MINISTÈRE
DES ARMÉES
Liberté
Égalité
Fraternité

Direction générale
de l'armement

Guide de rédaction d'un Plan d'Assurance de la Sécurité des Informations (PASI)

Edition 4.1 du 12 septembre 2022

DGA

Introduction générale

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].

À l'exportation[2], une procédure spéciale 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 CIEEMG[3].

Depuis 2010, les transferts de technologies prennent une part croissante des opérations soumises à contrôle des exportations. Contrôlés au titre des catégories ML21, ML22, AMA3 et AMA4[4], ce type d'exportation est susceptible de s'effectuer par des voies dites « intangibles » ou « dématérialisées », ce qui les font échapper aux contrôles traditionnels menés par les douanes. Il appartient alors à l'industriel exportateur de mettre en place une organisation et des moyens adéquats[5] pour assurer le respect de ses obligations, à la fois vis à vis des procédures d'exportations et du contenu de la licence.

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 sur la réalisation de l'opération, afin d'y apporter des garanties complémentaires.**

[1] Article L2332-1 du code de la défense.
[2] À des fins de simplification, le terme exportation utilisé dans ce document vise à la fois les exportations et les transferts.
[3] Commission Interministérielle pour l'Etude des Exportations de Matériels de Guerre (Décret n°55-965 du 16 juillet 1955).
[4] 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.
[5] À cet effet, consulter les recommandations publiées par la direction générale de l'armement concernant les échanges de technologies soumises à contrôle.

Sommaire

Introduction au plan d'assurance de la sécurité des informations (PASI)

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. Cinq thèmes majeurs sont attendus dans un PASI :

- **Une présentation détaillée de l'opération** ;
- **Une présentation des acteurs déployés** par l'industriel exportateur **en matière de sécurité de défense et de contrôle des exportations**, en particulier dans le cadre de l'opération ;
- **Une analyse des risques liés aux échanges de technologies soumises à contrôle dédiée à l'opération** ;
- **Une description des mesures prises** par l'industriel exportateur **afin de réduire les risques identifiés préalablement pour l'opération** ;
- **Une description des mesures prises** par l'industriel exportateur **afin de lui permettre de suivre l'adéquation entre l'analyse de risque et l'opération** tout au long de la durée de celle-ci.

Les PASI sont à transmettre[6] au bureau des licences globales et 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**) pour étude. Ce bureau, après éventuelle consultation d'autres services[7], se chargera de revenir vers l'industriel **en acceptant le plan d'assurance de la sécurité des informations, ou en transmettant une fiche de remarque**.

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.

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[8] sont susceptibles d'auditer la stricte application du PASI par l'industriel exportateur. Il appartient donc à l'industriel exportateur de s'assurer de sa capacité à démontrer qu'il respecte les mesures du plan d'assurance de la sécurité des informations qui a été accepté.

Il est rappelé qu'aucune exportation d'information ne peut avoir lieu tant que le PASI n'a pas été accepté, et que les mesures listées ne sont pas mises en œuvre[9].

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[10].

[6] De préférence par voie dématérialisée.
[7] Le directeur d'opération export (DOE) en lien avec l'opération ou le service de la sécurité de défense et des systèmes d'information (DGA/SSDI) par exemple.
[8] L'industriel exportateur en sera alors informé par le bureau des licences globales et générales et du contrôle sur place (DGA/DI/SPEM/SDCE/BLGC).
[9] Attention, certaines licences peuvent être soumises à des conditions particulières, avec par exemple l'approbation du document au moment de la signature du contrat.
[10] 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).

Exigences concernant le formalisme d'un plan d'assurance de la sécurité des informations (PASI)

Le plan d'assurance de la sécurité des informations (PASI) est un document de niveau « Diffusion Restreinte Spécial France »[11]. Le PASI prévoit que certaines de ses mesures 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).

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 indentification aisée[12] 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, à savoir :

- Le responsable de l'opération ;
- Le responsable de la sécurité de défense 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 mesures prescrites (M01 par exemple) afin de faciliter leur identification.

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, leur apport doit faire l'objet d'une description complète : 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.

[11] 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.
[12] Certains industriels exportateurs ont rédigé plus d'une dizaine de ces documents.

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 de vous orienter dans votre rédaction.

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.

Cette trame peut être adaptée par le rédacteur, notamment s'il est nécessaire, pour la bonne compréhension du sujet par le lecteur, de présenter dans le PASI des éléments complémentaires. D'autre part, en fonction des particularités de l'opération, des exigences particulières peuvent conduire à des mesures spécifiques, qui sont alors couvertes par des sections dédiées.

Chapitre 1 : L'opération
1.1 Périmètre de l'opération
1.2 Planning général de l'opération
1.3 Historique des contrats de l'opération
1.4 Licences délivrées
1.5 Identification et présentation des sites opérationnels en France
1.6 Identification et présentation des sites opérationnels à l'étranger
1.7 Identification des informations soumises à contrôle manipulées dans le cadre de l'opération

Chapitre 2 : Organisation contrôle export et sécurité de défense
2.1 Organisation du contrôle des exportations de l'entreprise
2.2 Organisation du contrôle des exportations dédiée à l'opération
2.3 Organisation de la sécurité de défense de l'entreprise
2.4 Organisation de la sécurité de défense dédiée à l'opération
2.5 Identification des profils spécifiques PASI mis en place pour l'opération

Chapitre 3 : Analyse des risques
3.1 Gestion des risques
3.2 Identification et évaluation des risques liés à l'opération

Chapitre 4 : Mesures pour lutter contre la transmission non autorisée d'information
4.1 Identification des personnels
4.2 Sensibilisation et formation du personnel
4.3 Locaux dédiés au projet
4.4 Identification des moyens informatiques utilisés dans le cadre de l'opération
4.5 Identification des outils et systèmes d'information utilisés dans le cadre de l'opération
4.6 Processus de transmission des informations soumises à contrôle
4.7 Règles spécifiques concernant la reproduction, l'enregistrement, le stockage, l'archivage ou la destruction des données

Chapitre 5 : Mesures pour lutter contre certaines catégories particulières de risques techniques
5.1 Mesures pour lutter contre la compromission technique
5.2 Mesures pour lutter contre la rétro-ingénierie
5.3 Mesures pour lutter contre le détournement de matériel

Chapitre 6 : Suivi de l'application du PASI
6.1 Gestion des incidents
6.2 Contrôles internes
6.3 Comptes rendus

Chapitre 1 : L'opération

1.1 Périmètre de l'opération

L'industriel doit décrire précisément l'objet de l'opération concernée, en faisant ressortir les domaines concernés par le PASI. Il est indispensable, afin de garantir une bonne compréhension de l'opération, que le périmètre de l'opération présente :

- Le schéma commercial et contractuel complet de l'opération ;
- Les différents acteurs (client final, partenaire industriel, sous-traitant[13], etc.) ;
- La finalité industrielle et technique (formations prévues, assistance à la conception, transfert de fabrication, etc.) ;
- Le périmètre exact couvert par le PASI (notamment pour les programmes complexes avec plusieurs PASI).

1.2 Planning général de l'opération

L'industriel doit présenter une chronologie de son 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.

1.3 Historique des contrats de l'opération

L'industriel doit 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.

1.4 Licences délivrées

L'industriel doit lister et décrire succinctement les licences qu'il a obtenues et qui ont eu pour conséquence la rédaction du PASI. 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.

1.5 Identification et présentation des sites opérationnels en France

L'industriel doit préciser la liste des sites situés sur le territoire français qui seront impactés par l'opération ainsi que leur niveau de protection (niveau d'habilitation, qualité de PIV[14], présence de ZRR[15], etc.). Il doit également indiquer, pour chacun des sites relevés, le type d'activité qui y sera réalisé et les conséquences vis à vis du PASI.

1.6 Identification et présentation des sites opérationnels à l'étranger

L'industriel doit lister les sites situés à l'étranger sur lesquels se déroulera l'opération. Pour chacun des sites énumérés, l'industriel devra indiquer le résident, le type d'activité qui y sera réalisé et les conséquences vis à vis du PASI.

1.7 Identification des informations soumises à contrôle manipulées dans le cadre de l'opération

En lien avec l'identification des moyens informatiques (§4.4), des outils (§4.5) et des canaux de transmission (§4.6) de l'information, l'industriel doit répertorier les types d'informations soumises à contrôle qui seront manipulées dans le cadre de l'opération.

---

[13] 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.

[14] Point d'Importance Vitale.

[15] Zone à Régime Restrictif.

Par manipulation, il est entendu les informations soumises à contrôle qui seront :

- Exportées vers les partenaires de l'opération ;
- Utilisées ou potentiellement utilisables par l'équipe programme dans son environnement[16].

Par type d'informations soumises à contrôle, il est entendu que soient listés les niveaux de protection et de confidentialité des informations manipulées (Non protégé, Diffusion restreinte, Secret, Très Secret, etc.) ainsi que la présence de marquage particulier (Spécial France, etc.).

[16] Par exemple : donnés utilisées par un *back office* afin de préparer des réponses filtrées destinées à un partenaire du programme.

Chapitre 2 : Organisation contrôle export et sécurité de défense

2.1 Organisation du contrôle des exportations de l'entreprise

L'industriel doit décrire 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.

2.2 Organisation du contrôle des exportations dédiée à l'opération

L'industriel doit préciser 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. Les responsabilités en terme de sensibilisation et de formation doivent être listées.

2.3 Organisation de la sécurité de défense de l'entreprise

L'industriel doit décrire son organisation générale en terme de sécurité 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.

2.4 Organisation de la sécurité de défense dédiée à l'opération

L'industriel doit préciser 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. Les responsabilités en terme de sensibilisation et de formation doivent être listées.

2.5 Identification des profils spécifiques PASI mis en place pour l'opération

L'industriel doit lister les fonctions spécifiques créées au sein de l'équipe programme en conséquence de la mise en place du PASI, et 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.

Chapitre 3 : Analyse des risques

3.1 Gestion des risques

L'industriel doit développer son processus d'analyse des risques dédiés à l'opération, en précisant notamment :

- Le responsable du processus ;
- Les acteurs impliqués ;
- La méthode d'analyse de risque utilisée ;
- Les conditions et l'organisation des revues des risques[17].

3.2 Identification et évaluation des risques liés à l'opération

L'industriel doit répertorier les risques[18] liés à l'opération qu'il a isolés lors de son analyse des risques. Dans le cadre du PASI, il faut entendre par risque tout événement dont la survenance est susceptible d'entrainer ou faciliter l'obtention par un opérateur étranger d'informations ou de capacités soumises à contrôle, autres que celles autorisées par la licence.

Ainsi, 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. Les grandes familles de risques[19] identifiables sont notamment :

- La transmission non autorisée d'information soumise à contrôle ;
- La transmission non autorisée d'information sensible[20] ;
- La compromission technique ;
- La rétro-ingénierie ;
- Le détournement de matériel ;
- La contamination d'information par la législation ITAR.

L'industriel doit indiquer la logique utilisée pour estimer la criticité des risques sous la forme d'une matrice. Quatre à cinq niveaux doivent être retenus afin de quantifier la probabilité et la gravité.

Pour chacun des risques redoutés, une fiche d'analyse de risque doit être créée. Chaque risque est ensuite évalué selon la méthode choisie, avant et après la mise en place de mesures adaptées (nomination d'un pilote et application des mesures prévues aux chapitres 4 et 5).

Afin de faciliter la lecture du PASI, les fiches d'analyse de risque sont annexées. L'industriel les synthétise sous la forme d'un tableau récapitulatif (numéro du risque, libellé du risque, criticité avant action de réduction, criticité après action de réduction, contexte, etc.).

[17] Pour rappel, l'apparition d'un nouveau risque lors d'une revue doit engendrer une mise à jour du PASI et son approbation.
[18] Un risque est un événement futur, incertain, ne dépendant pas exclusivement de la volonté des parties et dont la manifestation est susceptible d'engendrer des dommages.
[19] Liste non exhaustive.
[20] Telle que définie par l'IGI 1300.

Chapitre 4 : Mesures pour lutter contre la transmission non autorisée d'information

Les « mesures » décrites ici, numérotées, sont les mesures spécifiques prises pour réduire les risques identifiés en §3.2. Les mesures générales à caractère permanent sont décrites dans le chapitre 2.

4.1 Identification des personnels

L'industriel doit lister les différentes catégories de personnels impliqués dans l'opération, soit au minimum :

- Les personnels du programme ;
- Les personnels de la société ;
- Les personnels du client ou du partenaire industriel ;
- Les personnels d'éventuels sous-traitants.

Un fois les catégories de personnels déterminées, la société déterminera les **règles d'accès à l'information**, en fonction de la **nature des informations** manipulées telles que définies au paragraphe 1.7.

4.2 Sensibilisation et formation du personnel

La sensibilisation et la formation des employés doivent être réalisées lors de séances qui feront l'objet d'un émargement par les personnes conviées. En complément de l'émargement, un engagement de responsabilité concernant l'application des règles énumérées dans le PASI sera signé par les personnels ayant suivi une formation. Un suivi de ces personnels doit être tenu (traçabilité, date, etc.) et un responsable des sensibilisations/formations doit être identifié[21]. Il est convenu qu'un personnel ne peut avoir une interaction avec le client sans qu'il ait été au moins sensibilisé.

L'industriel listera les sensibilisations et formations obligatoires à toutes personnes en contact avec le client, qu'elles soient ou non directement liés au projet, et indiquera pour celles-ci les différentes catégories de personnels concernés[22]. Pour chacune des sensibilisations et formations, figurera un récapitulatif des objectifs. 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.

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

- Sensibilisation PASI et contrôle export – dédiée à tous les membres du projet 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.

4.3 Locaux dédiés au projet

L'industriel doit détailler les locaux utilisés dans le cadre de l'opération, à la fois en France et à l'étranger[23], en tenant compte de l'aspect sûreté.

En France, il précisera les locaux utilisés par les équipes projet et ceux fréquentés ou susceptibles d'être fréquentés par le client. Il définira les modalités d'accès aux différents locaux par le client (badges, plage horaire, circuit de notoriété, accompagnement, etc.). Les caractéristiques des locaux utilisés par le client doivent également être listées (capacité d'accéder aux réseaux, interdiction de tout appareil permettant une prise de vue, etc.).

À l'étranger, il indiquera les modalités d'accueil de ses équipes et prendra en compte son degré d'autonomie sur chacun des sites. Il est généralement convenu qu'un hébergement longue

[21] Cf. paragraphe 2.5.
[22] En cohérence avec les paragraphes 2.5 et 4.1.
[23] En cohérence avec les sites identifiés dans les paragraphes 1.5 et 1.6.

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, il listera les dispositions prises afin d'assurer la sécurité de ses personnels et des informations détenues.

4.4 Identification des moyens informatiques utilisés dans le cadre de l'opération

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

- Les réseaux accessibles au client (réseau de l'entreprise, réseau dédié au projet, etc.) ;
- 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.).

4.5 Identification des outils et systèmes d'information utilisés dans le cadre de l'opération

L'industriel doit présenter les outils et systèmes d'information déployés dans le cadre de l'opération et mis à disposition des personnels extérieurs à la société, en indiquant pour chacun d'entre eux leurs caractéristiques (architecture, responsabilités, règles d'accès, etc.).
Il doit également décrire de la même manière les réseaux et outils client/partenaire qu'il utilisera.

4.6 Processus de transmission des informations soumises à contrôle

L'industriel doit identifier les canaux de transmission des informations soumises à contrôle prévus dans le cadre de l'opération, que ceux-ci utilisent une voie dématérialisée ou matérielle. Aucune dérogation aux canaux identifiés dans le PASI ne peut être tolérée pour la transmission d'informations soumises à contrôle.
Pour chacun des canaux, elle expliquera les processus retenus 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.

Les situations suivantes[24] 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 ;
- Messagerie électronique ;
- Communications téléphoniques ;
- Réunion ou vidéoconférence ;
- Formation ;
- Plateau de travail collaboratif.

4.7 Règles spécifiques concernant la reproduction, l'enregistrement, le stockage, l'archivage ou la destruction des données

L'industriel peut indiquer dans cette rubrique les règles 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 règles 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.

[24] Liste non exhaustive, répertoriant les principaux canaux actuellement utilisés.

Chapitre 5 : Mesures pour lutter contre certaines catégories particulières de risques techniques

Les « mesures » décrites ici, numérotées, sont les mesures spécifiques prises pour réduire les risques identifiés en §3.2. Les mesures générales à caractère permanent sont décrites dans le chapitre 2.

5.1 Mesures pour lutter contre la 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 présenter les mesures 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.

5.2 Mesures pour lutter contre la 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 décrire les mesures qu'il applique afin de se prémunir des risques identifiés de rétro-ingénierie.

5.3 Mesures pour lutter contre le 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 indiquer les mesures qu'il a retenues afin de se protéger contre les risques identifiés de détournement de matériel.

Chapitre 6 : Suivi de l'application du PASI

6.1 Gestion des incidents

L'industriel doit développer 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.

6.2 Contrôles internes

L'industriel doit décrire son processus d'audit dédié à l'opération objet du PASI. Il est tenu de procéder à intervalles réguliers à des vérifications concernant la bonne application du PASI par les opérationnels.

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. Ces missions ont notamment vocation à :

- Vérifier la mise en place et l'application des mesures définies par le PASI ;
- Suivre l'évolution des risques ;
- Vérifier la conformité aux réglementations nationales et internationales applicables à l'opération.

6.3 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 en début d'année civile au service en charge des PASI (DGA/DI/SPEM/SDCE/BLGC).

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[25].

[25] Comité de suivi technique (CST), organisme de suivi de programme et de l'exportation du système (OSPES), etc.

Annexe :

Afin de faciliter la lecture du PASI, les fiches d'analyse de risque sont annexées.

Les fiches :

- Identifient le risque (numéro du risque, libellé du risque, …) ;
- N lien avec les éléments présentés dans le PASI, précisent en tant que de besoin les éléments pertinents du contexte dimensionnant la criticité : entité impliquée au sein du montage contractuel (§1.1), catégorie de personnel (§4.1), site (§1.5, §1.6, §4.3), phase (§1.2), type d'information (§1.7), voie de transmission (§4.6), etc ;
- Justifient de l'évaluation de la criticité avant action de réduction ;
- Indiquent les actions de réduction de criticité applicables (Chapitre 4 et 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 3.2.