 | À surveiller ou réduire | | | >4 | | À réduire | |

## Tableau de synthèse

Pour chacun des dangers redoutés, une fiche d’analyse de risque ☞ doit ensuite être créée. Afin de faciliter la lecture du PASI et sa mise à jour, ces fiches d’analyse de risque sont regroupées en annexe.

Chaque risque identifié ☞ doit être évalué selon la méthode choisie.

Si le niveau d’un risque est important, même compte tenu des dispositions générales de l’entreprise, des dispositions particulières à l’opération ☞ doivent être prises, et décrites en §5. Les risques ☞ doivent ensuite être réévalués dans l’hypothèse où les dispositions adaptées ont été mises en place (nomination d’un pilote et application des dispositions prévues).

* L’industriel synthétise ici l’analyse des risques sous la forme d’un tableau récapitulatif (numéro du risque, libellé du risque, probabilité, gravité et criticité, *a priori* avant action de réduction, puis après action de réduction).

Par exemple :

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Tableau récapitulatif des risques | | *A priori* | | | Après réduction | | |
| N° | Libellé | P | G | C | P | G | C |
|  |  |  |  |  |  |  |  |

Note : Un PASI ne peut être considéré comme achevé, et accepté par l’autorité, que si après réduction les risques identifiés sont tolérables ou sous surveillance.

# Dispositions de réduction de risque

Les « dispositions » (mesures et règles de maîtrise des risques pour la sécurité des informations) décrites ici se limitent aux dispositions spécifiques à l’opération. Il est entendu que l’analyse des risques peut conduire à identifier des dispositions habituellement retenues au titre de l’organisation générale de l’entreprise, et donc applicables *a priori* à l’opération. De telles dispositions sont alors reportées et décrites au titre de l’organisation de l’opération, dans le chapitre §3.

* Vérifier que les enregistrements disponibles permettront d’apporter les éléments justifiant le respect des dispositions applicables.

Pour la bonne lecture des fiches d’analyse de risque, les dispositions présentées doivent être numérotées de manière cohérente (section, sous-section et numéro à suivre) et clairement délimitées dans le document. Elles précisent en tant que de besoin leur cadre d’application (géographique, informationnel et humain).

* S’il faut mentionner une procédure, il n’est pas souhaitable d’en préciser ici le détail, mais (au titre de l’assurance de la sécurité des informations) son objet et son but. S’il paraît nécessaire d’en donner le détail, le faire sur une fiche annexe.

## Sensibilisation et formation du personnel

En fonction des catégories de personnel (§3.4), qu’elles soient ou non directement liés à l’opération, ou dans le cadre de l’organisation de l’opération (§3.3), l’industriel ☞ doit identifier la formation et la sensibilisation nécessaire pour l’opération, en complément de celle normalement dispensée au niveau de l’entreprise.

Il est entendu que plusieurs niveaux de sensibilisations ou de formations peuvent être envisagés en fonction du degré d’exposition des employés, et que celles-ci peuvent être cumulatives.

* Identifier dans l’organisation de l’entreprise (§2) ou celle de l’opération (§3.3) un responsable des sensibilisations/formations.
* Lister ici les sensibilisations et formations à prendre en compte, qu’elles soient spécifiques à l’opération ou habituellement dispensées dans l’entreprise.

Pour chacune des sensibilisations et formations identifiées :

* Indiquer les différentes catégories de personnels concernés.
* Récapituler les objectifs.

L’industriel ☞ doit indiquer les dispositions complémentaires applicables aux formations.

* La traçabilité de la formation doit être assurée : la sensibilisation et la formation des employés doivent être réalisées lors de séances qui font l’objet d’un émargement par les personnes conviées ; un suivi des personnels concernés doit être tenu.

Normalement, un personnel ne peut avoir une interaction avec le client sans qu’il ait été au moins sensibilisé sur les règles relatives à la protection des informations. Un engagement de responsabilité concernant l’application de ces règles ☞ doit être signé par les personnels concernés.

### Formations générales

Les sensibilisation « génériques » habituellement dispensées dans l’entreprise peuvent être par exemple :

* Sensibilisation aux règles relatives à la protection des informations.
* Sensibilisation / Formation au contrôle des exportations.
* Sensibilisation / Formation à la SSI.
* Sensibilisation / Formation aux règles de protection du secret.

Ces formations sont typiquement destinées aux différents intervenants dans les processus correspondants. N’indiquer que les formations effectivement rencontrées dans l’organisation de l’opération.

### Formations Spécifiques à l’opération

Quelques sensibilisations et formations, données à titre d’exemple :

* Sensibilisation aux règles relatives à la protection des informations.
* Sensibilisation PASI et contrôle export – dédiée à tous les membres de l’opération et aux personnels au contact ;
* Formation PASI et contrôle export – dédiée aux personnels pouvant échanger avec le client ;
* Sensibilisation culturelle et sûreté pays client – dédiée aux missionnaires longue durée de l’opération ;
* Information générale PASI – dédiée à être diffusée aux personnels travaillant dans les services physiquement proches de l’opération et destinée à garder une attention particulière ;
* Sensibilisation accueil client – dédiée aux personnels du client en séjour longue durée sur un site français afin d’expliquer les règles qui leurs seraient appliquées.

## Eléments matériels

Un fois les catégories de personnels déterminées (§3.4), l’industriel ☞ doit déterminer les règles d’accès applicables à ces différentes catégories :

* Dispositions d’accès aux locaux (§3.1) ;
* Dispositions d’accès aux moyens informatiques ;
* Règles d’accès à l’information, en fonction de la nature des informations manipulées telles que définies au paragraphe §3.2.
* Par rapport aux différents outils informatiques identifiés (§3.2), l’industriel ☞ doit déterminer et préciser ici les dispositions de sécurité opportunes :
* Identification / authentification ;
* Contrôle d’accès logique ;
* Journalisation ;
* Infrastructures de gestion des clés cryptographiques ;
* Signaux compromettants.

## Dispositions spécifiques concernant la reproduction, l’enregistrement, le stockage, l’archivage ou la destruction des données

L’industriel peut indiquer dans cette rubrique les dispositions spécifiques à l’opération qu’il appliquera ou fera appliquer à un tiers concernant la reproduction, l’enregistrement, le stockage, l’archivage ou la destruction des données.

Ces dispositions ne peuvent être en contradiction avec le code de la défense (notamment en terme de durée minimale d’archivage des preuves liées aux exportations) et les exigences de l’IGI 1300.

L’industriel précisera pour ces dispositions qui fait quoi, et qui doit autoriser quoi.

## Mesures de surveillance

Certains évènements redoutés peuvent voir leur probabilité d’apparition s’élever en fonction de « facteurs de risque » qu’il est possible de suivre dans un tableau de bord. Par exemple, le risque de voir une personne étrangère à l’entreprise pénétrer dans un local non autorisé devient plus important si le nombre d’autorisation d’accès augmente.

L’industriel peut indiquer dans cette rubrique les indicateurs permettant d’apprécier les facteurs de risque, les niveaux d’alerte qui doivent déclencher une mesure complémentaire, et la nature de cette mesure.

## Dispositions pour lutter contre certaines catégories particulières de risques techniques

L’inventaire de ces dispositions peut être adapté en tant que de besoin.

* Préciser la (ou les) fiche d’analyse de risque où est analysé le scénario de risque correspondant.

### Compromission technique

La compromission technique définit la capacité qu’aurait un tiers de disposer, directement ou indirectement, d’informations techniques sur le matériel équipant les forces armées françaises, lesquelles lui permettraient d’en réduire l’efficacité ou d’élaborer une parade.

L’industriel ☞ doit alors présenter les dispositions qu’il prend afin de se protéger contre les risques identifiés de compromission technique, par exemple lors de mouvements de matériels ou lors de la communication à un tiers de documentation technique, de résultats d’études, d’un savoir-faire de conception ou de fabrication, etc.

### Rétro-ingénierie

La retro-ingénierie désigne la possibilité qu’aurait un tiers d’acquérir un savoir-faire non prévu au titre de l’opération par le biais d’une étude approfondie d’un matériel ou d’un logiciel mis à sa disposition et lui permettant ainsi d’accéder à des informations relatives à son fonctionnement et/ou sa méthode de fabrication. La rétro-ingénierie a généralement pour conséquence l’arrivée sur le marché, à un cout réduit et dans des délais limités, d’un concurrent. La rétro-ingénierie peut également engendrer une compromission technique.

L’industriel ☞ doit alors décrire les dispositions qu’il applique afin de se prémunir des risques identifiés de rétro-ingénierie.

### Détournement de matériel

La notion de détournement de matériel exprime la possibilité qu’aurait un tiers (notamment le client) d’utiliser certains sous-systèmes pour les adapter sur d’autres matériels à l’insu de l’industriel exportateur.

Dans l’hypothèse d’un transfert de fabrication, il est ainsi possible d’imaginer un détournement d’autodirecteurs ou de centrales inertielles afin de les intégrer sur un matériel indigène, notamment grâce aux informations techniques obtenues directement ou indirectement.

L’industriel ☞ doit alors indiquer les dispositions qu’il a retenues afin de se protéger contre les risques identifiés de détournement de matériel.

### Transmission de logiciels

L’industriel ☞ doit indiquer les dispositions prises pour assurer que les logiciels transmis correspondent à la version approuvée à cette fin.

# Suivi de l’application du PASI

Toute disposition génère par elle-même des risques :

* Qu’elle ne soit pas appliquée ;
* Qu’elle ne soit pas pertinente (efficacité, efficiente) ;
* Qu’elle ne soit plus adaptée dans un contexte ayant évolué.

## Contrôles internes

L’industriel ☞ doit procéder à intervalles réguliers à des vérifications concernant la bonne application du PASI par les opérationnels. Les vérifications portent sur la conformité du programme à l’organisation planifiée (§2 et §3), ainsi que sur la bonne application des dispositions de réduction de risque (§5).

Ces missions d’audit ou de contrôle interne, dont la périodicité ne doit pas dépasser les deux ans, doivent faire l’objet d’un plan de contrôle et doivent être formalisées.

* Décrire les conditions de déclenchement des audits et leur organisation.

## Réévaluation des risques

En parallèle, l’industriel ☞ doit suivre l’évolution des risques, en s’assurant périodiquement :

* Que l’analyse qui a été faite d’un risque (en termes notamment de probabilité mais également d’impact) reste d’actualité.
* Que les dispositions de réduction de risque sont pertinentes.
* Décrire les conditions des revues des risques et leur organisation (si ce n’est fait au titre de l’analyse des risques). L’industriel décrira ici son processus de réévaluation (disposition et fréquence de déclenchement, dispositions de suivi) applicable à l’opération objet du PASI.

Pour rappel, l’apparition d’un nouveau risque ou la nécessité de modifier des dispositions ☞ doit engendrer à terme une mise à jour du PASI et son approbation. En cas d’urgence, s’il y a péril en la demeure, l’industriel se limitera dans un premier temps à en faire mention dans un compte-rendu immédiat, et mettra immédiatement en application les dispositions nécessaires sans en attendre l’approbation.

## Comptes rendus

L’industriel ☞ doit rédiger un compte-rendu annuel présentant au minimum :

* Un état d’avancement de l’opération sur l’année écoulée ;
* Les principaux changements d’identité des personnels (responsables de l’opération et de la mise en œuvre du PASI) ;
* Une actualisation du planning de l’opération pour l’année à venir (principales échéances, évènements critiques vis à vis du PASI et de son analyse de risque, etc.) ;
* Un état des lieux des contrôles et audits menés dans le cadre du PASI et une synthèse des constatations et des plans d’action ;
* Une synthèse des incidents constatés dans le cadre de l’application du PASI et des suites données.

Ce compte-rendu doit impérativement être diffusé au service en charge des PASI (DGA/DI/SPEM/SDCE/BLGC), au plus tard fin Janvier de chaque année.

Il est exigé même pour les opérations faisant l’objet d’un suivi particulier par un directeur d’opération export (DOE) ou par un comité de suivi mandaté par l’administration : Comité de suivi technique (CST), organisme de suivi de programme et de l’exportation du système (OSPES), etc.

# Annexe : Fiches d’analyse de risque

L’industriel ☞ doit répertorier les risques liés à l’opération qu’il a isolés lors de son analyse des risques.

Afin de faciliter la lecture du PASI, les fiches d’analyse de risque sont regroupées en annexe (à raison d’une nouvelle page par fiche).

Les fiches :

* Identifient le risque (numéro du risque, libellé du risque, …) ;
* Précisent le scénario de référence utilisé pour l’évaluation du risque ;
* Justifient de l’évaluation de la criticité avant action de réduction ;
* Indiquent les actions de réduction de criticité applicables (Chapitre 5) ;
* Justifient de l’évaluation de la criticité après action de réduction.

L’industriel les synthétise sous la forme d’un tableau récapitulatif en section §4.4.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Fiche d’analyse de risque | | *A priori* | | | Après réduction | | |
| N° | Libellé | P | G | C | P | G | C |
|  |  |  |  |  |  |  |  |

## Description du scénario

À partir d'un événement redouté, la première étape nécessaire pour caractériser quantitativement un risque sera de formaliser le scénario de référence dont on parle, dans la fiche d’analyse de risque.

En lien avec les éléments présentés dans le PASI, les fiches décrivent le scénario de référence servant de base à l’évaluation :

* Préciser la nature de l’événement redouté ;
* Préciser les circonstances en tant que de besoin les éléments pertinents du ***contexte*** dimensionnant la criticité : entité impliquée au sein du montage contractuel (§1.2), phase (§1.3), site (§3.1), catégorie de personnel (§3.2), type d’information et voie de transmission (§3.3), etc.
* Déroulement du scénario : Comment les choses s'enchaînent-elles pour que le risque se manifeste? Dysfonctionnements, contrôles inefficaces, … ?
* Résultat typique : Situation après le déroulement du scénario et les actions correctives éventuelles.

Le cas échéant, le scénario rappelle les dispositions générales de l’entreprise ayant un impact dimensionnant sur le scénario.

## Caractérisation du scénario

* Périmètre concerné (& taille) : Dans quel situation le problème se manifeste-t-il? Est-ce une situation générique ou spécifique à une activité? Quelle est la taille de la population concernée : nombre de personnel, de locaux, de documents, ...
* Contexte (& fréquence) : Dans le périmètre concerné, la situation à risque se présente-t-elle fréquemment?
* Facteurs additionnels de risque : Qu'est-ce qui peut faciliter l'incident?

## Analyse du risque

L’industriel ☞ doit appliquer la méthode d’évaluation décrite en §4.3 par rapport au scénario proposé.

## Disposition de réduction

En complément aux dispositions généralement applicables dans l’entreprise, l’industriel ☞ doit identifier les dispositions propres à l’opération nécessaires pour réduire les risques jugés trop critiques. Les dispositions généralement applicables pour une opération peuvent être, typiquement :

* Méthodologie : y a-t-il un changement d’approche dans l’organisation de l’opération susceptible de faire diminuer la criticité ?
* Eléments matériels : gestion de droits d’accès, séparation physique des informations, firewall, …
* Formation, sensibilisation, responsabilité : les acteurs du processus se sont-ils suffisamment approprié la méthode, les objectifs, et les facteurs de risques? Les profils et compétences sont-ils adaptés à la maîtrise du processus? La manière de procéder est-elle connue et appliquée?
* Contrôle : outre le suivi général de l’application du PASI (§6), quels sont les indicateurs qui permettent de déceler une dégradation de la situation et une augmentation du risque? Sont-ils suivis, avec quelle fréquence, quel formalisme, …?
* Présenter le numéro de disposition, son intitulé (la description de la disposition sera transférée au chapitre §5).
* Pour la bonne lecture des fiches d’analyse de risque, les dispositions doivent être numérotées de manière cohérente (section, sous-section où elles apparaissent et numéro à suivre).
* Préciser la réduction de probabilité (ou de gravité) qu’elle apporte.

Note : Il est rare qu’une disposition fasse varier la gravité d’un évènement redouté.

# Note sur l’évaluation des probabilités

Il est très difficile d’évaluer globalement la probabilité d’occurrence de scénarios peu vraisemblables, avec une précision suffisante pour faire autre chose que du « doigt mouillé ».

Pour une approche relativement objective de cette évaluation, il est nécessaire d’avoir une approche structurée de l’évaluation. Avec des personnes ayant une expérience pratique de la situation à risque, il faudra par exemple :

* Convenir du « scénario catastrophe » le plus vraisemblable conduisant à l’évènement redouté, en fonction des « facteurs de risque » susceptibles d’intervenir,
* Et en estimer la vraisemblance de chaque étape.

La méthode suivante peut servir de guide, la méthode effectivement retenue restant de la responsabilité de l’industriel :

**Ordres de grandeur des probabilités et des nombres de points à risque**

Les classes de probabilité peuvent se fonder sur un tableau de ce type, où une ligne sur la « vraisemblance » reflète l’ordre de grandeur de la probabilité.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Classe** | **Impossible** | **Improbable** | **Possible** | **Incertain** | **Probable** |
| **Probabilité** | <0.2 % | 0.2 à 1 % | 1 à 5% | 5 à 20 % | >20 % |
| **Cotation** | 0 | 1 | 2 | 3 | 4 |
| **Vraisemblance** | -4 | -3 | -2 | -1 | 0 |

De même, par rapport au déroulement d’un scénario sur un cas, la probabilité d’apparition sera d’autant plus forte que le nombre de situations où le cas peut se présenter est important : si la probabilité sur un « cas » (personne, local, document, enregistrement, …) est donnée, la probabilité sur cent « cas » du même type sera deux ordres de grandeur plus forte.

Ainsi, si le problème peut se présenter sur une centaine de locaux (102) l’ordre de grandeur du nombre de points à risque est 2, si les échanges comportant un risque portent sur trois mille courriers l’ordre de grandeur est de l’ordre de 3,5, etc.

**Evaluation d’un scénario à risque**

L’analyse d’un scénario peut alors se faire par étape, en décomposant un évènement redouté en différents facteurs de risque (et généralement, en étant « légèrement pessimiste »). Par exemple, la discussion pourra conduire à construire le tableau suivant, qui peut se reporter directement dans la fiche :

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Etape** | **Classe** | **V** | **Disposition** | **ΔV** |
| Une personne fait un malaise au travail pendant la durée de l’opération | Possible | -2 |  |  |
| Elle quitte son poste en urgence et laisse le bureau ouvert et la session en cours | Probable | 0 | R17 | -1 |
| Une personne étrangère au service passe dans le couloir pendant cette absence | Incertain | -1 | R1 | -2 |
| La personne cherche à récupérer de l’information intéressant sa partie | Possible | -2 |  |  |
| Sachant qu’il y près de trois cent postes de travail où ce problème peut se poser | 3.102 | +2,5 |  |  |
| **… ce scénario est jusqu’ici, au total,** | **Improbable** | **-2,5** | **Impossible** | **-5,5** |

Dans cette méthode d’évaluation collective et experte, rien n’interdit de faire une moyenne des estimations : si par exemple un expert juge un évènement « possible » et l’autre « improbable », sa cotation peut être fixée à -2,5. Ce qui est important est l’ordre de grandeur.

L’explicitation du scénario permet également de s’assurer que celui-ci est bien celui qui conduit le plus probablement à l’évènement redouté. Ici, on peut par exemple discuter de ce que trouver « bureau ouvert et session en cours » se rencontre plus fréquemment lorsqu’une personne se rend aux toilettes, mais l’état critique dure alors moins longtemps – l’un dans l’autre le risque est probablement du même ordre de grandeur.

**Dispositions de réduction du risque**

L’explicitation des étapes dimensionnantes du scénario permet d’identifier des dispositions de réduction du risque susceptibles d’avoir un impact direct et de réduire la probabilité du scénario.

* Dans l’exemple précédent, une sensibilisation à ne jamais laisser sa porte et sa session ouverte (disposition dite « R17 ») peut bloquer le scénario, mais sans renforcement actif cette disposition est d’application plutôt « incertaine » (-1).
* Dans un autre ordre d’idée, la disposition consistant à faire accompagner toute personne étrangère au service par une personne habilitée (disposition « R1 ») peut également bloquer le scénario, même si sa non-application reste « possible » (-2).
* Les dispositions consistant par exemple à surveiller la santé des collaborateurs (en vue d’une réduction de l’étape 1) ou à faire des enquêtes d’habilitation des visiteurs (étape 4) ne paraissent pas présenter un rapport coût/performance satisfaisant.

Au total, la superposition de ces deux dispositions simples et économiques fait passer la vraisemblance d’ensemble à -6, permettant de qualifier ce scénario de tout à fait « impossible ».

**Rattachement à l’organisation de l’opération**

Comme souligné précédemment, un changement dans l’organisation de l’opération peut également être une solution envisageable. Si au lieu de laisser l’accès à l’information sensible sur les trois cent postes (+2,5) on en limite l’accès à la dizaine où elle est réellement utile (+1), le scénario devient également « impossible » (-4) – mais ceci de manière plus discutable, il pourrait n’être que « improbable ».

Sauf précision contraire, un risque peut *a priori* se présenter dans tous les locaux de l’opération, pour tous les collaborateurs, à tout instant, sur toutes les classes d’informations sensibles, pour tous les documents gérés, sur toutes les parties du matériel, etc. C’est à ce niveau que les éléments pertinents du contexte dimensionnant la criticité sont discutés et identifiés, et permettent d’objecter que l‘ordre de grandeur du nombre de « cas », c’est-à-dire là où le problème est susceptible de se poser, est moindre que ce périmètre maximisant : quelles sont réellement les locaux où une information sensible est accessible, quelles sont les personnes qui y ont accès, etc.

* Ces facteurs organisationnels qui permettent de mieux cerner les risques sont ceux qu’il est nécessaire de présenter au titre de l’organisation de l’opération.
* Inversement, si un détail n’a pas d’influence notable sur l’analyse des risques, il est inutile (sauf demande en ce sens) de le mentionner dans un Plan d’Assurance de la Sécurité des Informations, dont l’unique objet est de documenter la maîtrise de ces risques.

1. Article L2332-1 du code de la défense. [↑](#footnote-ref-1)
2. Articles R. 2311-2 et suivants du code de la défense et nouvelle instruction générale interministérielle n° 1 300 du 9 août 2021. [↑](#footnote-ref-2)
3. CIEEMG (Décret n°55-965 du 16 juillet 1955). [↑](#footnote-ref-3)
4. À des fins de simplification, le terme exportation utilisé dans ce document vise à la fois les exportations et les transferts. [↑](#footnote-ref-4)
5. Arrêté du 27 juin 2012 modifié, relatif à la liste des matériels de guerre et matériels assimilés soumis à une autorisation préalable d'exportation et des produits liés à la défense soumis à une autorisation préalable de transfert. Voir pour plus de précisions le guide du classement ML sur armement.defense.gouv.fr. [↑](#footnote-ref-5)
6. À cet effet, consulter les recommandations publiées par la direction générale de l’armement concernant les échanges de technologies soumises à contrôle. [↑](#footnote-ref-6)
7. Articles L.2335-3 et L.2339-11-1 sanctionnant le non-respect des termes d’une licence d’exportation, ou articles L.2335-10 et L.2339-11-1 sanctionnant le non-respect des termes d’une licence de transfert (cinq ans d’emprisonnement et amende de 75 000 euros). [↑](#footnote-ref-7)
8. Certains industriels exportateurs ont rédigé plus d’une dizaine de ces documents. [↑](#footnote-ref-8)
9. Le rédacteur doit donc s’assurer que les informations contenues en son sein ne relèvent pas d’un niveau de classification supérieur. Si nécessaire, prendre contact avec DGA/DI/SPEM/SDCE/BLGC (adresse fonctionnelle : dga-di-blgc.contact.fct@intradef.gouv.fr). [↑](#footnote-ref-9)
10. De préférence par voie dématérialisée, encrypté par le logiciel Zed! ou Acid. Par courrier électronique les documents sont à transmettre à [dga-di-blgc.contact.fct@intradef.gouv.fr](mailto:dga-di-blgc.contact.fct@intradef.gouv.fr) [↑](#footnote-ref-10)
11. Arrêté du 30 novembre 2011 modifié, article 4 : les [contrôleurs sur place] peuvent […] demander aux titulaires des autorisations […] tous les documents, quel qu'en soit le support, dont ils jugent la production utile à l'exécution du contrôle […] notamment […] les pièces justifiant le respect des conditions et restrictions précisées dans les licences […]. [↑](#footnote-ref-11)
12. Les prestataires travaillant pour le compte de l’industriel exportateur au titre d’un contrat type ESI ne sont pas considérés comme sous-traitants mais comme personnels de la société. Il s’agit essentiellement, sauf cas particulier, de sous-traitance externe. [↑](#footnote-ref-12)
13. Par extension, le PASI peut également traiter d’informations de type « confidentiel industrie », ou tout autre type de confidentialité non soumises à contrôle réglementaire, mais dont la protection doit être assurée dans le cadre de l’opération. [↑](#footnote-ref-13)
14. Par exemple : donnés utilisées par un *back office* afin de préparer des réponses filtrées destinées à un partenaire du programme. [↑](#footnote-ref-14)