RÉPUBLIQUE
FRANÇAISE
Liberté
Égalité
Fraternité

COLLECTION
GESTION DES RISQUES CYBER

LE GUIDE DE L'HOMOLOGATION DE SÉCURITÉ DES SYSTÈMES D'INFORMATION

COLLECTION
GESTION DES RISQUES CYBER

LE GUIDE DE L'HOMOLOGATION DE SÉCURITÉ DES SYSTÈMES D'INFORMATION

PRÉAMBULE

Les systèmes d'information[1] sont devenus incontournables dans le fonctionnement des entités publiques et privées.

Leurs utilisations détournées peuvent entraîner des risques pouvant avoir des impacts humains, financiers, juridiques ou réputationnels catastrophiques.

La prise en compte et l'acceptation formelle de ces risques par une autorité est appelée « homologation de sécurité » et est réglementaire dans un grand nombre de cas.

Au travers de ce guide, il semblait important de comprendre et de détailler la démarche permettant aux organisations d'homologuer leurs systèmes d'information.

Ce guide s'adresse à toutes les personnes devant réaliser, porter ou accompagner une démarche d'homologation.

Écrit par l'ANSSI[2] en collaboration avec la DINUM[3], il se base sur des années d'élaboration et d'accompagnement dans des travaux d'homologation et sur les nombreux retours d'experts de la fonction publique et du secteur privé.

Ce guide se veut abordable dans sa lecture et applicable à tous les systèmes d'information, du plus simple au plus complexe, quelle que soit sa criticité ou son exposition aux sources de risques.

> NOTE : Le guide doit être lu comme un support permettant l'homologation de sécurité d'un système d'information, mais n'a pas vocation à remplacer une méthode, efficace, déjà en place dans votre organisation.

1. Pour des soucis de simplification le terme « système d'information » désigne tout système permettant le traitement d'information, qu'il soit physique (ordinateurs, équipements informatique), logiques (logiciels) ou virtuelles (système nuagique/cloud), quelle que soit sa complexité ou sa sensibilité.
2. Agence nationale de la sécurité des systèmes d'information
3. Direction interministérielle du numérique

Dans un monde numérique en constante évolution, le guide de l'homologation de sécurité sera amené à être amélioré régulièrement. Il fait partie de la collection « Gestion des Risques Cyber »[4] permettant de mieux appréhender les risques cyber.

Il est complété par des fiches méthodes qui prennent en compte les différentes topologies des systèmes d'information dans le processus d'homologation

4. Dont la méthode d'analyse de risque EBIOS RM (https://cyber.gouv.fr/la-methode-ebios-risk-manager) et MonServiceSécurisé (https://monservicesecurise.cyber.gouv.fr)

TABLE DES MATIÈRES

1

AVANT DE COMMENCER

LA NOUVELLE DOCTRINE D'HOMOLOGATION DE SÉCURITÉ

La nouvelle doctrine d'homologation de sécurité a été pensée par l'Agence nationale de la sécurité des systèmes d'information et par tous les interlocuteurs qu'elle a rencontrés afin de simplifier et d'accélérer la démarche d'homologation.

Des changements importants ont été apportés et seront détaillés plus en avant dans ce guide. *Par exemple* :

- L'homologation doit revenir à une acceptation des risques métier, par une autorité, pour une organisation.
- Trois niveaux progressifs de démarche ont été identifiés permettant d'adapter les efforts à fournir en fonction de la criticité et de l'exposition du système d'information.
- Un seul type d'homologation : les notions d'homologations temporaires (APE/IATO), de tests et fermes (ATO) disparaissent au seul profit de l'homologation. Seules les durées d'homologation comptent.
- Les systèmes d'information pas ou peu critiques, pas ou peu exposés peuvent bénéficier d'une démarche d'homologation simplifiée, basée sur la confiance.
- Le corpus documentaire nécessaire à une homologation est grandement simplifié.
- Les commissions d'homologation peuvent dans certains cas être dématérialisées.

1.1 L'APPROCHE PAR LES RISQUES

Comprendre les risques auxquels une organisation est exposée est essentiel pour anticiper et optimiser les prises de décision.

En adoptant une approche par les risques dans sa stratégie, une organisation peut identifier les menaces, devenir plus résiliente ou saisir plus d'opportunités.

Pour ce faire, il est crucial que tous les niveaux de l'organisation et notamment les responsables et les équipes de direction soient sensibilisés et comprennent les risques qui peuvent affecter l'organisation.

Le choix de l'utilisation d'un système d'information au sein d'une organisation et son homologation doivent faire partie de cette stratégie.

1.2 UNE HOMOLOGATION DE SÉCURITÉ, C'EST QUOI ?

L'emploi d'un système d'information peut entraîner des risques ayant des impacts graves pour une activité. Il convient donc qu'un responsable de l'organisation en soit conscient et décide, en toute connaissance de cause de sa mise ou de son maintien en service.

Cette décision, recommandée par l'ANSSI depuis plusieurs années et rendue obligatoire par un grand nombre de textes officiels[5] est appelée « décision d'homologation »[6].

Elle est donc un préalable à toute utilisation d'un système d'information.

Tout système d'information qui serait déjà en exploitation sans être homologué doit être arrêté ou obtenir une homologation dans un délai raisonnable[7].

> NOTE : Une homologation de sécurité est un acte formel qui engage l'autorité qui la prononce.

5. voir chapitre « Identifier les réglementations applicables ».
6. Dans certains pays, le principe d'homologation existe et peut être appelé « accreditation » ou « autorisation ».
7. Un délai raisonnable correspond au temps nécessaire pour présenter un plan d'action permettant de sécuriser le système d'information à homologuer.

Homologuer un système d'information permet de :

- s'assurer que les risques de sécurité liés à l'utilisation du système d'information ont été identifiés et que les mesures nécessaires pour les traiter sont ou vont être mises en œuvre dans un délai raisonnable ;
- s'assurer que les réglementations en vigueur sont correctement appliquées ;
- valider le plan d'actions à appliquer au système d'information afin de renforcer sa sécurité ;
- responsabiliser et engager l'autorité qui accepte son emploi et toutes les parties prenantes associées.

> NOTE : Homologuer un système d'information renforce son niveau de sécurité et permet de renforcer la confiance de ses usagers, clients et partenaires quand à son utilisation.

Le processus permettant l'obtention de l'homologation est nommé « démarche d'homologation ».

Il doit être adapté au système d'information, à son contexte d'emploi, à la nature des données qu'il traite, aux enjeux de sécurité et à l'état de la menace.

Les travaux menant à l'homologation débutent dès la conception du système d'information et se terminent lors de son décommissionnement[8].

Les travaux sont cycliques et itératifs. Chaque fin de cycle fait l'objet d'une décision d'homologation.

> NOTE : Une homologation de sécurité peut être prononcée même si les travaux de sécurisation du système d'information ne sont pas terminés.
> Un système d'information peut être homologué même s'il comporte des risques non traités mais acceptables par l'autorité.

8. Le décommissionnement d'un système d'information consiste à l'arrêter de façon permanente, de démanteler les équipements qui le composent et supprimer les données qu'il contient.

1.3 COMPRENDRE LE CONTEXTE DE L'ORGANISATION

Avant de s'intéresser au système d'information, il convient de comprendre l'organisation qui va l'employer. Cette étape permet d'identifier le contexte dans lequel l'organisation évolue, sa stratégie, ses challenges et surtout les risques auxquels elle est confrontée.

L'organisation doit avoir l'assurance que les risques à laquelle elle est exposée sont bien identifiés, évalués et traités.

Ce travail nécessite la participation des interlocuteurs[9] pertinents, ayant une vision globale de l'organisation. Des analyses telles que PESTEL[10] ou SWOT[11] utilisées au sein des équipes de direction peuvent être utiles pour identifier le contexte dans lequel le système d'information est employé.

Comprendre le contexte de l'organisation permet d'évaluer son appétence aux risques.

> NOTE : Le niveau de risques qu'une organisation est prête à accepter dépend fortement de sa stratégie.

1.4 ENGAGER LES ÉQUIPES DE DIRECTION

La prise en compte de la sécurité numérique dans une organisation ainsi que pour l'ensemble des systèmes d'information qu'elle utilise nécessite une volonté forte de la part de la direction en :

- s'assurant que les politiques de sécurité sont établies, comprises et appliquées ;
- s'assurant que les ressources humaines nécessaires à leur application sont disponibles, formées et engagées ;
- s'assurant que les budgets alloués à la sécurisation du système d'information sont disponibles ;

9. Le pronom personnel masculin est largement utilisé dans ce guide afin d'en simplifier sa lecture. Il peut être remplacé par son équivalent féminin.

10. L'analyse PESTEL (PESTLE en anglais) permet de décrire une stratégie d'organisation en couvrant les domaines Politique, Economique, Sociologique, Technologique, Légaux et Environnementaux.

11. Le SWOT est un outil stratégique permettant d'identifier les forces (Strenghts), les faiblesses (Weaknesses), les opportunités (Opportunities) et les menaces (Threats) d'un projet, d'une étude ou d'un système d'information donné.

- communiquant sur l'importance de la sécurisation des systèmes d'information dès leur conception en sensibilisant et formant les utilisateurs et les équipes ;
- améliorant régulièrement les procédés liés à la sécurisation des systèmes d'information.

1.5 COMPRENDRE LE SYSTÈME D'INFORMATION

L'objectif et les enjeux de sécurité du système d'information doivent être compris afin d'identifier son importance pour l'organisation.

Il convient d'avoir des réponses aux questions suivantes :

- À quels besoins métier répond le système d'information ?
- À quels autres systèmes d'information est-il connecté ?
- Quelles sont les conséquences pour l'organisation si le système d'information n'est plus en capacité d'accomplir sa mission ?
- Quels sont les impacts pour l'organisation si les informations que traite le système d'information sont perdues, dévoilées ou altérées ?

Les enjeux du système d'information doivent être compris :

- Quels sont les objectifs stratégiques du système d'information ? sociaux, politiques, contractuels, retombées financières, part de marché, informationnels…
- Existe-t-il une pression forte, stratégique ou politique pour démarrer le système d'information ?
- Quelles sont les dates clés du projet (*par exemple : date limite de mise en service*) ?
- Le système d'information est-il en concurrence avec d'autres systèmes d'information ?
- La technologie utilisée par le système d'information est-elle nouvelle et doit être lancée avant celle des concurrents ?
- Un investissement important a-t-il été apporté pour concevoir le système d'information et un retour sur investissement rapide est-il demandé par la direction générale ?

Des réponses simples aux questions doivent être apportées dans un format approprié[12].

12. Une fiche simple de présentation du système d'information doit être claire, synthétique et abordable pour tous.

NOTE : La compréhension du système d'information dans son contexte doit permettre d'identifier sa criticité et le niveau de sécurité requis.

L'ESSENTIEL :

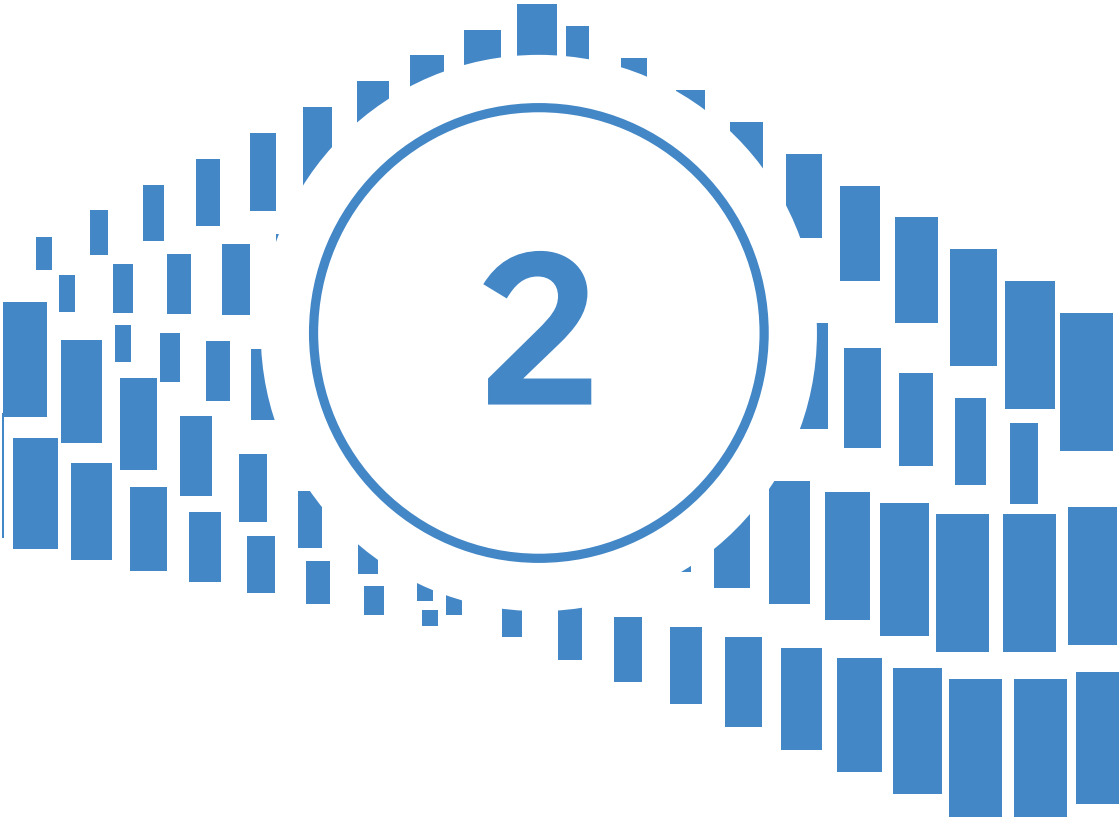
Homologuer un système d'information permet de s'assurer que les risques liés à son utilisation sont clairement identifiés et acceptés par le plus haut niveau d'une organisation (l'autorité d'homologation de sécurité).

Une décision d'homologation est un acte formel, réglementaire qui engage l'autorité qui la prononce. Elle découle d'une démarche qui doit débuter dès la conception du système d'information au même titre que sa sécurisation. Elle nécessite le support des équipes de direction.

Un système d'information peut être homologué même s'il comporte des risques non traités mais acceptables par l'autorité.

Le niveau d'acceptation des risques auxquels un système d'information est exposé est dépendant du contexte de l'organisation qui l'emploie et de son appétence aux risques.

SÉCURISER LE SYSTÈME D'INFORMATION



Les actions de sécurisation et d'homologation[13] d'un système d'information sont étroitement liées.

Elles doivent débuter dès la conception[14] du système d'information et se terminer à son décommissionnement. Elles doivent être menées au sein d'un projet qui doit être :

- ponctué de phases de validation, correspondant à des renouvellements d'homologation ;
- adapté au système d'information, à son contexte d'emploi, à la nature des données traitées et aux enjeux de sécurité.

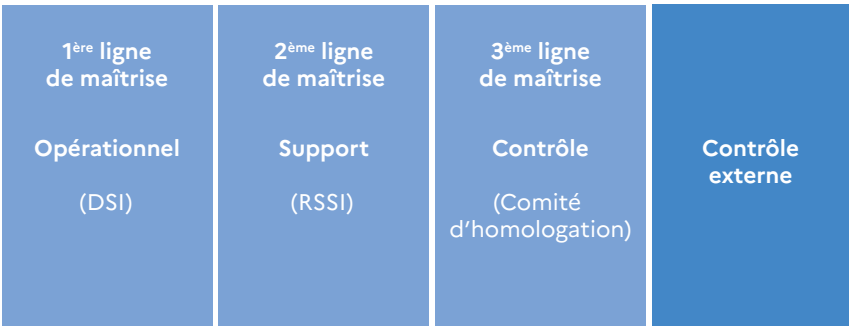
NOTE : Lorsque la réglementation l'impose, une démarche d'homologation doit être réalisée, mais dans tous les cas, elle est fortement recommandée par l'ANSSI pour tout système d'information critique à une organisation.

2.1 METTRE EN PLACE UNE GOUVERNANCE DE SÉCURITÉ

Les organisations, si elles le peuvent, doivent mettre en place une gouvernance adaptée, permettant de faciliter les travaux de sécurisation des systèmes d'information et de leur homologation.

Le modèle en trois lignes (appelé trois lignes de maîtrise dans ce guide ou de défense suivant les contextes) est adapté[15] à cet objectif.

13. Voir le chapitre « identifier le niveau de la démarche d'homologation »
14. Conception / sécurisation dès la conception Security by Design
15. cf Maîtrise du risque numérique – l'atout confiance (https://cyber.gouv.fr/publications/maitrise-du-risque-numerique-latout-confiance)



La première ligne de maîtrise est composée des équipes opérationnelles. Elle est responsable de mettre en œuvre et de maintenir les mesures issues des politiques de sécurité, des réglementations et du plan d'action.

Elle communique à la seconde ligne les informations appropriées *(par exemple les indicateurs de performance des contrôles – KPI).* Généralement les membres de la Direction des Systèmes d'Information (DSI) composent la première ligne de maîtrise.

La seconde ligne de maîtrise a un rôle de support. Elle regroupe les spécialistes des risques et apporte à la première ligne le soutien nécessaire à l'amélioration de la sécurité du système d'information.

Elle communique les mesures de sécurité à appliquer et s'assure qu'elles sont correctement appliquées par la première ligne.

Elle a la charge de piloter les audits du système d'information et les analyses de risque.

La seconde ligne est généralement responsable des travaux d'homologation de sécurité. Il s'agit généralement des Responsables de la Sécurité des Systèmes d'Information (RSSI).

Enfin **la troisième ligne de maîtrise** doit contrôler que les systèmes d'information sont suffisamment sécurisés pour être employés. Elle doit, en étroite relation avec les autres lignes de maîtrise, collecter les informations permettant une homologation, les évaluer et proposer un avis d'homologation à son autorité. Elle organise la commission d'homologation. Il est à noter que la troisième ligne de maîtrise peut être portée par la direction des risques de l'organisation.

Dans tous les ministères et les établissements publics de l'Etat, les conseillers à la sécurité numériques CSN[16] sont membres de la troisième ligne de maîtrise.

> NOTE : Pour atteindre un objectif commun de sécurisation et d'homologation du système d'information, les tâches et les responsabilités des trois lignes de maîtrise doivent être claires et bien définies.
> Les trois lignes de maîtrise doivent travailler en étroite collaboration.

Ce modèle en trois lignes permet une séparation des rôles et une clarification de la gouvernance. Il s'adapte parfaitement à une organisation disposant de suffisamment de ressources.

Idéalement, ces trois rôles doivent être tenus par des personnes différentes.

Dans les organisations où les ressources ne seraient pas suffisantes, les rôles identifiés peuvent être assurés par les mêmes personnes. Celles-ci pouvant être internes ou externes à l'organisation.

Une ligne de maîtrise supplémentaire peut intervenir lorsqu'un contrôle externe à l'organisation est requis. Celle-ci a la charge de vérifier que les travaux menés par la troisième ligne sont suffisants pour émettre un avis d'homologation de sécurité.

Il peut être opportun de présenter un RACI permettant d'identifier les rôles et responsabilités de chaque ressource affectée au projet.

16. Se référer à l'arrêté du 26 octobre 2022 portant approbation de l'instruction générale interministérielle n°1337/SGDS/ANSSI (https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000046503128)

2.2 DÉFINIR LE PÉRIMÈTRE DU SYSTÈME D'INFORMATION

Dans tout projet d'homologation, il est primordial d'identifier le périmètre sur lequel les travaux vont être menés.

> NOTE : Le périmètre du système d'information à homologuer est l'ensemble des composants du système d'information dans lequel l'information est traitée et pour lequel une autorité a été identifiée.

Dans ce cadre de responsabilité, le périmètre regroupe :

- l'ensemble des supports physiques qui permettent de produire, collecter, stocker, traiter et distribuer l'information ;
- les services, applications ou logiciels en charge du traitement et de l'échange de l'information ;
- les équipements physiques permettant l'échange d'information avec les systèmes d'information connectés. Il peut s'agir d'équipements de connexion ou de supports de masse amovibles ;
- les ressources humaines associées au système d'information. Les utilisateurs et les administrateurs du système d'information ;
- les localisations géographiques et physiques. Il peut s'agir *par exemple* des salles serveurs[17] et des lieux dans lesquels peut être utilisé le système d'information ;
- et l'ensemble des éléments qui permettent de faire fonctionner le système d'information et sur lesquels le responsable du périmètre a la maîtrise.

17. Data center

> NOTE : Le périmètre du système d'information doit clairement être identifié en termes techniques, fonctionnels et de responsabilités.

Il est à noter que le périmètre d'homologation doit, dans la mesure du possible être isolé de son écosystème par des mécanismes de filtrage (pare-feu, diode), de rupture protocolaire ou tout autre moyen permettant de ralentir ou de stopper une attaque cyber.

Le système d'information étudié dans le cadre d'une démarche d'homologation peut être le regroupement de plusieurs systèmes d'information complémentaires ayant une mission commune. Dans ce cas, on parle de périmètre capacitaire.

Par exemple deux systèmes d'information permettant l'un la gestion des congés des employés et l'autre l'établissement des fiches de salaire, peuvent appartenir au même périmètre d'homologation.

A contrario, pour faciliter les travaux, il peut s'avérer nécessaire de découper le périmètre et de procéder à plusieurs périmètres d'homologation.

Cela est notamment applicable, lorsque les systèmes d'information sont de natures ou de portées différentes.

Par exemple un système d'information composé de service d'hébergement de données (partage de fichiers), de messagerie et de téléphonie peut faire l'objet de trois homologations distinctes.

Quel que soit le périmètre de l'homologation, celui-ci doit être clair et facilement identifiable.

Le choix du périmètre dépend de la nature des données traitées et de sa complexité.

Deux systèmes de niveau de protection ou de classification[18] différents doivent faire l'objet de deux démarches d'homologation.

Un système d'information traitant de deux domaines[19] de données différents, mais de même niveau ne doit pas faire l'objet de deux démarches d'homologation distinctes.

Le périmètre ne comprend pas les éléments ayant une relation avec le système d'information et qui ne dépendent pas de l'autorité d'homologation du sujet.

Par exemple dans le cas d'un système d'information en mode PAAS[20], les serveurs hébergeurs ne font pas partie du périmètre d'homologation.

Néanmoins leurs utilisations peuvent entraîner des risques qui doivent être identifiés et traités lors de l'analyse des risques.

Ils appartiennent à l'écosystème et doivent être correctement identifiés.

18. Protection (donnée publique, confidentielle personnelle, confidentielle industrielle, restreinte), classification secrète, très secrète.

19. EU, OTAN, OCCAR…

20. PAAS : Platform As A Service est un ensemble de ressources mis à disposition par un tiers qui en a la responsabilité

Les systèmes d'information hébergés introduisent une séparation de responsabilité entre le propriétaire des données et l'hébergeur. Le périmètre de l'homologation doit correspondre au périmètre de responsabilité.

Responsabilité	SaaS[21]	PaaS	IaaS	On-prem[22]
Données	X	X	X	X
Ordinateurs (PC et mobile)	X	X	X	X
Annuaires d'identité		X	X	X
Application		X	X	X
Système (OS)			X	X
Virtualisation (machine, réseau)			X	X
Machines physiques (+hyperviseur)				X
Réseau physique				X
Local informatique				X

Les X indiquent le périmètre d'homologation à prendre en compte.

21. SaaS : Software as a Service, PaaS : Platform as a Service, IaaS Infrastructure as a Service

22. On Premise : dans les locaux

2.3 IDENTIFIER L'ÉCOSYSTÈME

L'écosystème contient tous les éléments ayant une interconnexion physique, technique ou organisationnelle avec le système d'information objet de l'homologation mais ne faisant pas partie de son périmètre.

Un élément de l'écosystème est appelé « brique » dans la suite de ce guide.

Il peut s'agir :

- d'un système d'information connecté ;
- d'interconnexion ;
- d'une API ou d'un service utilisé par le système d'information ;
- d'une plateforme hébergeur ou hébergé ;
- d'un poste de travail permettant l'accès au système d'information ;
- d'un local hébergeant les éléments techniques ;
- d'administrateurs n'appartenant pas au périmètre d'homologation ;
- d'utilisateurs extérieurs à l'organisation ;
- etc.

Chaque brique identifiée fournit un ou plusieurs services[23], des données ou des infrastructures.

Les risques qu'entraîne son utilisation doivent être connus.

> NOTE : Il convient donc que chaque brique apporte le niveau de garantie de sécurité correspondant à sa criticité et au niveau de confiance exigé par le système d'information à homologuer.

23. Les services fournis peuvent être par exemple des services fonctionnels spécifiques au métier, partagés avec un grand nombre de clients, des services d'identité…

Par exemple :

- *Un système d'information exigeant un fort taux de disponibilité doit s'appuyer sur un écosystème ayant au minimum ce même taux.*
- *Un système d'information traitant de données devant réglementairement être hébergées dans une zone sensible doit s'assurer que l'écosystème doit être conforme à cette exigence et être bien situé dans cette zone.*

Les garanties peuvent se traduire par une homologation, une certification, un contrat de service ou tout autre élément permettant d'apprécier sa sécurité, sa robustesse.

> NOTE : Les risques apportés par l'écosystème doivent être identifiés et traités.
> Un écosystème apportant des garanties suffisantes devrait théoriquement faire baisser la vraisemblance de ces risques.

Il est à noter que le système d'information, objet de l'homologation, est probablement défini comme partie prenante de « l'écosystème » d'un autre système d'information interconnecté.

Il convient donc qu'il lui apporte aussi les garanties nécessaires afin de ne pas affaiblir son propre écosystème.

Il est recommandé, lorsque cela est possible, de formaliser les garanties entre briques numériques au sein d'un contrat de service détaillant les engagements[24] et exigences[25] de sécurité de chaque partie.

> NOTE : Les garanties de sécurité apportées par chacune des briques numériques doivent être revues et maintenues durant toute la vie du système d'information.

24. Ce que la brique assure à « ses clients » en termes de sécurité

25. Ce que la brique demande à « ses fournisseurs » en termes de sécurité

Il est à noter que l'écosystème d'un système d'information à homologuer peut être composé de briques, elles-mêmes connectées à d'autres briques. L'origine et le niveau de sécurité de celles-ci doivent être contrôlés.

La frontière entre périmètre et écosystème n'est pas toujours évidente à identifier.

Le périmètre contient tous les objets qui permettent directement au système d'information de fonctionner et qui sont sous la responsabilité de l'autorité de l'homologation.

L'écosystème contient tous les objets qu'utilise le système d'information mais qui ne sont pas sous la responsabilité de l'autorité d'homologation, qui n'ont pas la même mission ou qui auraient été séparés du périmètre pour des raisons de simplification.

L'écosystème doit répondre aux exigences de sécurité minimums du périmètre. Les risques qu'il apporte doivent être identifiés et traités.

2.4 IDENTIFIER LES RÉGLEMENTATIONS APPLICABLES

Dans le cadre de la réglementation française, doivent être obligatoirement homologués avant toute mise en exploitation :

- les systèmes d'information traitant d'informations entre administrations ou entre administrations et administrés et devant appliquer la Politique de Sécurité des Systèmes d'Information de l'Etat (PSSIE), soumis au Référentiel Général de Sécurité (RGS[26]) ;
- les systèmes d'information soumis au décret n°2022-513[27] du 8 avril 2022 relatif à la sécurité numérique du système d'information et de communication de l'Etat et de ses établissements publics ;
- les systèmes d'information traitant d'informations restreintes publiques ou privées et soumis à l'Instruction Interministérielle 901 (II 901[28]) ;
- les systèmes d'information traitant d'informations classifiées et soumis à l'Instruction Générale Interministérielle sur la protection du secret de la défense nationale (IGI 1300[29]) ;
- les systèmes d'Information d'Importance Vitale (SIIV) au sein d'Opérateur d'Importance Vitale (OIV) dans le cadre de la Loi de Programmation Militaire (LPM[30]) ;

26. https://www.numerique.gouv.fr/publications/referentiel-general-de-securite

27. https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000045537693

28. https://www.legifrance.gouv.fr/download/pdf/circ?id=39217

29. http://www.sgdsn.gouv.fr/uploads/2016/10/igi-1300-20210809.pdf

30. https://www.legifrance.gouv.fr/jorf/article_jo/JORFARTI000028338907

… mais aussi, les règlementations internationales applicables en France :

- les systèmes d'information traitant d'informations classifiées de l'Union Européenne et soumis à l'Instruction Générale Interministérielle 2102 (IGI2102)[31] ;
- les systèmes d'information traitant d'informations classifiées de l'OTAN et soumis à l'Instruction Interministérielle 2100 (II2100)[32] ;

D'autres réglementations peuvent rendre obligatoire l'homologation de systèmes d'information. Il convient de rester informé à l'aide des sites gouvernementaux spécialisés.

31. https://www.legifrance.gouv.fr/download/pdf/circ?id=37307

32. https://www.legifrance.gouv.fr/download/pdf/circ?id=31869

2.5 RESPECTER LES RÉGLEMENTATIONS

Certaines réglementations définissent les exigences de sécurité (organisationnelles et techniques) applicables aux systèmes d'information amenés à traiter des informations sensibles.

Dans le cadre d'une démarche d'homologation, des particularités sont identifiées.

L'autorité d'homologation[33] :

- Par délégation du SGDSN[34], l'autorité d'homologation est l'ANSSI pour les systèmes d'information soumis aux réglementations suivantes :
  - l'Instruction Générale Interministérielle 1300 (IGI1300) pour les interconnexions entre systèmes d'information classifiés de même niveau dont l'un n'est pas sous maîtrise nationale ;
  - l'Instruction Générale Interministérielle 2102 (IGI2102) pour les systèmes d'information traitant d'informations classifiées de l'Union Européenne ;
  - l'Instruction Interministérielle 2100 (II2100) traitant d'informations classifiées de l'OTAN ;
- Pour toutes les autres réglementations, aucune exigence sur l'identité de l'autorité n'est spécifiée.

La durée de l'homologation :

- trois ans au maximum pour un grand nombre de systèmes d'information règlementés (voir tableau en page 32) ;
- trois ans au maximum pour les systèmes d'information soumis à l'IGI1300 et traitant d'informations classées SECRET ;
- deux ans au maximum pour les systèmes d'information soumis à l'IGI1300 et traitant d'informations classées TRES SECRET ;
- si aucune exigence réglementaire[35] n'impose de durée maximum d'emploi, l'ANSSI recommande fortement de ne pas dépasser trois ans.

33. Voir IGI1337 pour une définition complète de l'autorité d'homologation

34. Secrétariat Général de Défense et de Sécurité Nationale

35. Des politiques de sécurité des systèmes d'information (PSSI) propres aux organisations peuvent imposer des durées maximums.

Les contrôles spécifiques (audits[36]) :

- Des audits de conformité, technique et organisationnel doivent être réalisés pour les systèmes d'information soumis à :
  - l'Instruction Générale Interministérielle 1300 (IGI1300) pour les systèmes d'information traitant d'informations classifiées. Ils seront complétés par un audit TEMPEST[37] et un avis technique d'aptitude physique[38] du local hébergeant le système d'information ;
  - l'Instruction Générale Interministérielle 2102 (IGI2102) pour les systèmes d'information traitant d'informations classifiées de l'Union Européenne ;
  - l'Instruction Interministérielle 2100 (II2100) traitant d'information classifiées de l'OTAN ;
- Des audits organisationnels, de configuration et d'architecture doivent être réalisés pour les systèmes d'information soumis au :
  - Référentiel Général de Sécurité (RGS) pour les systèmes d'information traitant d'information entre administrations ou entre l'administration et un administré ;
  - Système d'Information d'Importance Vitale (SIIV). Les audits doivent être effectués par un Prestataire d'Audit de Sécurité des Systèmes d'Information (PASSI) qualifié par l'Etat français à travers le programme des visas de l'ANSSI ou par un prestataire qualifié[39].

36. Les types d'audits sont détaillés dans le paragraphe « audits de sécurité ».

37. L'audit TEMPEST a pour objectif de mesurer les performances relatives à la protection contre les signaux électromagnétiques compromettant. Il doit être effectué par des organismes accrédités par l'ANSSI (voir Instruction Interministérielle 300).

38. ATAP est un avis émis par le service enquêteur et portant sur la capacité physique des locaux à conserver et traiter des informations et supports classifiés (ISC).

39. L'opérateur peut réaliser lui-même l'audit ou recourir à un prestataire qualifié dans les conditions prévues au chapitre III du décret n° 2015-350 du 27 mars 2015.

En résumé, dans le cadre d'une démarche d'homologation, les points suivants sont à respecter :

	AUTORITÉ D'HOMOLOGATION	DURÉE MAXIMUM D'HOMOLOGATION	AUDIT SPÉCIFIQUE
IGI 1300	ANSSI sur délégation du SGDSN (uniquement TS faisant l'objet d'une classification spéciale[40])	TRES SECRET (TS) : 2 ans SECRET (S) : 3 ans	TEMPEST ATAP De conformité Technique Organisationnel
II 2100 (OTAN) IGI 2102 (EU)	ANSSI sur délégation du SGDSN	TRES SECRET (TS) : 2 ans SECRET (S) : 3 ans CONFIDENTIEL (C) : 3 ans RESTREINT (R) : 3 ans	TEMPEST (C, S et TS) ATAP (S et TS) Aptitude physique de conformité Technique Organisationnel
II 901 PSSIE IGI 1337	Aucune exigence	Recommandation ANSSI : 3 ans	Aucune exigence
RGS	Aucune exigence	Recommandation ANSSI : 3 ans	Configuration Architecture Organisationnel
LPM / SIIV	Aucune exigence	3 ans	Configuration Architecture Organisationnel et physique PASSI LPM obligatoire

Il est à noter que les réglementations sont amenées à évoluer, il convient de rester informé des éventuels changements impactant la démarche d'homologation.

Tout manquement à la réglementation peut entraîner la responsabilité de l'autorité de l'organisation et d'éventuelles sanctions.

NOTE : Les réglementations en vigueur définissant l'autorité d'homologation, sa durée et les audits associés doivent être appliquées.

40. voir Instruction Générale Interministérielle 1300

2.6 IDENTIFIER LES MESURES DE SÉCURITÉ À APPLIQUER

Les mesures de sécurité à appliquer doivent correspondre à la typologie et aux enjeux de sécurité du système d'information.

La bonne application de celles-ci permet de réduire un risque connu et ainsi de déjouer ou ralentir une attaque cyber.

Les mesures de sécurité à appliquer proviennent de plusieurs sources :

- des bonnes pratiques de sécurisation[41] des systèmes d'information ;
- des référentiels et réglementations en vigueur ;
- du plan d'actions issu de l'analyse de risque ;
- des résultats d'audit de sécurité ;
- des évènements de sécurité survenus ;
- des évolutions des menaces ;
- et de toute source pertinente.

Les mesures peuvent couvrir des aspects de gouvernance, de protection, de défense et de résilience.

Les politiques de sécurité[42] des systèmes d'information peuvent également ajouter des mesures applicables à l'ensemble des systèmes d'information d'une organisation.

Les règles qui la composent doivent être comprises et appliquées.

41. Guide de l'hygiène de l'ANSSI (https://cyber.gouv.fr/publications/guide-dhygiene-informatique)

42. La politique de sécurité des systèmes d'information (PSSI) décrit la stratégie de l'organisation en matière de sécurité des systèmes d'information. Elle doit être disponible, actuelle et révisée après chaque changement majeur impactant les systèmes d'information.

NOTE : Dans le cas d'une contradiction entre une politique de sécurité et une réglementation en vigueur, la réglementation doit être appliquée en priorité.
Lorsque deux réglementations imposent des mesures similaires, la plus restrictive doit être appliquée.

Il existe deux types de mesure :

- les mesures communes à une organisation, *par exemple, la sensibilisation des utilisateurs des systèmes d'information (RH-UTIL : II901) doit être dispensée à l'ensemble des collaborateurs d'une organisation ;*
- les mesures propres au système d'information à homologuer *comme l'élaboration des documents d'architecture (RES-CARTO : II901) qui doit correspondre au système d'information à homologuer ;*

Les mesures doivent être proportionnées aux risques qu'elles couvrent.

A ce titre, si l'application de la mesure coûte plus cher que le risque qu'elle couvre, il est envisageable de ne pas l'appliquer. Ce choix doit être justifié.

Il est fortement conseillé de suivre l'ensemble de ces mesures en identifiant celles qui peuvent être :

- entièrement appliquées ;
- partiellement ou pas appliquées ;
- pas applicables.

Pour chaque mesure, il est important de justifier son application ou sa non application[43]. Lorsqu'il est demandé, le retour sur investissement de la mesure (ROI) doit être étudié.

Dans certaines organisations, un suivi budgétaire des mesures peut s'avérer utile.

43. La non application d'une mesure peut être justifiée par son coût humain et financier plus important que l'impact sur le métier résultant d'un incident de sécurité lié à l'absence de la mesure.

Le suivi de toutes ces mesures (qui peut être comparé à une déclaration d'applicabilité[44]) permet de faire apparaître le taux de conformité du système d'information par rapport à la réglementation.

Il est à noter que toutes les mesures imposées par la réglementation doivent être appliquées lorsqu'elles sont applicables.

Par exemple, les mesures liées à la sécurisation des interconnexions ne seront pas applicables pour les systèmes d'information déconnectés de tout réseau.

> NOTE : Pour être efficace, une mesure de sécurité doit être appliquée, voire améliorée, tout au long de la vie du système d'information.

Un contrôle doit être effectué par la seconde ligne de maîtrise afin de s'assurer de la bonne application de la mesure. Ce contrôle peut être accompagné d'un audit.

44. La déclaration d'applicabilité (DdA) est une pièce maîtresse d'un SMSI dans le sens de la norme ISO27001.

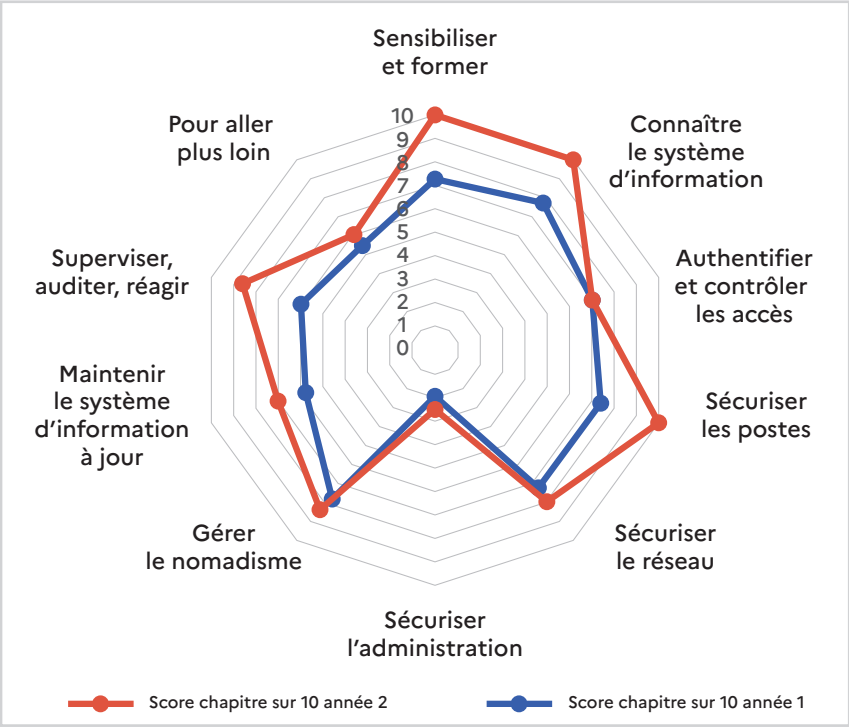
Pour évaluer l'efficacité d'une mesure de sécurité, il est fortement recommandé de créer des **indicateurs clés** (KPI[45]) permettant de suivre son évolution.

Ceux-ci, largement diffusables auprès de décideurs métiers permettent de fixer et de suivre les objectifs de sécurité principaux. Ils doivent être compréhensibles et utiles pour l'ensemble des personnes amenées à suivre l'évolution du système d'information. Ils permettent d'identifier rapidement les actions à prioriser pour renforcer la sécurité du système d'information.

Un indicateur de performance doit être pertinent, spécifique et atteignable par rapport à une cible.

Une représentation graphique améliore leur lisibilité.

EXEMPLE DE KPI



45. Key Performance Indicator : indicateur de performance

L'objectif d'une mesure pouvant être interprété, il convient de vérifier leur efficacité par rapport à l'objectif fixé. Dans ce cas, un contrôle par échantillon est envisageable.

2.7 ELABORER LA CARTOGRAPHIE DU SYSTÈME D'INFORMATION

La cartographie est un élément essentiel dans la sécurisation d'un système d'information. Suffisamment détaillée, elle permet une plus grande réactivité des équipes en cas d'incident ou d'attaque affectant le système d'information.

Elle facilite aussi le maintien en condition opérationnelle (MCO) et de sécurité (MCS).

> NOTE : Le périmètre de l'homologation doit clairement être identifié dans la cartographie.

La cartographie doit rendre lisibles et compréhensibles les différents aspects du système d'information.

De manière générale, la cartographie est composée de trois vues allant progressivement du métier vers la technique[46] .

- La vue métier décrit l'ensemble des processus et informations principales du système d'information. Il s'agit des « valeurs métiers » qui sont décrites dans le cadre de l'analyse de risque EBIOS Risk Manager ;
- La vue applicative présente les composants logiciels, les services et les flux de données qui les relient ;
- Enfin, la vue infrastructure illustre les différents équipements physiques et logiques du système d'information ainsi que toutes les informations permettant les communications réseau, comme *par exemple les plans d'adressage.*

46. Voir le guide de l'ANSSI https://cyber.gouv.fr/publications/cartographie-du-systeme-dinformation

De plus, une cartographie plus complète peut intégrer les éléments suivants :

- la liste des types de profil utilisant ou administrant le système d'information ;
- la liste des stratégies appliquées au système d'information (GPO) ;
- les informations essentielles au maintien en condition opérationnelle (MCO) et de sécurité du système d'information (MCS) ;
- les procédures liées à l'exploitation du système d'information ;
- les procédures permettant la résilience du système d'information.

Mais aussi :

- la liste des prestataires et fournisseurs informatiques contribuant à la mission du système d'information en incluant ceux de l'écosystème ;
- les contrats liant le système d'information à ceux interconnectés ;
- la liste et les contacts des partenaires internes et externes impliqués dans le système d'information ;
- l'inventaire (ou géolocalisation) des locaux dans lesquels est déployé le système d'information ;
- et toute information jugée utile à la connaissance et au maintien en fonctionnement du système d'information.

NOTE : Par définition, la cartographie d'un système d'information doit évoluer avec celui-ci. Il convient de la mettre à jour à chaque changement majeur du système d'information.

Afin d'éviter la démultiplication des documents, il est recommandé de ne maintenir qu'une seule cartographie par système d'information.

La cartographie doit être datée et/ou numérotée.

Le nom de la personne en charge de son maintien doit être clairement indiqué. Elle a la responsabilité d'apposer le niveau de confidentialité requis de la cartographie et ainsi permettre qu'elle ne soit consultable que par des personnes ayant le besoin d'en connaître.

La cartographie doit être sauvegardée dans un emplacement permettant son accès en cas d'indisponibilité complète du système d'information.

2.8 BÂTIR LES PLANS ET LES PROCÉDURES D'EXPLOITATION

Les procédures d'exploitation regroupent l'ensemble des instructions permettant de maintenir un système d'information performant et sécurisé durant tout le temps de son utilisation.

Les procédures d'exploitation peuvent couvrir un large éventail de tâches dont :

- la gestion des incidents ;
- la gestion des changements ;
- la gestion des sauvegardes et des restaurations ;
- la gestion des utilisateurs et des autorisations d'accès.

Les procédures d'exploitation doivent être rédigées, testées, appliquées et mises à jour selon un calendrier et une responsabilité définie. Elles doivent être accessibles aux personnes concernées.

Pour bâtir la liste des procédures à appliquer à un système d'information, il est primordial d'en connaître les éléments critiques. Pour ce faire, la cartographie est une aide précieuse.

Un mécanisme de traçabilité doit être mis en place afin de s'assurer qu'elles sont correctement effectuées par les équipes opérationnelles.

Les procédures d'exploitation doivent donner lieu à des indicateurs d'efficacité afin de suivre la santé du système d'information au sein d'un tableau de bord global.

PAR EXEMPLE :

	Mois de janvier	
DÉTAIL	ACTUEL	CIBLE
Volume sauvegardé / à sauvegarder	25To	25To
% de réussite	87%	90%
Nombre de restaurations effectuées dans la période	7	5

NOTE : Afin de garantir l'application des procédures d'exploitation, il est recommandé de les améliorer et de les évaluer régulièrement.

Par exemple :

- Si le système d'information et les données qu'il gère sont régulièrement sauvegardés, est-ce que des tests de restauration sont effectués ? Sont-ils concluants ?
- Si les comptes des utilisateurs sont revus, quel est le taux d'erreur ? Est-ce que la fréquence de revue est adaptée au public utilisateur ?
- Si le système d'information accepte l'intrusion de support USB, quelle est la procédure de nettoyage des clés ? Est-elle vérifiée ?
- Si un procédé de continuité d'activité est défini, a-t-il été testé ?
- Si le système d'information est situé dans un local sécurisé, est-ce que les accès physiques ont bien été contrôlés ?
- etc.

Afin de maintenir la sécurité du système d'information, des plans spécifiques doivent être appliqués :

- le plan de maintien en condition opérationnelle (MCO) ;
- le plan de maintien en condition de sécurité (MCS) ;
- le plan de résilience.

NOTE : Les plans doivent être rédigés par les équipes opérationnelles (première ligne de maîtrise).
La seconde ligne de maîtrise doit s'assurer de leur mise en place, de leur pertinence et de leurs bonnes applications.

2.8.1 LE PLAN DE MAINTIEN EN CONDITION OPÉRATIONNELLE (MCO)

Les procédures permettant de limiter les dysfonctionnements qui empêcheraient le système d'information d'accomplir sa mission font partie du plan de maintien en condition opérationnelle.

Le MCO regroupe les processus permettant de garantir à la fois la maintenance préventive, la maintenance corrective et l'obsolescence des équipements.

- La maintenance préventive regroupe tous les contrôles effectués avant qu'une panne ne survienne.
  Par exemple la vérification de l'espace libre restant sur un disque amené à recevoir de l'information ;
- La maintenance corrective qui détaille le plan de réparation après un dysfonctionnement.
  Par exemple la procédure de changement d'un disque dur endommagé sur un serveur en exploitation.

D'autres types de maintenance peuvent être ajoutés au plan de maintien en condition opérationnelle comme les maintenances évolutives et adaptatives qui consistent à intégrer de nouvelles fonctionnalités au système d'information en fonction des évolutions demandées ou de son environnement.

Les procédures de maintien en condition opérationnelle doivent aussi inclure les procédures d'achat, d'anticipation d'approvisionnement, de stockage des équipements critiques ainsi que la gestion des obsolescences. Les procédures de décommissionnement d'une partie ou de la totalité du système d'information doivent aussi être détaillées.

Les risques identifiés ne permettant pas d'exécuter pleinement les procédures de maintien en condition opérationnelle doivent être identifiés et déclinés sous forme d'actions.

Par exemple, une pénurie sur une pièce de rechange ne permettant pas un remplacement dans les temps impartis.

L'objectif du MCO est de minimiser les temps d'arrêt du système d'information et de garantir que celui-ci fonctionne à un niveau de performance voulu et adapté.

Les indicateurs importants de performance doivent être communiqués à la seconde ligne de maîtrise.

> NOTE : Les procédures du MCO peuvent être globales à un ensemble de systèmes d'information.

2.8.2 LE PLAN DE MAINTIEN EN CONDITION DE SÉCURITÉ (MCS)

Les procédures du plan de maintien en condition de sécurité ont pour objectif de corriger les vulnérabilités du système d'information avant qu'elles ne soient exploitées.

Le MCS doit détailler les procédures d'application des correctifs des systèmes d'exploitation et logiciels installés sur le système d'information.

Trois phases doivent être identifiées :

- La **surveillance** décrit la stratégie employée pour que les nouvelles vulnérabilités numériques soient communiquées aux personnes en charge de la sécurité du système d'information[47] ;
- La **reconnaissance** identifie les vulnérabilités pouvant impacter le système d'information. Cette phase doit se baser sur la cartographie du système d'information correctement mise à jour ;
- L'**application des correctifs** est la phase permettant de mettre à jour régulièrement ou de façon urgente les composants impactés sans perturber le fonctionnement du système d'information. Dans les environnements très critiques, elle doit être précédée d'une procédure de tests.

  Lorsque les correctifs ne peuvent pas être appliqués pour des raisons organisationnelles ou opérationnelles, il convient de mettre en place des bulles de confiance afin de contenir les éventuelles menaces liées aux vulnérabilités non corrigées.

Le plan de maintien en condition de sécurité doit être bâti en collaboration avec les équipes opérationnelles et de support, en charge de la sécurité des systèmes d'information. Il peut être opportun d'avoir un plan global à une organisation.

47. Le centre de veille, d'alerte et de réponse CERT est une bonne source d'information https://www.cert.ssi.gouv.fr/

NOTE : Le plan de maintien en condition de sécurité peut être fusionné avec celui de maintien en condition opérationnelle.

2.8.3 LE PLAN DE RÉSILIENCE

En dépit de toutes les protections apportées pour renforcer sa sécurité, un système d'information n'est pas à l'abri d'un événement provoquant son dysfonctionnement ou son arrêt. Un plan de résilience doit être mis en place.

La résilience est la capacité pour un système d'information à surmonter les altérations provoquées par un élément perturbateur, puis à retrouver un fonctionnement normal.

Un système d'information critique pour une organisation doit être intégré au plan de continuité des activités (PCA). Celui-ci se définit comme la capacité d'une organisation à poursuivre la livraison de produits et la fourniture de services dans des délais acceptables à une capacité prédéfinie durant une perturbation[48].

Un document de résilience doit détailler les différentes mesures envisagées en cas d'évènement majeur impactant le fonctionnement du système d'information.

Sans être exhaustif, le document de résilience doit au minima détailler les points suivants :

- la durée maximale d'interruption[49] du système d'information avant que des effets soient irréversibles pour l'organisation ;
- le délai nécessaire pour la remise en route[50] du système d'information après incident. Il s'agit d'un objectif ;
- les procédures de gestion de crise ;
- les procédures de gestion du plan de continuité et de reprise d'activité.

48. ISO22300:2021 (https://www.iso.org/obp/ui/#iso:std:iso:22300:ed-3:v1:fr)
49. MTPD en anglais pour Maximum Tolerable Period of Disruption
50. RTO : Recovery Time Objective

Le plan de résilience doit correspondre à la criticité du système d'information pour l'organisation. Plus le système est critique et plus le plan doit être détaillé et testé.

Le plan doit être accompagné d'un volet concernant la gestion de crise et plus particulièrement la crise d'origine cyber[51].

> NOTE : Pour rester synthétique, il est fortement recommandé de ne pas répéter ou détailler les mesures de résilience communes à l'ensemble des systèmes d'information de l'entité, une simple référence aux documents correspondants est suffisante.

51. https://cyber.gouv.fr/anticiper-et-gerer-une-crise-cyber : Anticiper et gérer une crise Cyber

2.9 IDENTIFIER ET TRAITER LES RISQUES

Avant de mettre en service un système d'information, les risques liés à son emploi doivent être identifiés, traités et acceptés par une autorité responsable.

> NOTE : Il convient d'employer une méthode d'analyse de risque adaptée, validée par la politique de sécurité de l'entité ou, à défaut, par l'autorité d'homologation[52] .

L'analyse de risque doit se focaliser sur le périmètre, objet de l'étude sans omettre les risques liés à son écosystème. Elle doit en dégager sa mission et les principaux processus et informations qui sont indispensables à la réalisation de cette mission (les valeurs métiers).

Pour rappel, un risque est la combinaison d'un événement redouté et d'un scénario de menaces. Le niveau de risque est apprécié en fonction de sa gravité et de sa vraisemblance.

L'analyse permet d'identifier les risques, de les hiérarchiser et de les traiter[53] afin de les amener à terme à des niveaux acceptables pour l'autorité d'homologation.

La criticité et l'exposition[54] du système d'information a un impact sur la profondeur de l'analyse de risque à mener :

- pour un système peu critique et faiblement exposé aux menaces numériques, une étude de conformité aux mesures de sécurité du guide d'hygiène informatique de l'ANSSI[55], complété, le cas échéant de guides thématiques adaptés[56] ou encore des recommandations des éditeurs et de la réglementation en vigueur suffit ;

52. Lorsque l'ANSSI est autorité d'homologation, l'utilisation de la méthode EBIOS RM est obligatoire. Dans tous les autres cas, elle est fortement recommandée.

53. Pour rappel, traiter un risque nécessite de l'accepter, de le réduire, de le transférer ou de le refuser (cf méthode EBIOS RM)

54. Voir chapitre 3.2.1 et 3.2.2

55. https://cyber.gouv.fr/publications/guide-dhygiene-informatique

56. Par exemple le guide « sécuriser un site web » de l'ANSSI : https://cyber.gouv.fr/publications/securiser-un-site-web

- Pour un système plus critique et/ou plus exposé, une analyse de risque est recommandée permettant d'identifier les risques principaux pour le système d'information ;
- Enfin pour un système plus critique à une organisation et/ou exposé, une analyse de risque complète doit être réalisée afin de bien prendre en compte la menace intentionnelle. Des scénarios d'attaques vraisemblables doivent alors être bien pris en compte.

> NOTE : Les actions permettant de traiter les risques doivent être réalisées avant la mise en service du système d'information ou planifiées dans un délai raisonnable en accord avec l'autorité d'homologation.

Le plan de traitement des risques doit être suivi et régulièrement mis à jour en prenant en compte les nouvelles actions provenant de l'évolution du système d'information, de son écosystème, du contexte d'utilisation et des menaces cyber. Il doit être intégré dans un plan d'action général.

La vraisemblance d'un risque évolue en fonction des menaces, de l'écosystème et du contexte dans lesquels évolue le système d'information. Il convient de la surveiller sous forme d'indicateurs (KRI[57]).

57. Key Risk Indicator (indicateur clé de risque)

2.10 AUDITER LE SYSTÈME D'INFORMATION

Il convient, une fois les mesures de sécurité appliquées, de tester la robustesse d'un système d'information face aux menaces numériques par l'intermédiaire d'une série d'audits.

Le périmètre choisi pour effectuer ces audits doit correspondre à celui défini lors de l'identification du périmètre de l'étude.

L'audit doit être effectué par des auditeurs indépendants et de confiance. L'audit doit être cadré et autorisé par le responsable du système d'information et par sa hiérarchie. Dans le cadre des systèmes classifiés, les auditeurs doivent être habilités au niveau du système d'information.

Le temps consacré à un audit doit être suffisant.

L'auditeur doit être libre de proposer ses propres scénarios.

Il est à noter que les réglementations rendent obligatoires certains audits :

- de conformité : le système d'information est-il conforme aux réglementations applicables ?
- organisationnel : la structure humaine mise en place pour sécuriser le système d'information est-elle suffisante et adaptée ? Bénéficie-t-elle de suffisamment de moyens pour garantir sa sécurité ? La documentation est-elle pertinente ?
- de configuration : les éléments du système d'information sont-ils bien paramétrés pour répondre aux enjeux de sécurité actuels ?
- d'architecture : la mise en œuvre technique et organisationnelle d'un système d'information est-elle cohérente au regard de ses objectifs de sécurité ?
- technique : regroupe tous les audits ayant attrait aux éléments techniques (architecture, configuration, intrusion) ;
- TEMPEST[58] : permet de se protéger des menaces issues des rayonnements électromagnétiques.

58. TEMPEST : Instruction Générale Interministérielle 300 (https://cyber.gouv.fr/ii-300sgdsnanssi)

D'autres types d'audit sont possibles[59] et sont adaptés à la nature du système d'information :

- les revues de code ;
- les tests de pénétration ou d'intrusion (pentest) ;
- les primes à la recherche de bogues (bug bounty).

Les audits peuvent identifier des non-conformités mineures et majeures.

Les audits permettent de vérifier l'efficience et l'efficacité des mesures de sécurité mises en place et identifier des scénarios qui n'auraient pas été pris en compte lors de l'analyse de risque.

Les vulnérabilités identifiées devront donner lieu à des actions permettant leur remédiation et seront intégrées au plan d'action.

La fréquence des audits doit correspondre :

- au changement des enjeux, du contexte ou de la menace ;
- à l'avancement des actions identifiées et corrigées lors des derniers audits ;
- aux disponibilités des ressources et des budgets alloués.

Lorsque cela est possible, il est préférable d'alterner le type d'audit afin de couvrir le maximum de vulnérabilités pouvant être exploitées par une menace.

59. Liste non exhaustive

2.11 APPLIQUER LE PLAN D'ACTION

L'amélioration de la sécurité d'un système d'information doit être une action menée dès sa conception et jusqu'à son décommissionnement.

Toutes ces actions permettent de réduire les risques et doivent être compilées dans un document unique, le plan d'action.

> NOTE : Le plan d'action doit être le regroupement des actions permettant de traiter les non-conformités réglementaires, de réduire les risques identifiés (le plan de traitement des risques - PTR), de mitiger les vulnérabilités identifiées lors des audits et de traiter des évènements et incidents de sécurité.

Pour être exploitable, il doit recenser des actions réalistes et utiles. La méthode SMART peut être utilisée :

- L'action doit être Spécifique au risque à diminuer ou à la mesure à appliquer ;
- Le résultat de l'action doit être Mesurable ;
- L'objectif de l'action doit être Atteignable et Réaliste ;
- Enfin l'action doit être Temporellement définie.

Il est à noter qu'une action peut adresser plusieurs risques.

> NOTE : Le plan d'action est la pierre angulaire de l'amélioration continue et doit permettre le renforcement de la sécurité du système d'information.

Un propriétaire nommé, une complexité, un délai et une date d'exécution doivent au minima être renseignés.

Les coûts associés à la réalisation de l'action peuvent être intégrés au plan.

PAR EXEMPLE :

Nom de l'action	Commentaires	Justification	Propriétaire	Complexité De + à +++	Date fin prévue
Suppression des services réseau non utilisés	Suppression des services telnet et http sur tous les serveurs, postes de travail et équipements réseau – environ 120 équipements	Respect du guide d'hygiène informatique	Responsable DSI : M ou Mme X	+	Février 2026

Toutes les informations utiles pour le suivi des actions doivent être ajoutées.

Les actions doivent être priorisées.

- Les actions permettant de traiter les risques ayant le plus grand impact et étant les plus vraisemblables doivent être effectuées en priorité.
- Les actions ayant une marge d'amélioration élevée sur la sécurité du système d'information sont aussi à privilégier.

L'ESSENTIEL :

Une gouvernance claire doit être mise en place afin d'atteindre l'objectif de sécurisation et d'homologation d'un système d'information. Le modèle en trois lignes de maîtrise permet de distribuer et de contrôler les tâches à accomplir.
Le périmètre du système d'information et son écosystème avec lequel il communique doivent être clairement définis.

Les mesures de sécurité issues de la réglementation et des politiques de sécurité auxquelles le système d'information correspond doivent être appliquées. Les mesures doivent être proportionnelles aux enjeux de sécurité du système d'information, dans son contexte.

Pour les systèmes les plus critiques[60] ou exposés[61] :

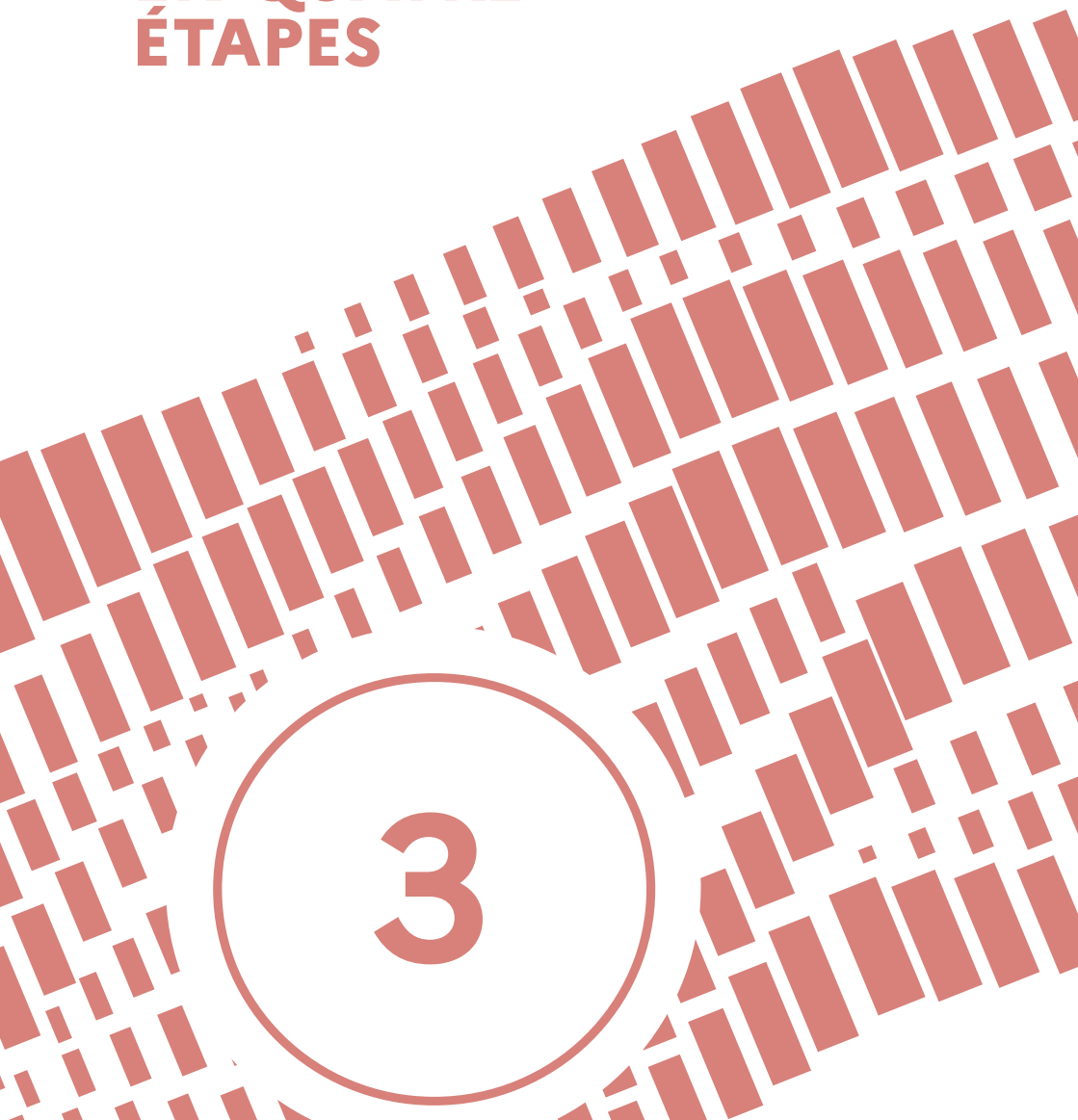
- Les plans opérationnels (MCO) de sécurité (MCS) et de résilience (PCA/PRA) doivent être identifiés et appliqués.
- Les risques liés à l'utilisation du système d'information et à son périmètre doivent être identifiés et traités lors d'une analyse de risque.
- Des audits doivent être réalisés.

Un plan d'action reprenant l'ensemble des mesures permettant de mettre en conformité le système d'information ou de réduire ses risques liés à son emploi doit être suivi.

60. voir chapitre « Evaluer la criticité du système d'information »

61. voir chapitre « Evaluer l'exposition du système d'information »

HOMOLOGUER EN QUATRE ÉTAPES



La démarche d'homologation d'un système d'information permet à l'autorité responsable de prendre connaissance des risques liés à son utilisation et de les accepter. Il s'agit de l'autorité d'homologation (AH).

Homologuer un système d'information autorise son emploi.

3.1 PREMIÈRE ÉTAPE : CONSTITUER LE COMITÉ D'HOMOLOGATION

Afin d'éclairer la décision d'homologation, un avis doit être rendu par le comité d'homologation. Celui-ci est présidé et animé par un responsable. Il s'agit généralement du responsable de la sécurité des systèmes d'information (RSSI) ou du conseiller à la sécurité numérique (CSN) pour les entités publiques.

Le comité d'homologation doit être constitué avant la mise en service du système d'information et avant chaque ré-homologation. Il peut regrouper autour de son responsable les profils suivants :

- Les responsables « métiers » qui apportent la connaissance des enjeux liés à l'utilisation du système d'information ;
- L'équipe en charge de la conception du système d'information qui peut être composée de la Maîtrise d'Ouvrage[62] (MOA) et/ou de la Maîtrise d'Œuvre[63] (MOE) ;
- L'équipe support (DSI) qui a la charge d'appliquer les procédures d'exploitation du système d'information ;
- Les auditeurs qui permettent d'identifier les écarts techniques, d'organisation ou de configuration par rapport aux objectifs de sécurité ;
- Les « experts » qui aident à guider la démarche ou à mener des ateliers de travail ;
- Le gestionnaire des risques[64] et ou le responsable de la conformité de l'organisation ;
- Tout interlocuteur nécessaire à la remise de l'avis de sécurité.

62. La maîtrise d'ouvrage est chargée de la définition du projet. Le maître d'ouvrage est le commanditaire du projet.

63. La maitrise d'œuvre est chargée de la conception.

64. Risk manager

NOTE : Le responsable du comité d'homologation doit s'assurer que les personnes qui l'accompagnent soient identifiées, disponibles et engagées.

Les contributeurs peuvent être internes ou externes à l'organisation. Il est néanmoins nécessaire que toutes les personnes devant participer à la démarche d'homologation soient sensibilisées et pour les systèmes classifiés aient le bon niveau d'habilitation.

NOTE : Il est important que chaque membre du comité soit impartial quant à l'avis de sécurité à proposer, quels que soient les intérêts à mettre ou à maintenir en service le système d'information.

3.2 SECONDE ÉTAPE : IDENTIFIER LE NIVEAU DE LA DÉMARCHE D'HOMOLOGATION

La démarche d'homologation est le processus qui permet de collecter, d'évaluer, d'émettre et de présenter à l'autorité un avis de sécurité.

L'avis doit s'appuyer sur la documentation constituée par les équipes support (première ligne de maîtrise).

Le niveau de la démarche est à identifier en fonction de la criticité du système d'information et de son exposition face aux sources de risques numériques.

L'ANSSI propose trois niveaux progressifs de démarche[65] (plus le niveau est élevé et plus le besoin de sécurisation doit être renforcé).

- Le niveau simplifié est adapté à un système d'information peu ou pas critique pour son organisation. Il peut s'agir *par exemple* d'un site internet vitrine, d'un système d'information interne basé sur un poste isolé, etc. La documentation demandée est minimale ;
- Le niveau intermédiaire est destiné aux systèmes un peu plus critiques ou exposés à ses sources de risque, traitant *par exemple* des données personnelles ;
- Enfin le niveau renforcé est adapté à tous les systèmes d'information devant gérer des informations sensibles ou ayant une importance critique pour une organisation.

La sélection du niveau est déterminante pour mener la démarche et peut être sujette à débat.

Le questionnaire d'évaluation de la criticité et de l'exposition aux sources de risque est proposé afin de guider dans cette sélection.

Il doit être justifié dans le document d'accompagnement qui présentera succinctement le système d'information.

65. Le nom des niveaux est proposé mais peut être adapté à l'organisation. Il est néanmoins important de garder ces trois niveaux.

3.2.1 EVALUER LA CRITICITÉ DU SYSTÈME D'INFORMATION

L'évaluation et la définition de la criticité d'un système d'information sont souvent représentées comme une action difficile à appréhender. Mais une approche simple et pragmatique, sous forme de questions, sur l'importance du système d'information et sur les conséquences d'une défaillance permet d'y répondre :

- Quels sont les impacts pour l'organisation ou les usagers en cas d'arrêt total du système d'information ?
- Quels sont les impacts pour l'organisation ou les usagers si les données traitées par le système d'information sont divulguées à des personnes ne devant pas y avoir accès ?
- Quels sont les impacts pour l'organisation ou pour les usagers si les données traitées par le système d'information sont effacées ou sont corrompues par accident ou suite à un acte malveillant ?

Afin de bien appréhender les conséquences, il convient d'apprécier les différents impacts sous différents angles[66] :

- biens et personnes ;
- financier ;
- juridique et contractuel ;
- image ;
- environnementaux ;
- ...

Il est préférable que le niveau de l'impact soit mesuré à l'aide d'échelles de gravité déjà existantes au sein de l'organisation. A défaut, l'échelle suivante peut être utilisée :

- impact mineur : l'impact est négligeable ;
- impact modéré : l'impact a des conséquences significatives mais surmontables malgré quelques difficultés ;
- impact important : l'impact a des conséquences importantes qui peuvent être surmontées avec des difficultés réelles ;
- impact critique : l'impact a des conséquences graves, voire irrémédiables sans doute insurmontables. La « survie » de l'organisation peut être engagée.

66. Une grille plus complète des risques existe dans le guide EBIOS RM de l'ANSSI.

3.2.2 EVALUER L'EXPOSITION DU SYSTÈME D'INFORMATION

L'exposition du système d'information aux risques numériques peut être connue en se posant les questions suivantes :

- Est-ce que le système d'information est accessible par un réseau qui n'est pas dans le périmètre, *par exemple* internet ?
- Est-ce que le système d'information est accessible uniquement par une population connue (employés, partenaires…) ?
- Est-ce que le système d'information est accessible par des équipements qui ne sont peu ou pas maîtrisés, *par exemple* des équipements de type IoT[67] ou BYOD[68].
- Est-ce que tous les lieux qui permettent l'accès au système d'information sont sécurisés ? Peut-on accéder au système d'information à partir d'un domicile (télétravail) ?
- Est-ce que les personnes chargées de la maintenance du système d'information sont de confiance et utilisent des équipements contrôlés ?
- Est-il facile de maintenir la sécurité du système d'information ?

Ces questions, dont la liste n'est pas exhaustive, ont pour objectif d'éclairer le comité d'homologation sur les vecteurs d'attaque pouvant être utilisés par des attaquants.

67. Internet Of Things (L'Internet des choses) sont les équipements physiques qui intègrent des technologies de captation et de connexion. Les IoT ne sont pas réputés pour leur sécurité informatique.

68. Bring Your Own Device (Apporter votre propre équipement personnel de communication) désigne l'usage d'équipement personnel dans un environnement professionnel. Ce principe permet une plus grande flexibilité en termes de choix de matériel mais entraîne une difficulté de gestion supplémentaire.

L'échelle ci-après peut être utilisée pour déterminer le niveau d'exposition, selon une vue macroscopique, du système d'information :

- nul : Le système d'information n'est ouvert sur aucun réseau et le transfert d'information est réalisé à l'aide de supports amovibles de confiance. L'accès au système est possible au seul personnel habilité par l'entité ;
- faible : Le système d'information est ouvert uniquement sur des réseaux maîtrisés (*par exemple sur un intranet*). L'accès au système est possible au seul personnel habilité par l'entité et n'autorise pas les accès nomades ;
- important : Le système d'information est indirectement ouvert sur des réseaux non maîtrisés (*par exemple à l'aide d'interconnexion de SI avec tunnel TLS*). L'accès au système est possible aux personnels habilités par l'entité et/ou à ceux d'entités tierces et n'autorise que certains accès nomades ;
- total : Le système d'information est directement ouvert sur Internet pour tous les types d'utilisateurs et d'équipements.

Il est à noter que l'exposition du système d'information aux sources de risque numérique est liée au niveau de la menace. Il existe trois types de menace :

- La menace activiste ou isolée qui regroupe des individus ayant peu de moyens, utilisant des outils peu sophistiqués. Ils peuvent néanmoins bénéficier d'accès privilégiés.
- La menace systémique peut affecter une large proportion d'entités. Les attaques liées à cette menace ont principalement un but lucratif. Les auteurs de ces attaques utilisent généralement des outils du marché de type rançongiciels.
- Enfin la menace stratégique s'illustre par la conduite d'attaques informatiques persistantes et ciblées. Elles peuvent être orchestrées par des états ou des grandes organisations, motivées et possédant d'importantes ressources.

NOTE : L'exposition d'un système d'information dépend de ses sources de risque identifiées et du niveau de menace.

3.2.3 SELECTIONNER LE NIVEAU DE DEMARCHE DE L'HOMOLOGATION

La sélection du niveau de la démarche doit faire l'objet d'un consensus entre les membres du comité d'homologation.

Il est à noter que le niveau de démarche d'homologation sélectionné peut évoluer tout au long de la vie du système d'information.

La matrice de correspondance ci-après vise à apporter une aide à la décision dans la sélection finale de la démarche d'homologation

Sélection du niveau de la démarche d'homologation de la sécurité

	Exposition* nulle	Exposition faible	Exposition importante	Exposition totale
Criticité** maximale	Intermédiaire	Renforcé	Renforcé	Renforcé
Criticité importante	Intermédiaire	Intermédiaire	Renforcé	Renforcé
Criticité modérée	Simplifié	Simplifié	Intermédiaire	Intermédiaire
Criticité mineure	Simplifié	Simplifié	Simplifié	Intermédiaire

* Le niveau d'exposition (aux sources de risque) doit directement dépendre du contexte dans lequel le système d'information est utilisé. Il peut être mesuré en fonction de la confiance accordée aux personnes ou services qui y ont accès de façon directe (par exemple via un réseau) ou indirecte (par exemple en « rebondissant » sur d'autres systèmes d'information).

** La criticité du système d'information est identifiée en fonction de l'échelle d'impact de l'organisation.

Le niveau de démarche choisi influe directement sur la liste des livrables qui permettent de constituer le dossier d'homologation.

Par exemple, une analyse de risque n'est pas nécessaire pour un système d'information de criticité mineure et ayant une exposition aux risques numériques quasi nulle. Une approche par conformité[69] *et une application des guides d'hygiène numériques permettant de couvrir les principaux risques.*

NOTE : La sélection du niveau de la démarche d'homologation ne doit pas dépendre de la complexité du système d'information, mais de sa criticité, de son exposition aux sources de risques numériques et au niveau de la menace.

La nature des travaux à effectuer dans le cadre de l'homologation est étroitement liée au niveau de la démarche retenu.

69. Cette approche correspond à l'analyse des écarts au socle de sécurité réalisée lors du premier atelier de la méthode EBIOS RM.

3.2.4 CONSTITUER LE DOSSIER D'HOMOLOGATION

Le comité d'homologation a la responsabilité de rassembler l'ensemble de la documentation nécessaire permettant de formuler un avis de sécurité sur le système d'information. Pour rappel, les documents doivent être rédigés par les « sachants » tout au long de la conception du système d'information. Ils doivent être maintenus à jour durant son exploitation.

> NOTE : La documentation constituant le dossier d'homologation doit exister pour le suivi et la sécurisation du système d'information, mais ne doit pas être spécifiquement rédigée pour la démarche d'homologation.

Il est à noter que les pièces du dossier d'homologation doivent être protégées et classifiées au juste besoin. Elles ne doivent être accessibles que par les personnes concernées ayant le besoin d'en connaître.

> NOTE : Les pièces qui composent le dossier d'homologation permettent de comprendre le système d'information ainsi que les risques liés à son emploi. Elles doivent être claires et utiles aux équipes qui en ont la charge. Il convient donc de privilégier la qualité à la quantité.

Un document d'accompagnement (ou de synthèse) destiné à la commission d'homologation et résumant le système d'information et les travaux de sécurisation effectués doit être rédigé, généralement par la seconde ligne de maîtrise ou par le responsable métier. Il doit répondre au minima aux questions suivantes.

- A quoi sert le système d'information ?
- Quel est le périmètre précis du système d'information à homologuer ?
- Quel est le contexte métier et technique du système d'information ?
- Quelles sont les informations qu'il traite ?
- Quels sont les flux d'informations entrants et sortants du système d'information ?
- De quoi est-il composé ? (Technologie, volumétrie)
- Comment est-il employé ? Qui sont ses utilisateurs ?
- Quelle est sa criticité pour l'organisation ?
- Quelle est son exposition face aux menaces numériques ?
- A quelles politiques et réglementations le système d'information doit-il être conforme ?
- Quel est son taux de conformité par rapport à ces politiques et réglementations ?
- Quelles sont les procédures mises en place pour maintenir le système d'information en état de marche et de sécurité ?
- Comment la sécurité du système d'information a-t-elle été éprouvée ?
- Quels sont les risques susceptibles de porter atteinte au système d'information et quelles sont les mesures prises pour les traiter ?
- Quels sont les risques résiduels liés à l'exploitation du système d'information ?
- Qui administre le système d'information ?
- Quelles sont les actions initiées pour améliorer la sécurité du système d'information ?
- Dans le cas où le système d'information est déjà en cours d'utilisation, que s'est-il passé depuis sa mise en service ?

Le document d'accompagnement doit être succinct, d'une à deux pages et doit être mis à jour pour chaque commission d'homologation.

Le niveau de la démarche sélectionné a un impact sur les informations à communiquer au comité d'homologation. Une démarche renforcée pour un système d'information critique nécessite un plus grand nombre d'éléments à fournir.

Par exemple, une démarche d'homologation de niveau renforcé implique la tenue d'une analyse de risque complète, ce qui n'est pas le cas pour une démarche de niveau simplifié.

En fonction du niveau de la démarche retenu, le tableau suivant définit les pièces que le comité d'homologation doit rassembler et étudier.

Pièces du dossier à présenter	Simplifié	Intermédiaire	Renforcé
Document d'accompagnement (présentation du système d'information dans son contexte et justification de la sélection de la démarche)	X	X	X
Dossier d'architecture technique		X	X
Matrice de conformité	X	X	X
Analyse de risque*	X **	X **	X
Procédures d'exploitation***		X	X
Plan de maintien en condition opérationnelle***		X	X
Plan de maintien en condition de sécurité***		X	X
Plan d'action	X	X	X
Plan de résilience			X
Audits		X	X
« Historique » du système d'information ****	X	X	X

* Les conformités avec le socle de sécurité, le socle réglementaire et les politiques de sécurité des systèmes d'information sont étudiées lors de l'analyse de risque.

** Dans le cadre d'une analyse de risque EBIOS RM, tous les ateliers ne sont pas nécessaires (*par exemple seuls les ateliers 1 et 5 doivent être effectués*).

*** Sont généralement communs à l'ensemble des systèmes d'information de l'organisation.

**** Pour les systèmes d'information déjà en exploitation, l'historique regroupe, au minima, ses grands évènements et incidents de sécurité, ses changements techniques et organisationnels et ses précédentes homologations.

3.3 TROISIÈME ÉTAPE : ÉVALUER LES PIÈCES DU DOSSIER D'HOMOLOGATION

Le comité d'homologation doit s'assurer que les procédures de sécurité existent, qu'elles correspondent bien aux enjeux de sécurité et qu'elles soient bien appliquées.

Elles doivent être documentées.

Les mesures appliquées doivent être analysées et évaluées de façon pragmatique afin d'obtenir un niveau de confiance suffisant pour l'emploi du système d'information.

Il est souvent utile d'organiser des sessions de questions-réponses avec les auteurs des documents pour aller au-delà des écrits.

> NOTE : Les informations échangées lors de la démarche d'homologation doivent être traitées au bon niveau de classification en appliquant la réglementation en cours.

En s'appuyant sur les documents collectés, le comité d'homologation doit pouvoir émettre un avis sur la sécurité du système d'information.

L'avis doit se baser sur la confiance que le comité obtient en analysant la documentation et en échangeant avec ses auteurs. Il doit vérifier que toutes les étapes de sécurisation ont bien été respectées.

Il est à noter que la documentation doit être adaptée à la démarche et au périmètre du système d'information à homologuer.

Le comité d'homologation n'a pas pour vocation de produire de la documentation sur le système d'information ou de l'auditer.

3.3.1 EMETTRE UN AVIS D'HOMOLOGATION

Le comité doit proposer un avis d'homologation du système d'information à l'autorité d'homologation. Celui-ci doit être justifié.

Deux cas se présentent :

- **Le système d'information n'est pas prêt à être homologué :**

  Malgré tous les travaux de sécurisation, la mise en route du système d'information entraîne trop de risques pour l'organisation. Le système d'information ne doit pas être employé en l'état. A ce stade, il n'est pas nécessaire d'organiser une commission d'homologation. Néanmoins, il est important de communiquer les risques aux différents acteurs et à l'autorité d'homologation.

> NOTE : Ne pas donner d'avis positif sur la sécurité d'un système d'information est un signal fort. Il permet d'alerter sur le manque de maturité d'un système d'information.
> Cet avis peut permettre un déblocage de ressources humaines et budgétaires.

- **Le système d'information est prêt à être homologué :**

  Les risques liés à l'utilisation du système d'information ont été identifiés et sont traités pour rendre leur vraisemblance acceptable ;

  ou

  Les enjeux du système d'information nécessitent qu'une autorisation d'emploi soit accordée, même si sa sécurisation n'est pas satisfaisante. Une revue du système d'information devra être planifiée dans un délai court ;

  et

  Le plan d'action permettant de maintenir et de renforcer la sécurité du système d'information est acceptable.

NOTE : Si le contexte le permet, il est préférable de repousser la date de remise de l'avis d'homologation afin de laisser le temps aux équipes en charge d'appliquer de nouvelles mesures de sécurité, plutôt que d'autoriser son emploi pour une période trop courte.

Pour des systèmes d'information ayant des risques résiduels trop importants mais devant être homologués pour des raisons stratégiques ou politiques, un avis d'homologation « sous réserve » peut être proposé.

Celui-ci permet d'autoriser l'emploi du système d'information et nécessite que les actions identifiées pour lever les réserves soient menées dans un délai de 12 mois maximum.

La levée de réserves permet au système d'information de garder son homologation au-delà de la période définie.

3.3.2 SIMPLIFIER ET ACCÉLÉRER LA DÉMARCHE D'HOMOLOGATION

Le mécanisme de simplification suivant peut être adopté :

- **pour les systèmes d'information peu critiques et peu exposés aux sources de risques numériques (niveau de démarche d'homologation simplifiée) :**

  La première ligne de maîtrise (équipe opérationnelle) déclare que toutes les mesures de sécurité identifiées et nécessaires pour protéger le système d'information, ses données et ses usagers sont appliquées.

  Dans ce cas, un avis positif de sécurité peut être émis par la seconde ligne de maîtrise (équipe fonctionnelle).

  Une fois validé par l'autorité d'homologation, l'emploi du système d'information est autorisé.

  Il est à noter qu'une commission n'est pas obligatoire pour ce cas et une validation sur support électronique est suffisante. L'enregistrement de la décision doit être effectué.

Même lorsque le système d'information est homologué, l'ANSSI recommande de contrôler la bonne application des mesures de sécurité, conformément aux déclarations de la première ligne de maîtrise.

Si plusieurs systèmes d'information sont dans ce cas, un contrôle par échantillonnage est envisageable.

NOTE : La méthode de contrôle par échantillonnage proposée consiste à :

- prélever un échantillon représentatif et aléatoire de systèmes d'information ;
- évaluer les mesures de sécurité des systèmes d'information sélectionnés et s'assurer qu'elles sont comprises, conformes aux attentes et correctement appliquées ;
- extrapoler les résultats à la totalité des systèmes d'information.

- **pour les systèmes moyennement critiques ou moyennement exposés (niveau de démarche intermédiaire) :**

  La première ligne de maîtrise doit déclarer que toutes les mesures de sécurité ont été appliquées et que tous les documents nécessaires à l'homologation du système d'information dans le cadre d'une démarche de niveau intermédiaire ont été fournis.

  Cette déclaration suffit à remettre un avis positif à l'autorité d'homologation.

  L'homologation de sécurité peut être prononcée.

  Durant la période de l'homologation, les informations fournies doivent être analysées dans le détail par le comité d'homologation.

  Si ceux-ci sont conformes aux attentes et aux enjeux de sécurité, l'homologation est maintenue.

  Dans le cas contraire, les écarts avec les exigences de sécurité doivent être présentés dans les plus brefs délais à une autorité d'homologation. L'homologation pourra dans ce cas être suspendue.

Pour ces systèmes d'information dont le niveau de démarche est simplifié ou intermédiaire, il est proposé de renforcer la confiance donnée aux équipes opérationnelles, de permettre une homologation plus rapide mais néanmoins de contrôler a posteriori les informations transmises.

- Si les contrôles sont concluants, l'homologation se poursuit et une reconduction de l'homologation dans les mêmes conditions est envisageable.
- Si les contrôles ne sont pas concluants, une commission d'homologation doit être réalisée dans les plus brefs délais. Elle permet de statuer sur les actions à mener pour permettre la continuité d'exploitation du système d'information.

Pour tous les autres systèmes (niveau de démarche renforcé)

L'avis de l'homologation de sécurité du système d'information ne peut être émis par le comité d'homologation qu'après l'évaluation des pièces justifiant de la prise en compte des risques de sécurité et des mesures mises en place.

La ré-homologation des systèmes d'information, quel que soit le niveau de démarche choisi, doit suivre le même procédé.

La prise de décision d'homologation de sécurité dépend du niveau de démarche sélectionné :

Prise de décision par niveau de démarche d'homologation	SIMPLIFIÉ	INTERMÉDIAIRE	RENFORCÉ
Dossier	**Auto déclaration de l'application des mesures de sécurisation**	**Auto déclaration de l'application des mesures de sécurisation et des informations nécessaires** (voir tableau « pièces du dossier à présenter »)	**Toutes les pièces du dossier** (voir tableau « pièces du dossier à présenter »)
Remise de l'avis d'homologation	**RSSI** (seconde ligne de maîtrise)	**RSSI** (seconde ligne de maîtrise)	**Comité d'homologation** (troisième ligne de maîtrise)
Commission d'homologation	**Peut être sous forme d'échange électronique**	**Peut être sous forme d'échange électronique**	**Commission en réunion** (présentielle ou à distance)
Revue	**Contrôle par échantillonnage**	**Contrôle des informations fournies durant la période d'homologation**	**Evaluation avant la commission d'homologation par le comité**

3.4. QUATRIÈME ÉTAPE : ORGANISER LA COMMISSION D'HOMOLOGATION

3.4.1 PRÉPARER LA COMMISSION D'HOMOLOGATION

La commission d'homologation est la réunion de présentation du système d'information à l'autorité d'homologation. Elle est nécessaire pour tous les systèmes d'information de démarche renforcée.

L'autorité peut être :

- L'autorité qualifiée de la sécurité du système d'information (AQSSI), directement responsable de la sécurité des systèmes d'information de l'organisation à laquelle elle appartient. Elle en a la responsabilité juridique et engage l'organisation au plus niveau ;
- Par délégation de pouvoir, l'AQSSI peut déléguer le pouvoir d'homologation à une autorité d'homologation (AH). L'AQSSI reste l'autorité juridiquement responsable ;
- Un dirigeant de l'organisation ou un responsable ayant reçu une délégation de signature du dirigeant. *Par exemple, le directeur des risques.*

> NOTE : Pour assurer une compréhension du contexte et une vraie prise en compte des risques, l'autorité d'homologation doit être au plus proche du métier du système d'information.

L'objectif de la commission d'homologation est de se prononcer sur la mise en service ou le maintien en service d'un système d'information.

La commission d'homologation doit être planifiée suffisamment à l'avance. L'organisateur doit s'assurer que l'autorité est disponible.

Afin de faciliter la fluidité du déroulement de la commission d'homologation, il est conseillé de réaliser une « pré-commission », sans l'autorité, afin de préparer le comité aux éventuelles questions qui pourraient être posées. Ce point permettra aussi d'aborder les désaccords résiduels et de préparer la présentation.

3.4.2 ANIMER LA COMMISSION D'HOMOLOGATION

> NOTE : Il n'est pas utile de rassembler tous les membres du comité d'homologation lors de la commission afin de ne pas surcharger la réunion. Néanmoins les membres clés[70] du comité doivent y participer.

La tenue de commission en présentiel est fortement recommandée pour favoriser les échanges.

Dans le cas d'une commission à distance, les équipements de réunion doivent être testés avant la réunion et les moyens de visioconférence doivent être au niveau d'habilitation requis.

Idéalement, la commission ne doit pas durer plus d'une heure en incluant la présentation et les éventuelles questions. Un « gardien du temps » est souvent préconisé afin de respecter les délais.

Les supports de commission doivent être synthétiques et présenter les points importants nécessaires à la prise de décision par l'autorité.

> NOTE : Les risques liés à l'emploi du système d'information doivent être ouvertement et clairement exposés à l'autorité. Ils ne doivent pas être sous-évalués ou cachés.

70. Par exemple DSI, RSSI, Responsable métier

La durée de l'homologation proposée dépend de la maturité de la sécurité du système d'information, des évolutions prévues et de son exposition aux sources de risques numériques.

En raison de l'évolution rapide des menaces, des changements éventuels des équipes informatiques, **L'ANSSI ne recommande pas de prononcer une homologation de plus de trois ans**.

Un système d'information pour lequel le plan d'action est conséquent ne peut pas être homologué sur une période trop longue.

Réduire la durée d'homologation revient à augmenter la surveillance d'un système d'information.

Il n'y a pas de renouvellement automatique d'une homologation.

A l'issue de la période d'homologation, pendant laquelle la sécurité du système d'information doit être améliorée, une nouvelle démarche doit être initiée.

Une homologation donnée ne peut être revue qu'à la fin de sa période ou en cas de changement notable du système d'information ou de son contexte. Dans ce cas, une nouvelle décision doit être formulée à la lecture des nouveaux documents d'homologation.

Il est à noter que l'homologation ne porte que sur l'emploi d'un système d'information en production réelle ou connecté à un autre système d'information en production.

Un système d'information en situation de test, en cours de conception, n'utilisant pas de véritables informations et déconnecté de tout système en production ne nécessite pas d'homologation.

Elle devient obligatoire avant son passage en condition réelle de fonctionnement.

NOTE : Si aucune réserve n'a été émise lors de sa prononciation, l'ANSSI recommande de ne pas revenir sur une décision d'homologation avant la fin de la période.

Dans le cas où une décision ne peut être prise, ou prise avec réserves, un plan d'action doit être établi et une nouvelle commission d'homologation doit être reprogrammée rapidement.

La décision doit être formalisée de façon écrite en utilisant les supports officiels de l'organisation et communiquée aux différentes personnes concernées.

NOTE : Informer l'utilisateur du système d'information de l'obtention de l'homologation renforce sa confiance. Cela peut se faire, *par exemple*, par l'affichage d'une mention au démarrage du système ou une communication dans un support utilisé par l'organisation.

L'ESSENTIEL :

La démarche d'homologation doit être menée par un comité animé par un responsable (généralement le RSSI ou CSN) et regroupant les personnes disponibles et engagées en lien avec le système d'information (responsables métiers, experts techniques...). Le comité doit permettre une vérification sur les risques identifiés liés à l'utilisation du système d'information et émettre un avis à l'attention de l'autorité.

Un niveau de la démarche d'homologation, parmi les trois proposés, doit être identifié. Il correspond à la criticité et à l'exposition aux sources de risque du système d'information.

Des informations proportionnelles au niveau de la démarche sélectionnée doivent être rassemblées pour composer le dossier d'homologation.

Une décision doit être prise par l'autorité d'homologation sur l'emploi du système d'information aux regards des risques identifiés. Cette décision peut être prise lors d'une commission ou via une communication électronique dans le cadre des démarches de niveaux simplifiés et intermédiaires.

La durée de l'homologation doit correspondre aux enjeux de sécurité du système d'information, au plan d'action engagé, au contexte de l'organisation et ne doit pas dépasser trois ans.

Pour accélérer et démultiplier les démarches, une déclaration de l'application des mesures de sécurité suffit à émettre un avis favorable d'homologation.

4

AMÉLIORER LA SÉCURITÉ DU SYSTÈME D'INFORMATION

La sécurité du système d'information ne doit pas s'arrêter une fois l'homologation obtenue. Elle doit être maintenue ou améliorée.

Cela se traduit notamment :

- par la réalisation des actions définies dans le plan d'action présenté lors de la commission et validé par l'autorité d'homologation ;
- par la réalisation des actions permettant de lever les éventuelles réserves émises lors de la commission ;
- par l'ajout d'actions suite à des changements impactant le périmètre ou l'écosystème du système d'information ;
- par le maintien en condition opérationnelle et de sécurité du système d'information ;
- par la correction de vulnérabilités identifiées ;
- par l'application de mesures liées à d'éventuels incidents de sécurité ;
- par la mise à jour de la documentation.

4.1 REVOIR RÉGULIÈREMENT LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

La sécurité de l'ensemble des systèmes d'information d'une organisation doit être revue au moins une fois par an, en dehors de toute commission d'homologation.

La revue doit être présidée par l'autorité d'homologation ou son délégué.

La durée et le contenu de la revue des systèmes d'information doivent être adaptés au nombre de systèmes d'information à étudier.

Durant cette revue, les points suivants doivent être présentés :

- l'état d'avancement des actions décidées lors de la précédente revue ;
- les indicateurs de performance ;
- les évènements marquants internes ou externes à l'organisation pouvant impacter la sécurité des systèmes d'information[71] ;
- les événements majeurs et incidents de sécurité survenus durant la période ;
- les actions d'amélioration de la sécurité proposées pour la période suivante.

Il est recommandé de présenter l'ensemble des systèmes d'information homologués ou non homologués. Pour ces derniers, il est important d'en comprendre la raison.

En fin de réunion, un rendez-vous doit être pris pour la revue annuelle suivante.

Il est à noter que tout évènement pouvant impacter la sécurité du système d'information et donc les risques liés à son emploi doit entraîner une adaptation du plan d'action et dans certains cas un passage devant une commission d'homologation.

NOTE : Durant la période d'homologation, l'autorité d'homologation peut être amenée à changer. Sauf demande spécifique, cela n'oblige pas à la tenue d'une nouvelle commission.

71. Par exemple, l'évolution de la menace sur l'organisation ou le système d'information, les changements structurants dans le maintien et l'amélioration du système d'information.

4.2 RENOUVELER UNE HOMOLOGATION DE SÉCURITÉ

Avant la date de fin d'homologation de sécurité d'un système d'information, prononcée par une autorité, l'avis de l'autorité doit être renouvelé.

Si elle a donné satisfaction, une démarche similaire à celle identifiée précédemment peut être réutilisée. Dans le cas contraire et pour les niveaux de démarches simplifié et intermédiaire, une commission présentielle peut s'avérer utile.

Un système d'information correctement suivi et dont la sécurité a été améliorée durant sa période d'homologation ne nécessite pas un gros effort de documentation.

Néanmoins un comité d'homologation doit être réuni pour rafraîchir les informations liées au système d'information.

Il peut être composé des mêmes personnes que pour l'homologation initiale.

Le comité doit se pencher sur les points suivants :

- « l'histoire » du système d'information depuis sa dernière homologation : les incidents, les changements notables, les améliorations apportées ;
- le suivi et l'avancée des actions présentées lors de la précédente commission ;
- l'évolution du contexte pour la prochaine période d'homologation.

L'avis et la durée proposés pour le renouvellement de l'homologation peuvent être différents des précédents. Ceux-ci dépendent du contexte et des enjeux de sécurité au jour de la commission.

> NOTE : Il n'est pas recommandé de renouveler l'homologation d'un système d'information si aucune action n'a été réalisée pour combler ses faiblesses de sécurité.

L'organisation d'une commission de ré-homologation est identique à celle d'une première homologation.

4.3 ARRÊTER UN SYSTÈME D'INFORMATION

Le système d'information est considéré comme arrêté lorsque toutes les données qu'il traite ont été détruites, déclassifiées, transférées à un autre système d'information ou conservées par un service spécialisé et que les éléments qui le composent ont été décommissionnés[72]. Des preuves doivent être apportées à ces actions.

Les processus comprenant des instructions claires doivent être établis avant le décommissionnement du système d'information. Ils doivent être accessibles et évalués par le comité d'homologation.

L'homologation prend fin lors du retrait du service et la suppression des risques associés.

L'ESSENTIEL :

Durant toute sa vie, la sécurité d'un système d'information doit être maintenue ou améliorée. Celle-ci doit être revue annuellement lors d'une réunion de suivi et durant la phase de ré-homologation.
L'homologation de sécurité se termine naturellement lors du décommissionnement du système d'information.

72. Les procédures de destruction des données et du système d'information doivent correspondre à leur niveau de classification.

L'ESSENTIEL :

Même si la démarche d'homologation de sécurité est une obligation réglementaire pour un certain nombre de systèmes d'information, elle est fortement recommandée pour les systèmes d'information les plus critiques.

L'homologation porte sur un système d'information dont le périmètre doit être clairement défini. Toutes les briques sur lesquelles il repose, son écosystème, et les risques qu'ils entraînent doivent être identifiés.

La nature des travaux permettant d'évaluer la sécurité du système d'information doit correspondre à sa criticité et à son exposition aux sources de risques numériques.

Il s'agit d'une décision prononcée par une autorité compétente au regard des risques liés à l'utilisation d'un système d'information, des actions déjà menées et de celles qui le seront pour réduire ou éliminer ces risques.

La décision s'appuie sur l'avis du comité d'homologation qui a la charge de collecter et évaluer les actions effectuées pour sécuriser le système d'information.

Un système d'information peut être homologué même s'il comporte des risques non traités mais acceptables par l'autorité.

La durée d'une homologation dépend des enjeux de sécurité, de la maturité du système d'information et des réglementations applicables.

Une revue de contrôle de la sécurité du système d'information doit être effectuée au minima une fois par an.

La démarche permettant d'obtenir une homologation est dans la continuité de la sécurisation d'un système d'information. Elle doit rester un processus simple, utile et adapté au système d'information et à ses enjeux de sécurité.

Le système d'information ne doit être employé qu'après avoir été homologué.

VOCABULAIRE

ANALYSE DE RISQUE

L'analyse de risque (AdR) est une démarche méthodologique visant à identifier, évaluer et traiter les risques. Elle doit mener à la création d'un plan de traitement des risques visant à réduire la vraisemblance de la survenance du risque.

COMITÉ D'HOMOLOGATION

Le comité d'homologation réunit les personnes aptes à vérifier la pertinence des mesures de sécurité appliquées à un système d'information pour que les risques auxquels il est exposé soient acceptables.

COMMISSION D'HOMOLOGATION

La commission d'homologation est l'acte durant lequel l'autorité d'homologation émet une décision d'homologation. Les échanges qui permettent cette décision peuvent être numériques (échanges par email) ou dans le cadre d'une réunion en présentiel réunissant les personnes impliquées par la décision.

DÉCISION D'HOMOLOGATION

Une décision d'homologation est prise par l'autorité d'homologation. Elle donne ou refuse l'autorisation d'employer un système d'information au regard des risques auxquels il est exposé. La décision d'homologation doit être renouvelée régulièrement.

DÉMARCHE D'HOMOLOGATION DE SÉCURITÉ

La démarche d'homologation est le processus qui suit le cycle de vie d'un système d'information. Elle est jalonnée par des phases d'homologation permettant une acceptation des risques par une autorité d'homologation.

EBIOS RM

EBIOS RM pour l'Expression des Besoins et Identification des Objectifs de Sécurité Risk Manager est la méthode d'évaluation des risques portée par l'ANSSI et le Club EBIOS. La méthode repose sur une approche en ateliers permettant de s'appuyer sur les socles de sécurité existants avant de s'intéresser aux scénarios d'attaque. Elle alterne les points de vue métier et technique et vise à être efficace plutôt qu'exhaustif.

REVUE DES SYSTÈMES D'INFORMATION

Point formel permettant d'identifier l'état de l'ensemble des systèmes d'information d'une organisation. La revue doit permettre à l'équipe de direction de prendre connaissance de l'état d'avancement des actions décidées lors des revues précédentes, des modifications pertinentes ayant un impact sur les risques et des opportunités d'amélioration.

SÉCURISATION D'UN SYSTÈME D'INFORMATION

Processus permettant de ralentir ou d'empêcher une attaque cyber sur un système d'information. La sécurisation se caractérise par l'application de mesures de gouvernance, de protection, de défense et de résilience.

SYSTÈME D'INFORMATION DE L'ETAT

D'après le Décret n° 2019-1088 du 25 octobre 2019 relatif au système d'information et de communication de l'Etat et à la direction interministérielle du numérique : Le système d'information et de communication de l'Etat est composé de l'ensemble des infrastructures et services logiciels informatiques permettant de collecter, traiter, transmettre et stocker sous forme numérique les données qui concourent aux missions des services de l'Etat et des organismes placés sous sa tutelle.

RÉFÉRENCES

LA MÉTHODE EBIOS RISK MANAGER

https://cyber.gouv.fr/la-methode-ebios-risk-manager

CARTOGRAPHIE DU SYSTÈME D'INFORMATION

https://cyber.gouv.fr/publications/cartographie-du-systeme-dinformation

GUIDE DE L'HYGIÈNE INFORMATIQUE

https://cyber.gouv.fr/publications/guide-dhygiene-informatique

MAÎTRISE DU RISQUE NUMÉRIQUE - L'ATOUT CONFIANCE

https://cyber.gouv.fr/publications/maitrise-du-risque-numerique-latout-confiance

ANTICIPER ET GÉRER UNE CRISE CYBER

https://cyber.gouv.fr/anticiper-et-gerer-une-crise-cyber

MON SERVICE SÉCURISÉ

https://monservicesecurise.cyber.gouv.fr

SI DU CENTRE DE VEILLE (CERT) DE L'ANSSI

https://www.cert.ssi.gouv.fr

EN SAVOIR PLUS

TÉLÉCHARGEZ TOUTE LA DOCUMENTATION POUR ASSURER VOTRE SÉCURITÉ NUMÉRIQUE SUR LE SITE DE L'ANSSI.

Plus d'informations sur le site de l'ANSSI : www.cyber.gouv.fr

Version 2.1 – Avril 2025
ISBN 978-2-11-167188-1 (imprimé) - ISBN 978-2-11-167189-8 (en ligne)
Dépot légal : mars 2025

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION
ANSSI — 51, boulevard de la Tour-Maubourg — 75 700 PARIS 07 SP
www.cyber.gouv.fr