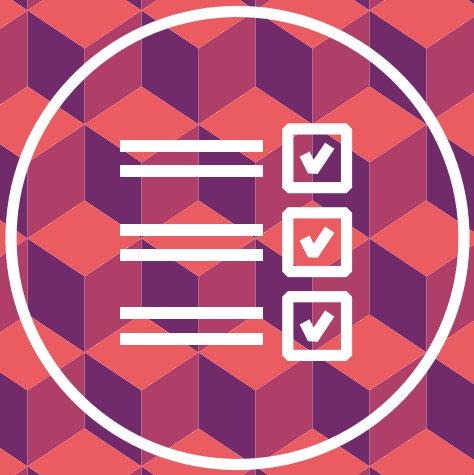
L'HOMOLOGATION DE SÉCURITÉ

en neuf étapes simples



AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION
ANSSI

Pourquoi l'homologation de sécurité ?

Lorsqu'un responsable (autorité administrative, élu, dirigeant d'entreprise) décide de faire déménager ses équipes dans de nouveaux locaux ou d'ouvrir un établissement recevant du public, il s'assure que les lieux sont conformes à la réglementation et que les bâtiments sont solides, afin que l'ensemble puisse fonctionner en toute sécurité pour les personnes et les biens. Il doit s'en assurer même s'il n'est pas un spécialiste de la construction et il s'appuie pour cela sur des garanties et des arguments portés à sa connaissance par des experts du domaine.

En matière d'informatique, l'homologation de sécurité joue le même rôle. Elle permet à un responsable, en s'appuyant sur l'avis des experts, de s'informer et d'attester aux utilisateurs d'un système d'information que les risques qui pèsent sur eux, sur les informations qu'ils manipulent et sur les services rendus, sont connus et maîtrisés. L'homologation est d'autant plus nécessaire, aujourd'hui, que les systèmes d'information sont de plus en plus complexes et que les impacts potentiels d'un incident sont de plus en plus graves.

La démarche d'homologation, recommandée depuis plusieurs années par l'Agence nationale de la sécurité des systèmes d'information (ANSSI), est donc un préalable à l'instauration de la confiance dans les systèmes d'information et dans leur exploitation.

Pour un certain nombre de systèmes, cette recommandation est rendue obligatoire par des textes, tels que l'instruction générale interministérielle n° 1300, le référentiel général de sécurité (RGS) et la politique de sécurité des systèmes d'information de l'État (PSSIE).

Qu'est-ce qu'une homologation de sécurité ?

En informatique, comme dans les autres domaines, le risque zéro n'existe pas. La démarche d'homologation de sécurité est destinée à faire connaître et faire comprendre aux responsables les risques liés à l'exploitation d'un système d'information.

Il s'agit d'un processus d'information et de responsabilisation qui aboutit à une décision, prise par le responsable de l'organisation. Cette décision constitue un acte formel par lequel il :

- atteste de sa connaissance du système d'information et des mesures de sécurité (techniques, organisationnelles ou juridiques) mises en œuvre ;
- accepte les risques qui demeurent, qu'on appelle *risques résiduels*.

La décision s'appuie sur l'ensemble des documents que le responsable estime nécessaire et suffisant à sa prise de décision.

La démarche d'homologation doit être adaptée aux enjeux de sécurité du système, notamment au contexte d'emploi, à la nature des données contenues, ainsi qu'aux utilisateurs :

- dans les cas de systèmes complexes ou à fort enjeu de sécurité, il est souhaitable que le responsable s'entoure d'experts techniques et fonctionnels (la commission d'homologation). Il peut déléguer la prise de décision à l'un de ses représentants qui présidera ce comité d'experts ;
- dans le cas de systèmes simples, le responsable peut mettre en place des procédures simplifiées associant un nombre plus limité d'acteurs.

Comment homologuer un système d'information ?

La démarche d'homologation peut être décomposée en neuf étapes, dont la mise en œuvre est directement liée à la complexité du système à homologuer.

Les questions posées lors de ces neuf étapes permettent de constituer un dossier, sur lequel l'autorité d'homologation s'appuie pour prendre sa décision.

Définition de la stratégie d'homologation

Étape n° 1 : Quel système d'information dois-je homologuer et pourquoi ?
Définir le référentiel réglementaire applicable et délimiter le périmètre du système à homologuer.

Étape n° 2 : Quel type de démarche dois-je mettre en œuvre ?
Estimer les enjeux de sécurité du système et en déduire la profondeur nécessaire de la démarche à mettre en œuvre.

Étape n° 3 : Qui contribue à la démarche ?
Identifier les acteurs de l'homologation et leur rôle (décisionnaire, assistance, expertise technique, etc.).

Étape n° 4 : Comment s'organise-t-on pour recueillir et présenter les informations ?
Détailler le contenu du dossier d'homologation et définir le planning.

Maîtrise des risques

Étape n° 5 : Quels sont les risques pesant sur le système ?
Analyser les risques pesant sur le système en fonction du contexte et de la nature de l'organisme et fixer les objectifs de sécurité.

Étape nº 6 : La réalité correspond-elle à l'analyse ?

Mesurer l'écart entre les objectifs et la réalité.

Étape nº 7 : Quelles sont les mesures de sécurité supplémentaires à mettre en œuvre pour couvrir ces risques ?

Analyser et mettre en œuvre les mesures nécessaires à la réduction des risques pesant sur le système d'information. Identifier les risques résiduels.

Prise de décision

Étape nº 8 : Comment réaliser la décision d'homologation ?

Accepter les risques résiduels : l'autorité d'homologation signe une attestation formelle autorisant la mise en service du système d'information, du point de vue de la sécurité.

Suivi a posteriori

Étape nº 9 : Qu'est-il prévu pour maintenir la sécurité et continuer de l'améliorer ?

Mettre en place une procédure de révision périodique de l'homologation et un plan d'action pour traiter les risques résiduels et les nouveaux risques qui apparaîtraient.

Table des matières

Objectifs de l'homologation de sécurité

En informatique, comme dans les autres domaines, le ***risque zéro*** n'existe pas.

L'objectif de la ***démarche d'homologation*** d'un système d'information (SI) est de trouver un équilibre entre le risque acceptable et les coûts de sécurisation, puis de faire arbitrer cet équilibre, de manière formelle, par un responsable qui a autorité pour le faire.

Cette démarche permet d'améliorer la sécurité pour un coût optimal, en évitant la « sur-sécurité », mais en prenant également en compte le coût d'un éventuel incident de sécurité. Elle permet de s'assurer que les risques pesant sur le SI, dans son contexte d'utilisation, sont connus et maîtrisés de manière active, préventive et continue.

La démarche d'homologation doit s'intégrer dans le cycle de vie du système d'information. Elle comprend plusieurs étapes clés, détaillées au sein du présent document. Il est nécessaire de les suivre en même temps que les phases de développement du système : opportunité, faisabilité, conception, réalisation, validation, exploitation, maintenance et fin de vie. En outre cette démarche doit être lancée suffisamment tôt, afin de pouvoir déterminer les exigences de sécurité qui seront intégrées dans les cahiers des charges de développement ou d'acquisition.

La ***décision d'homologation*** est le résultat du processus. Son objet est de vérifier que le responsable a analysé les risques de sécurité et a mis en œuvre les dispositifs adaptés à la menace.

Le terme « homologation » recouvre donc deux notions distinctes :

- **la démarche d'homologation**, avant tout destinée à faire connaître et faire comprendre aux responsables les risques liés à l'exploitation d'un système d'information. Elle se conclut par une décision, soutenue par la constitution et l'analyse d'un dossier de sécurité ;
- **la décision formelle d'homologation** (également appelée *attestation formelle*).

Se lancer dans une démarche d'homologation est relativement simple : il s'agit de vérifier que la sécurité n'a pas été oubliée avant la mise en place du système d'information et d'appliquer les mesures de sécurité nécessaires et proportionnées.

Les neuf étapes simples présentées dans ce document permettront à un chef de projet ou à un comité de pilotage SSI de préparer un dossier d'homologation et de le présenter au responsable, désigné *autorité d'homologation*.

L'autorité d'homologation pourra alors prendre une décision éclairée sur la base de ce dossier, qui doit apporter des réponses pertinentes à l'ensemble des questions qu'elle se pose.

étape n°

1

Quel système d'information dois-je faire homologuer et pourquoi ?

Durant la première étape, vous allez préciser le référentiel réglementaire applicable et délimiter le périmètre du système à homologuer.

1 . Préciser le référentiel réglementaire

La démarche d'homologation est recommandée depuis plusieurs années par l'Agence nationale de la sécurité des systèmes d'information (ANSSI). Pour un certain nombre de systèmes, cette recommandation est rendue obligatoire par :

- **l'instruction générale interministérielle n° 1300** (IGI 1300), pour les systèmes traitant d'informations classifiées de défense ;
- **le référentiel général de sécurité** (RGS), pour les systèmes permettant des échanges entre une autorité administrative et les usagers ou entre autorités administratives ;
- **la politique de sécurité des systèmes d'information de l'État** (PSSIE), pour les systèmes des administrations de l'État.

Il est indispensable de déterminer à quel titre le système d'information doit être homologué. En effet, même si la démarche d'homologation reste identique dans tous les cas, le référentiel réglementaire constitue un élément crucial pour la délimitation du périmètre et la constitution du dossier d'homologation.

2 . Délimiter le périmètre du système

Le périmètre du système d'information à homologuer doit comporter tous les éléments indispensables au fonctionnement du système. La délimitation du périmètre ne doit comporter aucune ambiguïté, car elle permet de déterminer et de caractériser précisément les systèmes qui seront homologués. La description de ce périmètre comprend :

- **des éléments fonctionnels et d'organisation :** fonctionnalités du système, type d'utilisateurs, contexte et règles d'emploi, procédures formalisées, conditions d'emploi des produits de sécurité, gestion des droits, dispositifs de détection et de gestion des incidents ;
- **des éléments techniques :** architecture du système (en précisant notamment les interconnexions avec d'autres systèmes), possibilité d'utilisation de supports amovibles, d'accès à distance ou de cloisonnement, mécanismes de maintenance, d'exploitation ou de télégestion du système, notamment lorsque ces opérations sont effectuées par des prestataires externes ;
- **le périmètre géographique et physique :** localisations géographiques et caractéristiques des locaux.

Le périmètre peut évoluer au cours de la démarche d'homologation, mais il est recommandé d'aboutir rapidement à une délimitation stable de celui-ci. Il est également recommandé d'appliquer une démarche d'homologation pour chaque service applicatif ou système d'information.

Les questions qui se posent à la première étape

Le système d'information est (ou sera) composé de certaines briques matérielles et logicielles que je ne maîtrise pas, car je les achète à un industriel, un éditeur ou un intégrateur. Comment garantir leur niveau de sécurité ?

Lorsque ces briques sont des composants essentiels de sécurité, elles doivent de préférence faire l'objet d'une labellisation de sécurité (qualification ou à défaut certification).

Lorsque ces briques sont des composants essentiels de la fonction applicative, il faut

*exiger auprès du fournisseur un **cahier de sécurité**, qui offre des garanties, précise les conditions d'emploi et définit des règles de sécurité. Le cas échéant, des audits de code peuvent être réalisés (cf. étapes suivantes).*
Ces documents sont versés au dossier d'homologation du système.

Plusieurs services applicatifs, nécessitant chacun une homologation, sont hébergés sur une même plate-forme technique avec des ressources mutualisées. Dois-je inclure la plate-forme dans toutes les homologations ?

Dans ce cas, il est recommandé d'homologuer séparément la plate-forme technique, en étudiant les risques qui lui sont propres et qui impactent potentiellement tous les services applicatifs qu'elle héberge.

J'aurais dû faire homologuer le système d'information avant sa mise en service, mais je ne l'ai pas fait et le service est opérationnel. Est-il trop tard ?

Non. La démarche d'homologation doit s'inscrire dans un processus itératif d'amélioration continue de la sécurité. Il est préférable et plus efficace de la démarrer avant les phases de développement et d'intégration, mais si le service est déjà opérationnel, les objectifs de l'homologation restent les mêmes.
Le contenu du dossier d'homologation sera légèrement différent et certaines mesures de sécurité ne pourront être mises en œuvre que lors des prochaines évolutions du système.
Si les risques identifiés sont trop importants et que les mesures de sécurité sont impossibles à mettre en œuvre, il faut envisager l'arrêt du service.

étape n°

2

Quel type de démarche dois-je mettre en œuvre ?

Durant la deuxième étape, vous allez définir le niveau de profondeur de la démarche d'homologation, afin que celle-ci soit adaptée aux enjeux de sécurité du système, d'une part, et aux capacités de votre organisme à la mener, d'autre part.

La démarche la plus adaptée à l'homologation du système doit être définie en fonction du contexte, du niveau de complexité et de criticité du système, du niveau de sensibilité des données hébergées et du niveau de maturité en matière de SSI de l'organisme qui met en œuvre l'homologation.

1 . Autodiagnostiquer les besoins de sécurité du système et le niveau de maturité SSI de l'organisme

Deux outils d'autodiagnostic vous sont proposés. Ils sont détaillés en annexe du présent document.

L'annexe 1 permet d'évaluer les besoins de sécurité du système d'information à homologuer, en estimant la gravité des conséquences potentielles d'une défaillance du SI, la sensibilité des données, le degré d'exposition aux menaces et l'importance des vulnérabilités potentielles du système.

Un questionnaire simple et rapide vous permet de déterminer si le besoin de sécurité du système est nul, faible, moyen ou fort.

L'annexe 2 permet de déterminer le niveau de maturité SSI de l'organisme, c'est-à-dire le niveau de maîtrise et de rigueur atteint par l'organisme, dans la gestion de la sécurité des systèmes d'information.

Un questionnaire simple et rapide vous permet de déterminer si la maturité SSI de votre organisme est élémentaire, moyenne ou avancée.

2 . En déduire la démarche appropriée

En fonction des résultats de l'autodiagnostic des besoins de sécurité et du niveau de maturité, vous pouvez déterminer, à l'aide du tableau *infra*, le type de démarche d'homologation à mettre en œuvre dans le cadre de votre projet.

Les autodiagnostics doivent être réalisés avec sérieux et objectivité. L'adoption d'une démarche inadaptée aux enjeux ou aux capacités de l'organisme hypothéquerait les chances de réussite du projet d'homologation.

Les démarches possibles sont les suivantes :

- **Pianissimo :** démarche autonome a minima, que l'autorité d'homologation peut mener sans recours à une assistance conseil externe, par l'application des outils et des indications donnés dans le présent guide.

- **Mezzo Piano :** démarche autonome approfondie, que l'autorité d'homologation peut mener sans recours à une assistance conseil externe, par l'application des outils et des indications donnés dans le présent guide et ses ressources internes.

- **Mezzo Forte :** démarche assistée approfondie, que l'autorité d'homologation mène avec l'aide d'une assistance conseil externe, en plus des outils et des indications données dans le présent guide.

- **Forte :** le niveau de maturité de l'organisme en matière de sécurité des systèmes d'information dispense l'autorité d'homologation de la lecture du présent guide qui apporte des outils qu'elle maîtrise déjà. Cette démarche n'est donc pas traitée dans ce guide.

		Besoin de sécurité du Système		
		Faible	Moyen	Fort
Niveau SSI de l'organisme	élémentaire	**Pianissimo :** démarche autonome a minima	**Mezzo Forte :** démarche assistée approfondie	**Mezzo Forte :** démarche assistée approfondie
	moyen	**Pianissimo :** démarche autonome a minima	**Mezzo Piano :** démarche autonome approfondie	**Mezzo Forte :** démarche assistée approfondie
	avancé	**Pianissimo :** démarche autonome a minima	**Forte :** hors champ de ce guide	**Forte :** hors champ de ce guide

étape n°

3

Qui contribue à la démarche ?

Durant la troisième étape, vous allez identifier l'ensemble des acteurs de l'homologation et bien définir leur rôle (décision, assistance ou expertise technique notamment).

Une homologation s'appuie sur plusieurs acteurs distincts auxquels sont associés différents rôles et niveaux de responsabilité.

1 . L'autorité d'homologation (AH)

L'autorité d'homologation est la personne physique qui, après instruction du dossier d'homologation, prononce l'homologation de sécurité du système d'information, c'est-à-dire prend la décision d'accepter les risques résiduels identifiés sur le système.

L'autorité d'homologation doit être désignée à un niveau hiérarchique suffisant pour assumer toutes les responsabilités. Il est donc nécessaire que l'autorité d'homologation se situe à un niveau de direction dans l'organisme.

L'autorité d'homologation désigne un responsable du processus d'homologation, qui mènera le projet d'homologation en son nom.

Lorsque cela est nécessaire, elle peut rédiger une lettre de mission à l'attention de la personne chargée d'organiser les tâches du processus d'homologation, en lui indiquant de quelle manière la synthèse des résultats de chaque étape de la démarche d'homologation lui sera communiquée.

Lorsque le système est sous la responsabilité de plusieurs autorités, l'autorité d'homologation est désignée conjointement par les autorités concernées

2 . La commission d'homologation

La commission d'homologation assiste l'autorité d'homologation pour l'instruction de l'homologation et est chargée de préparer la décision d'homologation.

La taille et la composition de cette commission doivent être adaptées à la nature du système et proportionnées à ses enjeux. Cette commission réunit les responsables métier concernés par le service à homologuer et des experts techniques. Elle peut donc être de taille très réduite dans des cas très simples.

La commission d'homologation est chargée du suivi des *plannings*, de l'analyse de l'ensemble des documents versés au dossier d'homologation. Elle se prononce sur la pertinence des livrables et peut les valider dans certains cas.

3 . Les acteurs de l'homologation

La maîtrise d'ouvrage

La maîtrise d'ouvrage représente les acteurs métier et assure la bonne prise en compte des contraintes liées à l'utilisation du système d'information. Elle joue un rôle-clé dans plusieurs étapes de la maîtrise des risques, y compris dans les arbitrages sur le traitement des risques.

Le RSSI

Lorsque l'entité dispose d'un responsable de la sécurité des systèmes d'information, celui-ci est impliqué dans la démarche d'homologation. Selon les cas, il peut être désigné responsable du processus d'homologation, chargé du secrétariat de la commission d'homologation ou être membre de droit de cette commission.

Le responsable d'exploitation du système

Le responsable d'exploitation du système, ou autorité d'emploi, remplit le rôle opérationnel. Il s'agit de l'entité exploitant le système d'information destiné à être homologué.

Les prestataires

En fonction de leur statut (interne ou externe), de leur implication dans le projet et de leurs relations avec l'autorité d'homologation, les prestataires peuvent être intégrés dans la commission d'homologation, ou simplement consultés en cas de besoin.

Ils remplissent un rôle d'assistance et produisent des livrables qui seront versés au dossier d'homologation ainsi que des réponses aux interrogations de la commission d'homologation.

Les systèmes interconnectés

Les autorités d'homologation des systèmes interconnectés au système concerné peuvent jouer un rôle dans l'homologation et être associés à la démarche lorsque :

- le système à homologuer a un impact sur leurs propres systèmes ;
- ils émettent des avis ou des certificats qui peuvent concerner le système.

Les questions qui se posent à la troisième étape

Qui doit être désigné autorité d'homologation ?

L'autorité d'homologation doit être choisie au niveau hiérarchique suffisant pour assumer toutes les responsabilités, y compris éventuellement pénale, afférentes à cette décision d'homologation.

L'autorité d'homologation doit-elle être unique ?

C'est très largement préférable, car il s'agit d'une prise de responsabilité individuelle.

Lorsque le système est sous la responsabilité de plusieurs autorités qualifiées, une autorité d'homologation multiple peut toutefois être envisagée, mais le partage des responsabilités doit demeurer absolument limpide.

L'autorité d'homologation peut-elle être déléguée ?

Parfois, une autorité d'homologation est désignée pour un système complexe ou ensemble de systèmes. Dans certains cas, elle souhaite déléguer la prise de décision

pour un système particulier ou un sous-système. C'est possible, mais avec beaucoup de précautions et dès le début du projet :

- *la délégation doit être donnée en accord avec l'autorité qui a désigné l'autorité d'homologation initiale ;*
- *l'autorité d'homologation doit rester à un niveau hiérarchique suffisant pour assumer toutes les responsabilités qui lui incombent ;*
- *il ne doit pas exister de mélange des genres et l'autorité d'homologation doit garder l'objectivité nécessaire ;*
- *le délégataire doit conserver une vue sur les systèmes déployés, les programmes en cours et les travaux de maintien en condition de sécurité.*

Au sein d'un organisme, les membres de la commission d'homologation sont-ils désignés une fois pour toutes ?

Cela dépend beaucoup du nombre et de la nature des systèmes d'information à homologuer au sein de l'organisme. La composition de la commission d'homologation peut être définie :

- *par projet, s'ils sont différents les uns des autres ;*
- *pour l'ensemble des projets de la direction, s'ils sont similaires les uns aux autres ;*
- *de manière mixte avec un noyau stable et des intervenants spécifiques au projet.*

étape n°

4

Comment s'organise-t-on pour recueillir et présenter les informations ?

Durant la quatrième étape, vous allez inventorier le contenu du dossier d'homologation et définir le planning de la démarche qui permettra de le constituer et de l'instruire.

1 . Le contenu du dossier d'homologation

Le dossier d'homologation est alimenté pendant toutes les phases de la démarche, essentiellement avec des documents nécessaires à la conception, à la réalisation, à la validation du projet ou à la maintenance du SI après sa mise en service, ainsi que des documents produits spécifiquement pour l'homologation. L'annexe 3 propose une liste complète des documents qui peuvent être intégrés dans un dossier d'homologation.

Le contenu du dossier pourra varier selon la démarche choisie. Le tableau ci-dessous synthétise les éléments constitutifs du dossier d'homologation en fonction de la démarche adoptée. L'annexe 3 établit la liste plus complète des documents pouvant être contenus dans un dossier d'homologation et en propose une description détaillée.

<table>
<tr><th></th><th>Pianissimo</th><th>Mezzo Piano</th><th>Mezzo Forte</th></tr>
<tr><td>Stratégie d'homologation</td><td colspan="3">Indispensable</td></tr>
<tr><td>Référentiel de sécurité</td><td colspan="3">Si existant</td></tr>
<tr><td>Document présentant les risques identifiés et les objectifs de sécurité</td><td colspan="3">Indispensable</td></tr>
<tr><td>Politique de sécurité des systèmes d'information</td><td>Recommandé</td><td colspan="2">Fortement recommandé</td></tr>
<tr><td>Procédures d'exploitation sécurisée du système</td><td colspan="3">Indispensable</td></tr>
</table>

Journal de bord de l'homologation	Recommandé	Fortement recommandé	
Certificats de qualification des produits ou prestataires	Si existant		
Résultats d'audits	Si existant	Recommandé	Fortement recommandé
Liste des risques résiduels	Indispensable		
Décision d'homologation	Indispensable		
Spécifiquement pour les systèmes déjà en service :			
Tableau de bord des incidents et de leur résolution	Recommandé	Fortement recommandé	Indispensable
Résultats d'audits intermédiaires	Si existant	Recommandé	
Journal des évolutions du système	Si existant		

Démarche Pianissimo :

Tous les documents décrivant les procédures de sécurité en vigueur au sein de l'organisme peuvent être intégrés au dossier, par exemple :

- la charte d'utilisation des postes informatiques ;
- les règles de contrôle d'accès physique et logique au système ;
- les clauses de sécurité des contrats de sous-traitance informatique.

Démarche Mezzo Piano et Mezzo Forte :

Les documents constitutifs du référentiel de sécurité de l'organisme peuvent être intégrés au dossier. En particulier :

- la politique de sécurité des systèmes d'information (PSSI) de l'organisme ;

- la législation ou la réglementation particulière au contexte de l'organisme ;
- le dossier de sécurité des systèmes interconnectés au système à homologuer.

La PSSI, quand elle existe, est un document de référence pour l'homologation, car elle contient des éléments stratégiques (périmètre du système, principaux besoins de sécurité et origine des menaces), ainsi que les règles en vigueur au sein de l'organisme.

L'homologation peut aussi être l'occasion de compléter (ou de rédiger) la PSSI, par exemple pour généraliser des règles indispensables au SI homologué.

2 . Planning

L'homologation doit être prononcée préalablement à la mise en service opérationnelle du système d'information.

La démarche visant à l'homologation doit donc être lancée en amont puis être totalement intégrée au projet dès les phases d'étude préalable et de conception, afin d'éviter tout risque calendaire.

Le calendrier de l'homologation est directement dépendant du calendrier du projet dont il doit tenir compte en permanence. Les principales étapes de l'homologation sont fixées dans la stratégie d'homologation.

Il est indispensable de déterminer les tâches de chacun des acteurs de l'homologation et les formaliser dans un planning associé, reprenant les principales étapes. Au besoin, en fonction de l'évolution du projet, ces échéances peuvent être révisées, avec l'accord de l'autorité d'homologation.

Ainsi, une homologation est rythmée par deux temps forts :

- la construction du référentiel documentaire et l'analyse de risque (dont la mise en œuvre peut être longue) ;
- le déploiement, l'audit, l'homologation et la mise en service opérationnel (a contrario, il s'agit d'une étape courte et très rapide).

Les échéances prévues pour les différentes étapes de la démarche d'homologation doivent figurer dans le planning :

1. lancement de la procédure d'homologation (par exemple date de formalisation de la stratégie d'homologation) ;
2. début et de fin de l'analyse des risques (dates des entretiens avec l'autorité) ;
3. remise des différents documents du dossier d'homologation (cf. section suivante) ;
4. engagements liés à d'éventuels contrats avec des prestataires impliqués dans le système (hébergeurs, fournisseurs de sous-systèmes, d'applications…) ;
5. réunions de la commission d'homologation ;
6. audits éventuels sur les composants du système (techniques ou organisationnels), logiciels plates-formes matérielles, interfaces réseaux ;
7. homologation du système ;
8. mise en service du système.

Les questions qui se posent à la quatrième étape

Un audit sera-t-il nécessaire au cours de la démarche d'homologation ?
Un contrôle sera systématiquement effectué à la sixième étape, mais ce contrôle ne prendra la forme d'un audit technique formel que si les enjeux de sécurité le justifient.

Quelle que soit la démarche adoptée, c'est à l'autorité d'homologation de décider s'il est nécessaire d'effectuer un audit sur le système d'information, et à quel niveau. Cet audit permettra de mettre en évidence d'éventuelles failles sur le système, et d'identifier rapidement les risques encourus par l'organisme en conséquence.

étape n°

5

Quels sont les risques pesant sur le système ?

Durant la cinquième étape, vous allez identifier et ordonner les risques qui pèsent sur le système d'information à homologuer.

1 . L'analyse de risque

Un risque est la combinaison d'un événement redouté (susceptible d'avoir un impact négatif sur la mission de l'entité) et d'un scénario de menaces. On mesure le niveau du risque en fonction de sa gravité (hauteur des impacts) et de sa vraisemblance (possibilité qu'il se réalise).

Il s'agit d'identifier les risques pesant sur la sécurité des systèmes d'information, de les hiérarchiser et de déterminer des objectifs généraux qui permettront de diminuer certains d'entre eux et, à terme, de les amener à un niveau acceptable.

La durée et le coût de la réalisation d'une analyse de risques sont fonction de la complexité du système d'information et de la sensibilité des données (données propres ou données de tiers, telles que celles des usagers ou des partenaires).

L'analyse des risques pesant sur le système peut être simplifiée dans le cadre d'une démarche Pianissimo. Dans le cas d'une démarche Mezzo Piano ou Mezzo Forte, on privilégiera l'utilisation d'une méthode éprouvée d'analyse de risque.

Démarche Pianissimo

Le tableau d'autodiagnostic de l'annexe 1 vous a permis d'identifier, lors de la deuxième étape, que les enjeux de sécurité du système d'information étaient limités et que les besoins de sécurité étaient faibles.

Pour une analyse de risque simplifiée, vous pouvez alors procéder de la manière suivante :

1. Partez de la liste des menaces courantes présente dans l'annexe 4. Ces menaces sont d'ordre volontaire ou accidentel (inondation, panne de cli-

matisation entraînant une panne des équipements informatiques, erreur de saisie), de nature physique (intrusion sur le système) ou logique (intrusion réseau, défiguration de site, etc.).

2. Écartez celles qui ne sont pas pertinentes dans le contexte du système d'information étudié ;
3. Pour chaque menace conservée, déterminez un ou plusieurs biens essentiels qui pourraient être affectés. Les biens essentiels sont les informations traitées au sein du système, ainsi que leurs processus de traitement. Ils constituent la valeur ajoutée du système d'information pour l'organisme.
4. Pour chaque lien identifié entre une menace et un bien essentiel, décrivez l'impact négatif sur la disponibilité, l'intégrité ou la confidentialité de ce bien essentiel. Vous obtenez un scénario de risque.
5. Hiérarchisez les scénarios de risque obtenus, en identifiant les plus probables et ceux dont l'impact est le plus pénalisant.
6. Si un scénario de risque plausible aboutit à un impact très fort, cela signifie que le besoin de sécurité évalué lors de la deuxième étape a été sous-évalué. Envisagez alors une démarche plus complète, de type Mezzo Piano ou Mezzo Forte.

Démarche Mezzo Piano ou Mezzo forte

Dans le cadre de la mise en œuvre d'une démarche Mezzo Piano ou Mezzo Forte, la mise en œuvre d'une méthode d'analyse de risque éprouvée est très fortement recommandée. La méthode EBIOS 2010 est une méthode d'analyse de risque développée par l'ANSSI.

La méthode EBIOS 2010 présente les risques et les objectifs de sécurité identifiés dans une **Fiche d'Expression Rationnelle des Objectifs de Sécurité (FEROS).**

Dans le cadre d'une démarche Mezzo Piano, l'analyse est effectuée par l'autorité d'homologation, avec ou sans l'assistance d'un consultant ayant une expérience confirmée de la méthode. Elle nécessite la participation des acteurs clés du système à homologuer, qui sont interrogés sur leurs besoins, leur contexte d'emploi du système et les événements qu'ils redoutent. C'est la direction de l'entreprise ou l'autorité administrative, par exemple, qui fournissent les

informations sur les besoins de disponibilité ou de confidentialité du système, ce qui permet d'identifier les objectifs de sécurité du système.
Pour la démarche Mezzo Piano, le résultat de l'analyse (la FEROS) peut ensuite constituer un élément du cahier des clauses techniques particulières d'un appel d'offres pour la réalisation ou la mise en conformité du système à homologuer. Les soumissionnaires doivent y répondre en indiquant de quelle manière ils proposent d'atteindre les objectifs de sécurité identifiés par l'*autorité d'homologation*.

2 . Identifier les mesures de sécurité

À l'issue de l'analyse de risque, il convient de définir les mesures de sécurité permettant de couvrir les risques identifiés. Ceux qui demeurent après l'application des mesures sont considérés comme des *risques résiduels* qui doivent être acceptés dans le cadre de l'homologation.

Démarche Pianissimo

Pour déterminer les mécanismes de sécurité à mettre en œuvre, vous pouvez également vous référer à plusieurs documents publiés par l'ANSSI (sur http://www.ssi.gouv.fr) :

- le guide des 40 règles d'hygiène informatique ;
- le guide d'externalisation pour les systèmes d'information ;
- le guide sur la virtualisation ;
- les notes techniques, notamment celle sur la sécurité web.

Démarche Mezzo Piano et Mezzo Forte

Dans le cadre d'une démarche Mezzo Piano et Mezzo Forte, les objectifs de sécurité identifiés au cours de l'analyse de risque selon la méthode EBIOS permettront de définir les mesures de sécurité destinées à couvrir les risques considérés comme inacceptables.

Outre les documents présentés dans le paragraphe précédent, de nombreux référentiels de sécurité proposent des catalogues de mesures.

étape n°

6

La réalité correspond-elle à l'analyse ?

Durant la sixième étape, vous devez mesurer l'écart entre les résultats de l'étude de risque et la réalité, en réalisant un contrôle plus ou moins formalisé du système. Ce contrôle peut intervenir à tout moment du cycle de vie du système : en amont, avant la mise en service voir au cours de la conception, mais également en aval, si le système est déjà opérationnel.

Le degré de formalisation du contrôle dépend de la démarche entreprise. Vous avez déterminé lors de la quatrième étape quel type d'audit était adapté. Certains systèmes n'appellent qu'une vérification peu formelle. En revanche, un audit complet et indépendant se justifie dans le cas de systèmes à fort enjeu de sécurité.

1 . Réalisation du contrôle

Démarche Pianissimo
Pour la démarche Pianissimo, un audit technique est optionnel.

Démarche Piano
Pour la démarche Piano, il est recommandé de procéder à un audit formalisé sur les segments les moins maîtrisés du système.

Démarche Mezzo forte
Pour la démarche Mezzo Forte, il est fortement recommandé d'effectuer un audit technique du système d'information. Cet audit permettra de mettre en évidence d'éventuelles failles et d'identifier rapidement les risques encourus par l'organisme.

Les audits doivent être menés dans les formes prévues par le référentiel d'exigences relatif aux prestataires d'audit de la sécurité des systèmes d'information, disponible sur le site de l'ANSSI .

2 . Définition du périmètre du contrôle

Le contrôle effectué, qui peut prendre la forme d'un audit formalisé, porte sur un système dont le périmètre doit être soigneusement délimité par l'autorité d'homologation. Les éléments à contrôler peuvent être de différente nature (code source, configuration des équipements, architecture du système, organisation mise en place, etc.).

Dans certains cas, des tests d'intrusions peuvent être effectués.

3 . Conséquences de l'audit sur le dossier d'homologation

Le contrôle de sécurité doit faire l'objet d'une trace écrite. A fortiori, s'il s'agit d'un audit de sécurité, celui-ci doit faire l'objet d'un rapport, qui doit faire apparaître :

- une évolution des menaces sur le système ;
- la découverte éventuelle de nouvelles vulnérabilités ;
- la préconisation de mesures correctrices, le cas échéant.

Le rapport d'audit est intégré au dossier d'homologation, qui doit être complété en tenant compte des nouveaux risques mis en lumière.

étape n°

7

Quelles sont les mesures de sécurité supplémentaires pour couvrir les risques ?

Durant la septième étape, vous devez définir un plan d'action pour amener le risque identifié à un niveau acceptable.

1 . Le traitement du risque

Au vu des résultats de l'analyse de risques et du contrôle de sécurité, l'autorité d'homologation se prononce sur l'ensemble des risques qui ne sont pas, à ce stade, complètement couverts par des mesures de sécurité. Il convient ainsi, pour tout ou partie de chaque risque de choisir parmi les options suivantes :

- l'éviter : changer le contexte de telle sorte qu'on n'y soit plus exposé ;
- le réduire : prendre des mesures de sécurité pour diminuer l'impact et/ou la vraisemblance ;
- l'assumer : en supporter les conséquences éventuelles sans prendre de mesure de sécurité supplémentaire ;
- le transférer : partager les pertes occasionnées par un sinistre ou faire assumer la responsabilité à un tiers.

On peut choisir plusieurs options pour chaque risque. Par exemple, un risque peut être partiellement réduit par la mise en œuvre de mesures de sécurité, partiellement transféré par le recours à une assurance et partiellement assumé pour ce qui subsiste.

2 . La mise en œuvre de mesures de sécurité

Les mesures de sécurité peuvent être de nature technique, organisationnelle ou juridique. Elles sont décidées par l'autorité d'homologation sur proposition de la commission d'homologation.

En cas de recours à un prestataire externe (hébergement de site ou de services par exemple), les mesures de sécurité peuvent être intégralement mises

en œuvre à travers un contrat garantissant, par exemple, que les processus et les données sont protégés et accessibles uniquement aux utilisateurs légitimes.

3 . Définition du plan d'action

Les risques résiduels identifiés lors du contrôle et de l'analyse de risques et qui ne peuvent pas être couverts par des mesures techniques ou organisationnelles sont identifiés dans un plan d'action. Ce dernier indique les vulnérabilités éventuelles, leur degré (critique, majeure, mineure…), l'action correctrice envisagée, le pilote désigné, ainsi que l'échéance associée.

étape n°

8

Comment réaliser la décision d'homologation ?

Durant la huitième étape, vous devez concrétiser la décision d'homologation par une attestation formelle autorisant, du point de vue de la sécurité, l'exploitation du système d'information.

La décision d'homologation est l'acte par lequel le responsable de l'autorité administrative atteste de l'existence d'une analyse de sécurité et de sa prise en compte. La décision d'homologation doit nécessairement comprendre un certain nombre d'éléments, référencés ci-dessous.

1 . Le périmètre de l'homologation

Il doit, au minimum, tenir compte des éléments suivants :

- référentiel réglementaire ;
- références des pièces du dossier d'homologation ;
- périmètre géographique et physique (localisations géographiques, locaux, etc.) ;
- périmètre fonctionnel et organisationnel (fonctionnalités, types d'informations traitées par le système et sensibilité, types d'utilisateurs, règles d'emploi, procédures, conditions d'emploi des produits de sécurité, etc.) ;
- périmètre technique (cartographie, architecture détaillée du système, produits agréés, prestataires qualifiés, etc.).

2 . Les conditions accompagnant l'homologation

L'autorité d'homologation peut, en fonction des risques résiduels identifiés, assortir l'homologation de conditions d'exploitation ainsi que d'un plan d'action visant à maintenir et à améliorer le niveau de sécurité du système dans le temps. À chaque action, ce plan associe une personne pilote ainsi qu'une échéance.

3 . La durée de l'homologation

L'homologation doit être décidée pour une durée maximale.
Cette durée doit prendre en compte l'exposition du système d'information aux nouvelles menaces, ainsi que les enjeux de sécurité du système, c'est-à-dire le degré de criticité des informations et des processus du système.

Pour un système bien maîtrisé, avec peu de risques résiduels et ne présentant pas de difficultés particulières, il est recommandé de prononcer une homologation d'une durée maximale de cinq (5) ans, avec revue annuelle. Cette durée maximale doit être réduite à trois (3) ans pour un système avec de nombreux risques résiduels ou à un an (1) pour un système présentant de nombreux risques résiduels.

4 . Conditions de suspension ou de retrait de l'homologation

L'homologation de sécurité ne demeure valide que tant que le système d'information est exploité dans le contexte décrit dans le dossier d'homologation.
Les changements suivants doivent impliquer un réexamen du dossier, pouvant conduire à une nouvelle décision d'homologation ou à un retrait de la décision :

- raccordement d'un nouveau site sur le système d'information ;
- ajout d'une fonctionnalité majeure ;
- succession de modifications mineures ;
- réduction de l'effectif affecté à une tâche impactant la sécurité ;
- changement d'un ou de plusieurs prestataires ;
- prise de fonction d'une nouvelle autorité d'homologation ;
- non-respect d'au moins une des conditions de l'homologation ;
- changement du niveau de sensibilité des informations traitées et, plus généralement, du niveau du risque ;
- évolution du statut de l'homologation des systèmes interconnectés ;

- publication d'incidents de nature à remettre en cause les garanties recueillies dans le dossier de sécurité ;
- décision de l'autorité d'homologation.

À ce titre, il est recommandé que la commission d'homologation soit réunie annuellement par l'autorité d'homologation, afin de procéder à une revue du respect des conditions de l'homologation.

Les questions qui se posent à la huitième étape

La démarche d'homologation a mis en évidence que les risques résiduels restent trop élevés pour une homologation, mais des contraintes d'ordre supérieur imposent une mise en service opérationnelle du système. Comment faire ?

Si l'autorité d'homologation considère que les conditions ne sont pas réunies pour une homologation, la meilleure solution est de refuser l'homologation. Si cette possibilité n'est pas envisageable, il est toujours possible de prononcer une autorisation provisoire d'emploi (APE) pour une durée courte (3 ou 6 mois), assortie de conditions strictes et d'un plan d'action précis, destiné à supprimer ces risques trop élevés et qui doit être réalisé durant le temps de l'APE.

Certaines mesures de sécurité ne pourront être mises en place que dans deux ans pour une homologation de 3 ans. Est-ce trop long ?

Il est impératif de spécifier dans la décision d'homologation que la mise en place des mesures est progressive, planifiée et suivie. Elle doit commencer dès la date de publication de la décision.

étape n°

9

Qu'est-il prévu pour continuer d'améliorer la sécurité ?

Durant cette dernière étape, qui intervient après la décision d'homologation proprement dite, vous devez mettre en œuvre une procédure de révision périodique de l'homologation, ainsi que le plan d'action pour traiter les risques résiduels et les nouveaux risques dans le cycle de vie du système.

1 . Suivi de l'homologation

À la suite de la décision proprement dite, l'autorité d'homologation doit veiller au maintien du niveau de sécurité du système. La commission d'homologation réalise annuellement un suivi de l'homologation. Cette étape n'est pas une nouvelle instruction. Elle doit donc rester simple et se limiter à une mise à jour du dossier et à une analyse succincte des évolutions et des incidents intervenus au cours de l'année, afin de juger de l'opportunité d'une révision plus approfondie de l'homologation.

En préparation du renouvellement de l'homologation, le dossier d'homologation est régulièrement complété par les éventuelles analyses de vulnérabilités, les comptes rendus de contrôle et les rapports d'audits complémentaires. La version consolidée est transmise aux membres de la commission d'homologation

Il est recommandé de réunir périodiquement la commission d'homologation pour reprendre la liste des critères et vérifier que les conditions d'homologation sont toujours respectées. Cela permet également d'éviter de reprendre l'homologation à zéro au terme de sa durée de validité.

2 . Maintien en conditions de sécurité

Il est nécessaire que les conditions de l'homologation soient respectées dans le temps. À ce titre, l'entité en charge du maintien du dossier d'homologation doit également assurer une veille technologique. Celle-ci permet d'identifier les vulnérabilités qui apparaîtraient sur le système et s'assurer qu'elles soient corrigées, notamment les plus sérieuses.

Il est également nécessaire de vérifier :

- les clauses de sécurité et de maintien en conditions de sécurité du système, le cas échéant en se référant au guide d'externalisation publié par l'ANSSI ;
- les capacités d'évolution et d'interopérabilité de son système, notamment au regard de ses capacités de développement ou de ses contrats de prestations de service.

Les questions qui se posent à la neuvième étape

Si une nouvelle vulnérabilité est découverte, dois-je relancer le processus d'homologation ?

Cela dépend de l'impact de la vulnérabilité sur le système. S'il est fort, il faudrait effectivement relancer le processus d'homologation sans attendre l'issue de la durée d'homologation en cours.

CONSEILS PRATIQUES

La démarche d'homologation est un projet en soi, qui doit s'intégrer complètement au projet global et au cycle de vie du système d'information. C'est une démarche qui peut se révéler complexe et qui se heurte parfois à des difficultés organisationnelles, techniques ou calendaires. Les conseils contenus dans cette fiche vous permettront d'aboutir plus facilement à un résultat satisfaisant.

Conseils d'ordre général

Les conseils d'ordre général listés ci-dessous doivent, dans la mesure du possible, être suivis pour maximiser les chances de réussite d'une démarche d'homologation :

- débuter suffisamment tôt la démarche d'homologation ;
- prévoir une validation formelle des décisions au niveau hiérarchique adéquat ;
- désigner un véritable chef de projet, qui sera disponible tout au long du projet ;
- maîtriser le calendrier et ne pas être trop contraint par des nécessités opérationnelles ;
- bien définir le périmètre et disposer d'une architecture précise du système ;
- bien prendre en compte les interconnexions éventuelles ;
- s'appuyer sur des documents écrits, explicites, sans ambiguïté, afin d'éviter les quiproquos entre les parties prenantes au projet.

Avant l'étude

Une réflexion menée en amont permet de bien préparer la démarche d'homologation et d'assurer sa réussite de façon optimale.

Au préalable, il faut que la démarche soit portée à haut niveau par l'autorité d'homologation et que l'ensemble des acteurs concernés soit impliqué et motivée.

Il faut également désigner un chef de projet, qui disposera des moyens pour mener à bien sa mission et rapporter toute difficulté à l'autorité d'homologation.

Enfin, dès que les acteurs de l'homologation sont identifiés, il est indispensable de les sensibiliser sur la démarche, les concepts et le vocabulaire qui seront utilisés.

Pendant l'étude

Pour chaque activité à réaliser, il est conseillé de s'organiser en mode projet, en identifiant un responsable de l'activité, en constituant un groupe de travail et en lui confiant une mission précise, associée à une date de réalisation.

Certaines missions sont essentielles pour la réussite du projet :

> la sensibilisation des acteurs

- rappeler l'objectif de l'activité
- présenter les concepts, le vocabulaire
- s'assurer que l'ensemble des acteurs ait une vision commune de la problématique

> la collecte des informations

- réaliser des entretiens
- rassembler les documents existants sur l'organisme, le projet

> le suivi du projet

- présenter des exemples pour lancer les discussions
- synthétiser les informations récoltées pour validation par le groupe de travail
- nommer des responsables et fixer des échéances
- se rencontrer périodiquement

Il est également nécessaire d'adapter les livrables aux destinataires en ce qui concerne :

- la forme : tableaux, textes, schémas, etc. ;
- le niveau d'information : recherche d'exhaustivité ou forme synthétique ;
- l'intégration aux documents existants ;
- l'adaptation au vocabulaire habituel de l'organisme,
- leur nomenclature, qui doit être explicite,
- leur libellé, qui doit être court et descriptif.

Enfin, il est recommandé de faire valider chaque étape par la commission d'homologation. Cela permet d'éviter les retours en arrière improductifs, tout en impliquant les autorités tout au long de la réalisation du dossier de sécurité.

ANNEXES

Annexe 1

Estimation rapide du besoin de sécurité d'un système d'information

Le tableau suivant permet d'évaluer les besoins de sécurité du système d'information (SI) à homologuer, en estimant la gravité des conséquences potentielles d'une défaillance du SI, la sensibilité des données, le potentiel des attaquants, le degré d'exposition aux menaces et l'importance des vulnérabilités intrinsèques du SI.

Si vous répondez « Je ne sais pas » à plus de deux questions, faites-vous aider par la maîtrise d'ouvrage, qui connaît les enjeux du système.

				Note
Question nº 1 : Votre système est-il important pour remplir vos missions ?				
1	*2*	*3*	*4*	
Non, le système est accessoire à l'accomplissement des missions	Oui, les missions seraient fortement perturbées par un dysfonctionnement du SI.	Oui, les missions dépendent totalement du SI	Je ne sais pas	
Question nº 2 : Si un sinistre atteint votre SI, causant un dysfonctionnement ou une perte de données, les conséquences en interne (pour vos services) seraient-elles graves ? *Exemple :* une panne électrique ne permet pas d'utiliser le système, le contenu d'une base de données a été supprimé, etc.				

				Note
1	*2*	*3*	*4*	
Non, les conséquences internes d'un sinistre seraient négligeables	Oui, les conséquences internes d'un sinistre seraient significatives	Oui, les conséquences internes d'un sinistre seraient graves, voire fatales	Je ne sais pas	
Question n° 3 : Si un sinistre touche la sécurité de votre système (il ne fonctionne plus ou pas bien, vol d'informations…), les conséquences pour l'extérieur (pour vos usagers, administrés…) seraient-elles graves ?				
1	*2*	*3*	*4*	
Non, les conséquences d'un sinistre pour l'extérieur seraient négligeables	Oui, les conséquences d'un sinistre pour l'extérieur seraient significatives	Oui, les conséquences d'un sinistre pour l'extérieur seraient graves, voire fatales	Je ne sais pas	
Gravité des conséquences potentielles (reportez ici la valeur maximale des réponses aux questions 1 à 3)				
Question n° 4 : Le fait que les données de votre système soient inaccessibles est-il grave ? *Exemple :* vous ne pouvez pas accéder aux données en raison d'une panne matérielle.				
1	*2*	*3*	*4*	
Non, le fait qu'il ne soit pas accessible ne gêne quasiment pas l'activité	Oui, le fait qu'il ne soit pas accessible perturbera l'activité de manière significative	Oui, le fait qu'il ne soit pas accessible peut être fatal pour l'activité	Je ne sais pas	

				Note
Question nº 5 : Le fait que les données de votre système soient altérées est-il grave ? *Exemple :* un virus a modifié des valeurs dans une base de données, les remettant toutes à 0.				
1	*2*	*3*	*4*	
Non, le fait que les données soient altérées ne gêne quasiment pas l'activité	Oui, le fait que les données soient altérées perturbera l'activité de manière significative	Oui, le fait que les données soient altérées peut être fatal pour l'activité	Je ne sais pas	
Question nº 6 : Le fait que les données de votre système ne soient pas ou plus confidentielles est-il grave ? *Exemple :* la liste des bénéficiaires du service social est dévoilée.				
1	*2*	*3*	*4*	
Non, le défaut de confidentialité ne gêne quasiment pas l'activité	Oui, le défaut de confidentialité perturbera l'activité de manière significative	Oui, le défaut de confidentialité peut être fatal pour l'activité	Je ne sais pas	
Sensibilité des données du système (reportez ici la valeur maximale des réponses aux questions 4 à 6)				
Question nº 7 : Quel est le niveau de compétence maximal présumé de l'attaquant ou du groupe d'attaquants susceptibles de porter atteinte au système ?				

				Note
1	*2*	*3*	*4*	
Individu isolé de niveau de compétence élémentaire	Individu isolé de niveau de compétence avancé	Groupe d'individus organisés, de niveaux individuels de compétence faibles à moyens, ou individu isolé aux compétences expertes	Groupe d'individus experts, organisés, aux moyens quasi illimités	
Question nº 8 : Quelle est la précision des attaques potentielles envers le SI ?				
1	*2*	*3*	*4*	
Attaques « au hasard » sur le cyberespace	Attaques orientées vers le continent européen ou la France	Attaques ciblant un groupe de victimes présentant des caractéristiques communes	Attaques visant précisément le système	
Question nº 9 : Quel est le niveau de sophistication des attaques potentielles contre le SI ?				
1	*2*	*3*	*4*	
Outils d'attaque triviaux (logiciel de scan de ports, virus connus, etc.)	Outils élaborés génériques prêts à l'emploi (réseaux de botnet loués, faille connue, etc.)	Outils sophistiqués, adaptés pour le SI (zéro-day, etc.)	Boîte à outils très hautement sophistiquée.	

				Note
Question nº 10 : Quelle est la visibilité des attaques potentielles contre le SI ?				
1	*2*	*3*	*4*	
Attaque annoncée (revendications « d'hacktivistes », rançon, etc.)	Attaque constatée immédiatement par ses effets sur le SI	Attaque discrète, qui laisse des traces dans les journaux d'événements, mais ne perturbe pas le fonctionnement du SI	Attaque invisible, réalisée en laissant le minimum de traces	
Question nº 11 : Quelles sont la fréquence et la persistance des attaques potentielles contre le SI ?				
1	*2*	*3*	*4*	
Unique : l'attaque ne se produit sur la cible qu'une seule fois	Ponctuelle : l'attaque survient plusieurs fois sans régularité dans sa fréquence (elle peut être liée à l'actualité).	Récurrente : attaque par vagues successives importantes	Permanente.	
Base d'estimation des potentiels d'attaques cyber (reportez ici la valeur maximale des réponses aux questions 7 à 11)				
Question nº 12 : Quel est le niveau d'hétérogénéité du système ? *Exemple :* plusieurs logiciels, matériels ou réseaux différents pour un même système.				

				Note
1	*2*	*3*	*4*	
Le système est jugé comme homogène	Le système est jugé comme faiblement hétérogène	Le système est jugé comme fortement hétérogène	Je ne sais pas	
Question nº 13 : Quel est le degré d'ouverture/interconnexion du système ? *Exemple :* Internet, un autre système interne ou externe (celui d'un prestataire, d'une autre autorité administrative…)…				
1	*2*	*3*	*4*	
Le SI n'est pas ouvert	Le SI n'est ouvert qu'à des systèmes internes maîtrisés	Le système est ouvert à des systèmes internes non maîtrisés ou externes	Je ne sais pas	
Question nº 14 : Le contexte dans lequel se trouve le SI et ses composants (matériels, logiciels, réseaux) évolue-t-il régulièrement ?				
1	*2*	*3*	*4*	
Le SI et son contexte sont jugés stables	Le SI et son contexte changent souvent	Le SI et son contexte évoluent en permanence	Je ne sais pas	
Question nº 15 : Les composants du SI sont-ils mis régulièrement à jour ?				
1	*2*	*3*	*4*	
Les composants du SI sont tous tenus à jour en permanence	Une partie des composants du SI est régulièrement mise à jour	Les mises à jour sont effectuées de manière irrégulière	Je ne sais pas	

Exposition et vulnérabilités (reportez ici la valeur maximale des réponses aux questions 12 à 15)		
Additionner les valeurs maximales des réponses aux questions	**TOTAL**	

Avec ces résultats que l'on additionne, on estime ainsi le besoin de sécurité de son système :

Somme des quatre valeurs	Besoin de sécurité du système
De 4 à 6	1 - Faible
De 7 à 9	2 - Moyen
De 10 à 16	3 - Fort

Annexe 2

Estimation rapide du niveau de maturité de l'organisme

Le tableau suivant permet d'évaluer le niveau de maturité en sécurité de votre organisme.

Le niveau de maturité en sécurité ne correspond pas au niveau réel de sécurité, mais à la capacité de l'organisme à gérer les risques, pour chaque système d'information.

Questions	Oui / Non
Les activités de sécurité sont-elles réalisées en utilisant des pratiques de base (bonnes pratiques de sécurité, référentiels de mesures…) ?	
Si la case précédente est à **Oui**, alors votre organisme a un **niveau de maturité élémentaire en sécurité**, *sinon, une démarche assistée est indispensable.*	
Les activités de sécurité sont-elles planifiées ?	
Les acteurs affectés à des activités de sécurité sont-ils formés (en interne ou par un organisme de formation) à la SSI (niveau de compétence en sécurité jugé suffisant) ?	
Certaines pratiques de sécurité sont-elles formalisées dans des documents spécifiques (procédures) ?	
Des mesures de sécurité sont-elles en place ?	

Les autorités compétentes sont-elles informées des mesures effectuées ?	
Si toutes les cases précédentes sont à **Oui**, alors votre organisme a un **niveau de maturité moyen en sécurité.**	
Les processus de sécurité sont-ils définis, standardisés et formalisés (définir la stratégie, gérer les risques, gérer les règles, superviser…) ?	
Des acteurs spécifiques sont-ils affectés à la gestion des processus de sécurité et sont formés en conséquence ?	
L'organisme dans sa globalité soutient-il les processus de sécurité (les différents niveaux hiérarchiques…) ?	
Les processus de sécurité sont-ils coordonnés dans tout le périmètre choisi ?	
L'efficacité des mesures de sécurité en place est-elle mesurée ?	
Des audits sont-ils effectués pour vérifier la suffisance des mesures en place ? (Les mesures de sécurité effectuées sont-elles contrôlées [auditées] ?)	
Les processus de sécurité sont-ils améliorés en fonction des mesures de sécurité effectuées ?	
Si toutes les cases précédentes sont à **Oui**, alors votre organisme a un **niveau de maturité avancé en sécurité.**	

Annexe 3

Liste des documents pouvant être contenus dans un dossier d'homologation

Le dossier d'homologation peut contenir, en fonction de leur pertinence au regard du contexte et de la complexité du système, les éléments suivants.

1 . La stratégie d'homologation

L'autorité d'homologation, ou son représentant, formalise l'organisation de l'homologation dans un document de synthèse. Cette *stratégie d'homologation* décrit les modalités de réalisation du processus d'homologation. Elle rappelle l'ensemble des parties prenantes à l'homologation et précise :

- le cadre réglementaire applicable (règles de protection des informations confidentielles, règles sectorielles, etc.) ;
- l'organisation (acteurs, missions, etc.) ;
- la démarche ;
- le périmètre ;
- le calendrier ;
- la criticité des informations utilisées dans le cadre de l'homologation ;
- les pièces constitutives du dossier d'homologation.

2 . L'analyse de risques

Elle peut être menée selon une méthode éprouvée conforme aux normes existantes en matière de gestion des risques SSI

3 . La politique de sécurité du système d'information (PSSI)

La PSSI définit les principes et les exigences techniques et organisationnelles de sécurité du système d'information. Il s'agit du document de référence SSI applicable à l'ensemble de l'organisme ou dédié à un système.

L'homologation peut aussi être l'occasion d'élaborer ou de compléter la politique de sécurité des systèmes d'information (PSSI) de l'organisme, par exemple afin de généraliser des règles indispensables au système d'information homologué. Le guide [PSSI] de l'ANSSI fournit une aide pour élaborer une PSSI .

Ce document revêt différentes formes en fonction des interlocuteurs (directives, procédures, codes de conduite, règles organisationnelles et techniques, etc.)

La PSSI inclut :

- les éléments stratégiques ;
- le périmètre du SI, les enjeux liés, les orientations stratégiques, les aspects légaux et réglementaires ;
- les principes de sécurité par domaine (organisationnel, technique, mise en œuvre, etc.).

Elle peut être complétée par une ou plusieurs politiques d'application, par exemple les procédures d'exploitation de la sécurité (PES).

4 . Le journal de bord de l'homologation

Il s'agit du registre des décisions et des principaux événements qui sont intervenus pendant la démarche d'homologation. Il présente les caractéristiques suivantes :

- il s'enrichit au fur et à mesure du projet (document de travail, feuille de route) pour adapter le processus aux évolutions du projet, notamment pour le planning ;

- Il permet de formaliser les prises de décisions et les mises au point nécessaires et de disposer d'un point de situation sur l'avancement du processus d'homologation (et les blocages éventuels) ;
- Il constitue la base pour réaliser le plan d'action associé à la décision d'homologation ;
- Il peut se présenter sous plusieurs formes :
  - » documents isolés (comptes rendus de réunions, notes, etc.) ;
  - » document unique (registre formel de décisions, ou tableau de synthèse avec renvois à des documents isolés par exemple).

5 . Les référentiels de sécurité

La démarche d'homologation doit être réalisée conformément aux exigences décrites dans les référentiels de sécurité de l'autorité et en particulier :

- la politique de sécurité des systèmes d'information (PSSI) de l'autorité ;
- la législation ou la réglementation particulière applicable à l'autorité administrative ;
- les exigences de sécurité des systèmes interconnectés au système à homologuer.

6 . Le tableau de bord de l'application des règles d'hygiène informatique

Les « 40 règles d'hygiène informatique » publiées par l'ANSSI sont applicables dans toutes les situations. Un tableau de bord mesurant l'application de ces mesures d'hygiène montre la progression au sein du système, l'objectif étant de toutes les appliquer.

7 . La cartographie des systèmes d'information de l'organisme

La cartographie complète du réseau local doit être établie. Elle comprend :

- **la cartographie physique du réseau** qui correspond à la répartition géographique des équipements et permet de connaître la position d'un équipement réseau au sein des différents sites.
- **la cartographie logique du réseau** (plan d'adressage IP, noms de sous-réseaux, liens logiques entre ceux-ci, principaux équipements actifs, etc.). Elle fait notamment apparaître les points d'interconnexion avec des entités « extérieures » (partenaires, fournisseurs de services, etc.) ainsi que l'ensemble des interconnexions avec Internet.
- **la cartographie des applications.** Le point de vue applicatif correspond aux applications métier et logiciels d'infrastructure utilisant l'architecture réseau comme support
- **la cartographie de l'administration du système d'informations.** Elle représente le périmètre et le niveau de privilèges des administrateurs sur les ressources du parc informatique. Ce point de vue permet, en cas de compromission d'un compte d'administration, d'identifier le niveau de privilège de l'attaquant et la portion du parc potentiellement impactée.

8 . Les schémas détaillés des architectures du système

Les schémas détaillés des architectures techniques et fonctionnelles dépendent avant tout du périmètre choisi de l'homologation du SI, ainsi que du niveau de maturité de l'organisme.

Les schémas doivent permettre de savoir quelle est la fonction principale du SI et comment ce SI fonctionne.

À cette fin, il faut disposer, au minimum, de l'annuaire (gestion des comptes), du plan d'adressage, de la liste des fonctions de sécurité et de la cartographie du SI.

Cette documentation doit être mise à jour afin de suivre les modifications subies par le SI.

Par exemple, si le périmètre de l'homologation est une application de téléservice, il faut fournir les éléments suivants :

- les procédures d'exploitation de sécurité (PES) ;
- le plan du maintien en condition opérationnelle ;
- la matrice des flux entrant/sortant (interconnexions) ;
- la documentation de la gestion des comptes de l'application ;
- la documentation de l'administration du SI et de l'installation ;
- plan de sauvegarde et d'archivage des données ;
- plan de continuité ou de reprise d'activité.

9 . Le document présentant les risques identifiés et les objectifs de sécurité

Ce document doit être élaboré à l'issue d'une analyse de risques, réalisée (sauf pour la démarche Pianissimo) en suivant une méthode éprouvée et maintenue, si possible respectant la norme ISO 27005. Il présente les caractéristiques suivantes :

- il décrit les besoins et objectifs de sécurité du système en termes de disponibilité, d'intégrité et de confidentialité par rapport aux menaces identifiées. Au besoin, il peut être présenté sous la forme d'une Fiche d'Expression Rationnelle des Objectifs de Sécurité (FEROS) .
- il indique la nature et la sensibilité des informations traitées par le système et précise les contraintes qui restreignent la conception, l'exploitation et la maintenance du système.
- il doit prendre en compte les architectures d'interconnexion, les moyens partagés avec d'autres entités, leurs conditions d'exploitation et de contrôle.
- sa rédaction nécessite la participation des acteurs clés du système à homologuer, qui sont interrogés sur leurs besoins, le contexte d'emploi du système et les événements susceptibles d'impacter positivement ou négativement le système.

- dans le cadre des systèmes OTAN, il est demandé un énoncé des impératifs de sécurité (SRS) (ou un équivalent national). Le SRS est un énoncé complet et explicite des principes de sécurité détaillés à satisfaire. Il existe plusieurs types de SRS :
  - CSRS, énoncé des impératifs de sécurité applicables à un ensemble d'interconnexions lorsque plusieurs SI sont interconnectés ;
  - SSRS, énoncé des impératifs de sécurité propres à un système dans des situations simples (système autonome, par exemple) ;
  - SISRS, énoncé des impératifs de sécurité applicables à une interconnexion de systèmes, lorsque deux SIC doivent être connectés entre eux pour échanger des informations, le SISRS constitue la base d'un accord entre les deux autorités d'exploitation des SIC et les deux autorités d'approbation ou d'homologation de sécurité ;
  - le SEISRS qui est la cible de sécurité (ou énoncé des impératifs de sécurité électronique propres à un système.

10 . Les procédures d'exploitation du système

Ces procédures doivent être détaillées et directement applicables. Elles exposent les mesures de sécurité permettant de répondre aux objectifs de sécurité fixés par l'autorité d'homologation. Elles présentent les droits et les devoirs des accédants au système ainsi que les actions à réaliser dans le cadre de l'utilisation quotidienne du système.

Ces procédures sont établies par les équipes d'exploitation internes à l'organisme et/ou par les fournisseurs du système à homologuer, éventuellement à l'aide des guides publiés par l'ANSSI .

L'autorité d'homologation doit s'assurer que les procédures fournies ont été testées avec succès avant de prononcer l'homologation. Un dossier de tests complétera utilement le dossier d'homologation.

11 . Les exigences de sécurité à destination des systèmes interconnectés

Les systèmes contenant des informations sensibles ne doivent pas être connectés directement aux réseaux publics tels qu'Internet ou les réseaux WiFi des hôtels, des gares ou des aéroports.

12 . Les décisions d'homologation des systèmes interconnectés

Si les systèmes connectés au système concerné, ont déjà fait l'objet d'une homologation, il faut joindre les décisions d'homologation associées aux systèmes ainsi que les dossiers associés, si possible et si nécessaire. En effet, il est impératif de savoir, au minimum, par qui le système a été homologué, à quelle date et quelle est la référence de cette dernière homologation.

13 . Les certificats de sécurité des produits utilisés

Les agréments des dispositifs de sécurité, prononcés en application des dispositions de l'IGI 1300, doivent figurer dans le dossier d'homologation.

Les décisions de ne pas faire agréer par l'ANSSI un dispositif de sécurité, lui-même utilisé comme moyen de protection contre les accès non autorisés aux informations classifiées ou au système, doivent être également jointes au dossier, ainsi que les éléments ayant contribué à ces décisions.

14 . Les attestations de qualification des produits ou prestataires

Dans la mesure où le système met en œuvre des produits de sécurité certifiés ou qualifiés ou encore des services de confiance qualifiés, il est nécessaire d'inclure les attestations correspondantes dans le dossier d'homologation.

Si elles sont disponibles, les analyses de sécurité des produits de sécurité, en particulier les instructions techniques d'emploi, peuvent également être intégrées au dossier d'homologation.

15 . Les plans de tests et d'audits

Des documents doivent identifier formellement les tests et les audits nécessaires et préciser par qui ils doivent être effectués et selon quel planning.

Pour mémoire, des audits doivent être prévus après la décision d'homologation, afin d'assurer le maintien en conditions opérationnelles du système.

16 . Les rapports de tests et d'audits et les plans d'action associés

Pour les systèmes déjà en production depuis un an ou plus, il est recommandé de procéder d'emblée à un audit technique sur le système à homologuer, le cas échéant avant l'analyse des risques.

Pour les systèmes en cours de conception, l'audit pourra être réalisé à l'occasion de la procédure de recette applicative.

Pour les systèmes existants requérant un besoin particulier de sécurité, il est recommandé de procéder, en première action, à un audit technique et organisationnel afin d'optimiser la procédure d'homologation.

L'audit doit mener à la l'établissement d'une liste des vulnérabilités détectées et du plan d'action afférent.

Les audits doivent être réalisés par des équipes préalablement validées par l'autorité d'homologation.

Ils doivent porter sur les mesures de sécurité liées à l'exploitation du système et les comparer à l'état de l'art.

Les audits doivent être menés dans les formes prévues par le référentiel d'exigences relatif aux prestataires d'audit de la sécurité des systèmes d'information.

17 . Le dossier des risques résiduels

Ce dossier comporte une analyse de la couverture des risques et de l'atteinte des objectifs de sécurité au travers :

- des procédures d'exploitation sécurisée du système ;
- de la PSSI.

Il présente également les vulnérabilités résiduelles constatées lors des tests et des audits et non corrigées ainsi que les plans d'action associés.

18 . Les éventuelles décisions d'homologation antérieures

Le dossier doit comporter tous les documents relatifs aux éventuelles homologations précédentes.

19 . Le tableau de bord des incidents et de leur résolution

Ce tableau recueille l'ensemble des incidents survenus sur le SI avec l'identification de leur(s) cause(s), les conséquences et les modalités de résolution de l'incident. Il précise également le plan d'action associé.

20 . Le journal des évolutions

Ce journal consigne les évolutions du système, notamment celles ayant une incidence sur les critères et conditions de l'homologation.

Il comprend, en particulier, la liste des mesures de sécurité apportées en prévention de risques ou en correction d'anomalies ou de vulnérabilités constatées dans les audits.

Annexe 4

Liste de menaces, issue de la base de connaissance EBIOS

Menaces sur les matériels

Usage d'un équipement ou d'un matériel :

- utilisation abusive d'un ordinateur à des fins personnelles, voire pour un usage inapproprié ou illicite ;
- stockage de fichiers personnels sur l'ordinateur de bureau (ex. vidéos non professionnelles) ;
- usage d'une imprimante à des fins personnelles ou au détriment d'autrui ;
- stockage d'informations sensibles sur des supports inappropriés (disque dur non protégé, clé USB, CDROM laissé sur un bureau…) ;
- perte ou vol d'un ordinateur (surtout portable), ou d'un support de données électronique (clé USB, CDROM, disque dur amovible) notamment lors d'un déplacement ou d'un déménagement.

Observation d'un équipement :

- observation d'un écran à travers une fenêtre ;
- observation de la saisie d'un code au clavier ;
- écoute d'une conversation diffusée sur les haut-parleurs de l'ordinateur ;
- géolocalisation d'un matériel (à partir de son adresse IP ou par le réseau téléphonique) ;
- interception de signaux compromettants émis par l'affichage à l'écran ou les touches du clavier ;
- pose d'un dispositif-espion matériel (*keylogger*) sur la face arrière d'un poste de travail.

Fonctionnement du matériel :

- surcharge d'un disque dur ou d'un serveur aboutissant à une panne ;
- perturbations électriques ou électromagnétiques ;
- panne électrique involontaire (remplacement d'un poste par un ordinateur plus consommateur en énergie, rupture de câbles électriques suite à des travaux de terrassement, court-circuit dû à la foudre, erreur de branchement ou incident électrique…) ;
- vieillissement du matériel susceptible d'entraîner un crash du disque dur ;
- multiples déplacements du matériel (ordinateur portable) ;
- ordinateur travaillant dans un milieu pollué, humide, ou corrosif (atelier industriel…), ou en présence d'ondes électromagnétiques ou de vibrations ;
- chute du matériel pendant une installation ou un déménagement (voir vandalisme) ;
- effacement des données par passage d'un aimant sur un disque dur ;
- présence d'un code malveillant destiné à empêcher le fonctionnement de tout ou partie du matériel.

Menaces sur les logiciels

Menaces sur l'usage de logiciels

- un logiciel est piégé (*keylogger*), ou corrompu par un code malveillant ;
- un logiciel accède ou copie de manière inappropriée voire illicite des données métiers, des données de configuration d'équipements, ou collecte des données métiers partagées dans un réseau ;
- un logiciel supprime de manière inappropriée des données, journaux d'événements, enregistrements de conversations, etc. qu'ils soient en mémoire, sur un disque dur ou sur un support ;
- un logiciel crée ou modifie des données de manière inappropriée : messages injurieux sur un forum, configuration d'un système, insertion d'une page web ou défiguration sur un site Internet, élévation de privilèges d'un

compte utilisateur, effacement de traces d'opérations dans un journal d'événements, fraude ;

- un logiciel collecte des données de configuration d'un réseau, balaie les adresses internes réseau ou recense les ports ouverts ;
- un logiciel exploite des données de base pour en extraire des informations confidentielles (recoupement, infocentre) ;
- un logiciel utilise des mécanismes de stéganographie pour transmettre des données discrètement ;
- un agent utilise un logiciel professionnel pour des besoins personnels ;
- un agent connecte son ordinateur portable personnel compromis par un attaquant au réseau ;
- un agent transfère systématiquement tous les messages qu'il reçoit sur un compte de messagerie personnel dont le mot de passe a été cassé par un groupe d'attaquant notoire ;
- une machine du réseau est compromise pour réaliser un envoi massif d'informations par courrier électronique (*spam*) ;
- un utilisateur utilise, volontairement une copie d'un logiciel dont le fonctionnement n'est pas garanti (par exemple une contrefaçon) ;
- un logiciel est utilisé sans achat de la licence correspondante, ou la licence n'est pas renouvelée ;
- un logiciel est analysé par l'attaquant en vue d'être corrompu : observation de son fonctionnement, observation de l'emploi de son espace mémoire, ingénierie inverse, etc. ;
- tout ou partie du logiciel est détruit par un virus (bombe logique…) ;
- le logiciel est modifié de manière involontaire : mise à jour avec une mauvaise version, modification de la configuration en maintenance, activation ou désactivation de fonctions, changement de paramétrage du réseau, modification des règles de routage ou de résolution des noms de domaine.

Menaces sur les réseaux

- un attaquant écoute les informations circulant sur le réseau informatique ou téléphonique, et réémet un message confidentiel vers l'adresse d'un forum public ;
- un attaquant sature le réseau par un envoi massif de messages ;
- un point d'accès sans fil mal configuré permet l'écoute de l'ensemble des données qui transitent par Wifi ;
- un attaquant sectionne les câbles d'une ligne téléphonique (tord la fibre optique) empêchant physiquement la transmission des messages ;
- une équipe de maintenance remplace un câble existant par un autre de moins grande capacité, etc. ;
- des voleurs dérobent les câbles de transmission en cuivre pour les revendre à la ferraille.

Menaces sur les personnels

- l'unique administrateur d'une application critique est victime d'une épidémie de grippe
- une grève des transports paralyse l'accès au site hébergeant les postes de travail ;
- une contamination dans le restaurant d'entreprise crée une intoxication alimentaire chez de nombreux agents ;
- l'un des agents se déplaçant régulièrement bavarde avec des inconnus rencontrés au wagon-bar du TGV des anomalies de fonctionnement du système ;
- un agent, perturbé par une surcharge de tâches, commet des erreurs de manipulation du système ;
- l'ergonomie du poste de travail (mauvais éclairage, siège inconfortable, etc.) nuit au bon usage du logiciel ;
- un agent passe une part significative de son temps de travail sur les sites de jeux en ligne, ce qui nuit à l'efficacité du système ;

- l'agent expert dans l'usage d'une fonction critique du système demande sa mutation pour se rapprocher de son conjoint ;
- une réorganisation ou un déménagement rompent les échanges entre personnes qui s'étaient établies pour pallier les faiblesses fonctionnelles du système.

Menaces sur les locaux

- il existe un risque qu'un incendie se déclenche dans les locaux sans être détecté ;
- le bâtiment hébergeant le système se situe dans une zone industrielle comportant des entreprises soumises à autorisation préfectorale (ex. SEVESO) susceptibles de générer un accident industriel (explosion) ;
- emploi de mauvais matériaux, construction défectueuse, mouvements de terrain sapant les fondations, infiltration d'eau dans le sol, etc.

Version 1.0 - Août 2014
20140821-1128

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

ANSSI - 51, boulevard de la Tour-Maubourg - 75700 PARIS 07 SP

www.ssi.gouv.fr / communication@ssi.gouv.fr

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
Premier ministre