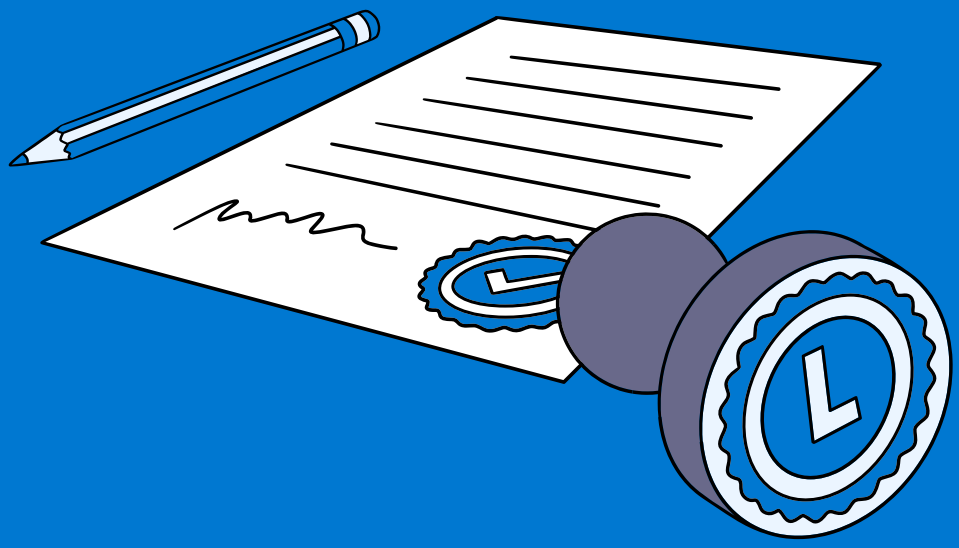
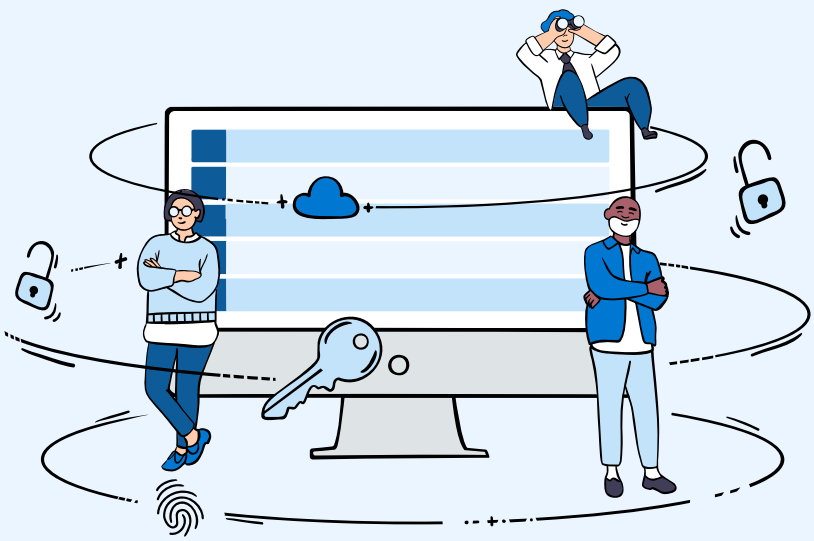
RÉPUBLIQUE
FRANÇAISE
Liberté
Égalité
Fraternité

L'homologation simplifiée

LES GRANDS PRINCIPES ET ÉTAPES DE L'HOMOLOGATION DE SÉCURITÉ





SOMMAIRE

Ce document propose un éclairage simplifié et pédagogique des grands principes et étapes de l'homologation de sécurité détaillés dans le « guide d'homologation de sécurité des systèmes d'information ».

POURQUOI HOMOLOGUER ?

Les systèmes d'information des entités publiques et des entreprises font face à un risque de cyberattaques pouvant entraîner des conséquences parfois graves sur le fonctionnement de ces organisations, sur le plan juridique, financier ou réputationnel ainsi que pour les usagers, les clients et les partenaires.

L'ensemble des systèmes d'information dans leur diversité est exposé à des risques d'origine cyber :

- Quelle que soit leur nature : ex. système d'information d'une organisation, infrastructure d'hébergement ; service numérique (site web, application, mobile, API, etc.).

- Quelle que soit leur criticité : ex. : site web d'information ; système d'information classifié ; traitement de données extrêmement sensibles.

Protéger ces systèmes contre ces risques est indispensable.

Pour cela, des mesures de sécurité doivent être mises en œuvre afin de répondre aux risques cyber les plus courants mais aussi aux risques parfois spécifiques auxquels sont exposés certains systèmes et contre lesquels chaque entité publique choisit de se protéger.

Afin de garantir que les risques cyber à l'encontre d'un système d'information soient connus, pris en compte et acceptés par chaque entité concernée, **la réglementation française prévoit l'obligation de prononcer une décision d'homologation de sécurité pour de nombreux systèmes.** Cette obligation concerne principalement les entités publiques mais également certaines entreprises privées réglementées.

L'homologation de sécurité est donc une démarche essentielle de gouvernance de la sécurité des systèmes d'information.

Même lorsque celle-ci n'est pas obligatoire, elle constitue une excellente pratique en matière de pilotage de la sécurité des systèmes d'information que toute organisation est encouragée à adapter.

Elle permet de :

1

S'engager dans une démarche de **réduction des risques** cyber à l'encontre des services, processus et données traitées.

2

S'approprier et **renforcer dans la durée la sécurité numérique** de ses systèmes d'information.

3

Renforcer la confiance des salariés, usagers, clients et partenaires dans les systèmes et services numériques mis à leur disposition.

Les principales sources réglementaires de l'homologation de sécurité incluent :

- **Le référentiel général de sécurité (RGS)** qui fixe des exigences en matière de sécurité des services publics en ligne en France et oblige leur homologation. Toutes les entités publiques sont concernées par cette obligation : Etat, établissements publics, collectivités.
- **Le décret n°2022-513 du 8 avril 2022** qui étend, pour l'Etat et les établissements publics, cette obligation à l'ensemble de leurs systèmes d'information et de communication.
- **D'autres réglementations soumettant systèmes d'information plus sensibles à une obligation d'homologation de sécurité (ex. IGI1300).**

QU'EST-CE QU'UNE HOMOLOGATION DE SÉCURITÉ ?

Une décision

L'homologation de sécurité prend la forme d'une décision. Celle-ci permet de s'assurer que les risques liés à l'emploi d'un sstème d'information sont clairement identifiés, traités et acceptés au plus haut niveau d'une organisation par une autorité (« l'autorité d'homologation »). Cette décision permet la mise et le maintien en service d'un système d'information.

La décision d'homologation **atteste que les mesures de sécurité mises en œuvre pour protéger un système, ainsi que les efforts additionnels planifiés, sont suffisants pour faire face aux risques cyber les plus courants et/ou les risques cyber spécifiques identifiés contre** lesquels une entité choisit de se protéger.

les risques cyber spécifiques identifiés contre lesquels une entité choisit de se protéger. **En cas d'avis défavorable de l'autorité d'homologation, l'homologation n'est pas validée** mais le refus d'homologation peut être enregistré formellement. En l'absence de décision, un système d'information est réputé ne pas pouvoir être mis ou maintenu en service.

Forme de la décision

La décision d'homologation est formalisée par un écrit sans exigence de forme particulière (ex. note administrative, document signé, etc.). Rien n'interdit qu'une décision d'homologation soit prise électroniquement.

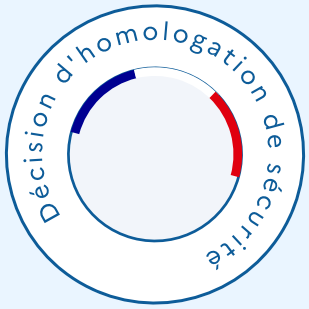
Une décision d'homologation indique à minima

- Le nom de l'entité
- Le nom/prénom et la fonction de l'autorité d'homologation
- Le nom ou l'identifiant du système et son périmètre
- La date de la décision et la durée de validité de l'homologation
- Les recommandations / exigences de l'autorité d'homologation pour la suite de la sécurisation du système et les réserves éventuelles.

[1] Selon le Cyberdico de l'ANSSI, un système d'information est un ensemble organisé de ressources (matériels, logiciels, personnels, données et procédures) permettant de traiter et de diffuser de l'information.

Publicité de la décision

La publication d'une décision d'homologation n'est pas obligatoire mais est fortement recommandée par l'ANSSI dans un souci de transparence et de renforcement de la confiance avec l'ensemble des personnes et parties prenantes utilisant le système d'information.



L'information publique sur une décision d'homologation devrait inclure a minima :

- Le nom de l'entité
- Le nom ou l'identifiant du système
- La date de la décision et la durée de validité de l'homologation

Portée juridique

La portée juridique d'une décision d'homologation varie d'une réglementation à une autre, selon par exemple, la sensibilité du système (ex. les systèmes classifiés relèvent du droit pénal).

Une décision d'homologation de sécurité engage juridiquement l'entité concernée représentée par l'autorité d'homologation.

Dans le cas où la personne ayant validé une décision d'homologation quitte l'entité, l'homologation ne perd pas sa validité et la responsabilité est transférée à une autre personne assurant le rôle d'autorité d'homologation.

QUAND HOMOLOGUER ET POUR QUELLE DURÉE ?

Quand commencer à se préoccuper de l'homologation d'un système ?

Il est recommandé de prendre en compte l'enjeu de la sécurisation d'un système d'information et de sa future homologation, dès la phase de réflexion de conception du projet.

L'homologation de sécurité d'un système doit être renouvelée régulièrement, jusqu'à son décommissionnement.

A quel moment prendre une décision d'homologation ?

La première décision d'homologation doit être prise avant la mise en service d'un système d'information (concernant l'homologation des projets agiles, voir « cas spécifiques »).

Le renouvellement d'une homologation intervient :

- **à échéance de la durée de validité de la décision d'homologation**
- **pendant la durée de validité d'une décision,** en cas d'évolution significative des caractéristiques du système :
  - Des caractéristiques du système (ex. nouvelles fonctionnalités)
  - De son environnement (ex. changement d'hébergeur)
  - Des risques et de l'exposition à ces derniers

Quelle est la durée de validité d'une décision d'homologation ?

La durée de validité d'une homologation est fixée librement par l'autorité d'homologation.

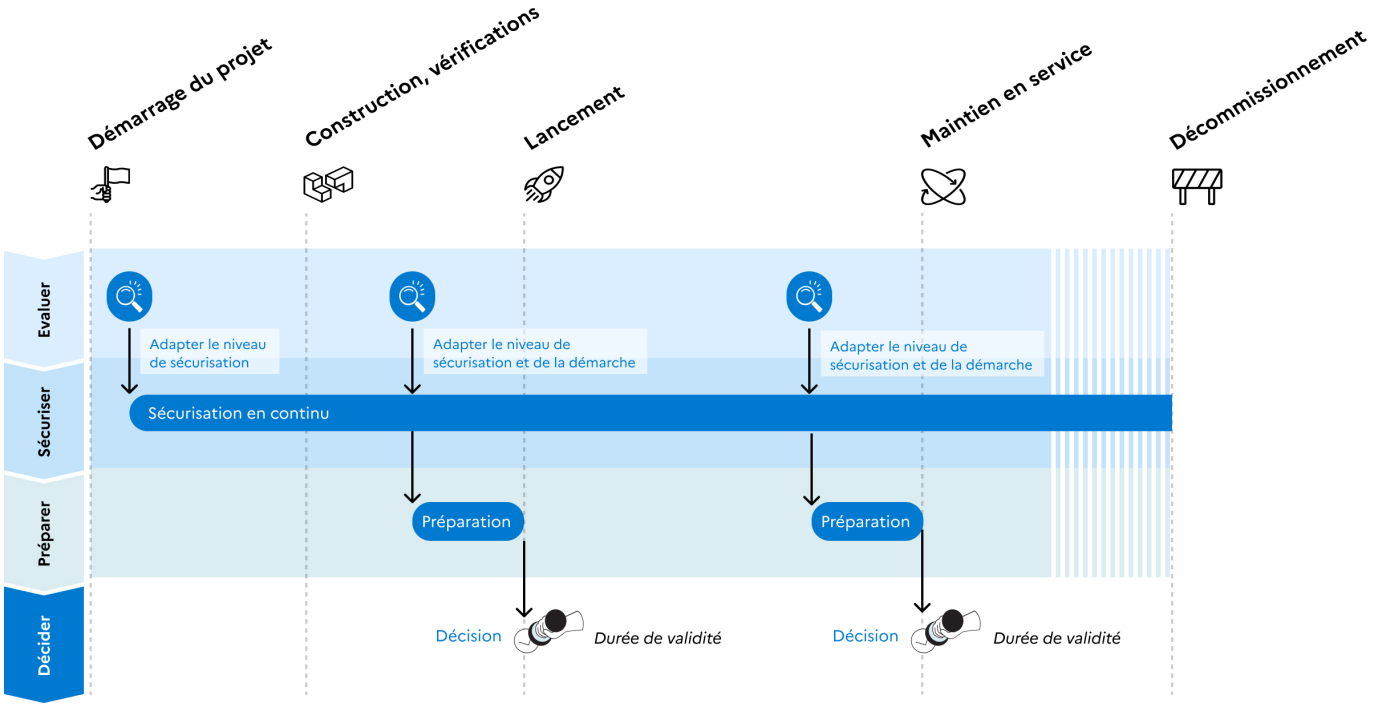
Elle ne doit toutefois pas excéder 3 ans. Il n'est pas non plus recommandé de fixer une durée de validité inférieure à 6 mois, au risque de consacrer plus de temps à la préparation de la prochaine décision qu'à implémenter le plan d'action de sécurisation du système concerné.

De manière générale, **la durée d'homologation tend à être corrélée au niveau de confiance de l'autorité dans la sécurité du système d'information.**

Plus cette confiance est élevée, plus la durée de validité de l'homologation aura tendance à être élevée.

Indépendamment de la durée d'homologation d'un système, **des points de rendez-vous intermédiaires doivent être organisés** afin de passer en revue les avancées du plan d'action de sécurisation du système. **Ces points de rendez-vous peuvent être mutualisés à l'occasion, par exemple, d'une revue annuelle de la sécurité et du statut d'homologation de l'ensemble des systèmes d'information d'une organisation.**

Le cycle de vie de l'homologation d'un projet



QUELS SONT LES ACTEURS DE L'HOMOLOGATION DE SÉCURITÉ ?

Les rôles concourant à la préparation de la décision d'homologation

On distingue généralement 3 rôles dans un projet de sécurisation et d'homologation d'un système d'information.

	ACTION	QUI
 **Opérationnel**	Opère et sécurise concrètement un système d'information.	Equipe produit, développeurs, architectes, chefs de projets intrapreneurs responsables techniques etc. Internes ou prestataires
 **Fonctionnel**	Conseille et supervise le niveau opérationnel sur les actions à mettre en oeuvre.	RSSI, délégué à la protection des données, prestataire de conseil cyber, etc.
 **Contrôle**	Contrôle le travail de sécurisation réalisé en amont de la commission d'homologation	Auditeur externe, conseiller à la sécurité numérique au sein d'un ministères, RSSI, etc.

Le succès de la démarche d'homologation dépend de la qualité et de la régularité des échanges entre les niveaux opérationnel, fonctionnel et de contrôle afin de faire progresser ensemble la sécurité du système.

Les rôles peuvent être assurés par des personnes distinctes ou par les mêmes personnes, adaptant leur positionnement selon le rôle joué.

Par exemple, **une même personne peut être appelée à jouer à la fois :**

- **Un rôle opérationnel**, en mettant en oeuvredes mesures concrètes de sécurisation d'un système.
- **Un rôle fonctionnel**, en conseillant une équipe sur les mesures de sécurité à mettre en œuvre.
- **Un rôle de contrôle**, en vérifiant que l'ensemble des étapes et actions devant être prises dans le cadre de l'homologation l'ont bien été.

Il est néanmoins recommandé, lorsque cela est possible d'attribuer le rôle de contrôle à une ou plusieurs personnes n'assurant pas les rôles opérationnel et fonctionnel, dans un souci d'impartialité.

Cela est, en particulier, recommandé s'agissant des démarches d'homologation de systèmes aux besoins de sécurité élevés (voir « identifier la démarche adaptée »).

Pour les démarches d'homologation des systèmes d'information aux besoins de sécurité élevés, un comité d'homologation doit être constitué en vue d'assurer le rôle de contrôle de la démarche menée, **avant la tenue de la commission d'homologation.**

Celui-ci doit être composée des personnes disposant d'une expertise métier et cyber, capables d'examiner les pièces fournies en vue de vérifier si la démarche a été menée de manière adéquate et si les mesures mises en œuvre sont satisfaisantes pour répondre aux risques identifiés.

L'autorité d'homologation

La décision d'homologation est prise par l'autorité d'homologation prenant la responsabilité, pour l'organisation, de la mise ou le maintien en service du système d'information.

L'autorité d'homologation est la personne placée au plus haut niveau hiérarchique d'une entité responsable d'un système d'information, en capacité d'assumer la responsabilité de la mise en ligne d'un service numérique au regard des risques identifiés et des mesures de sécurité mises en œuvre.

Le rôle d'autorité d'homologation peut être délégué de manière ponctuelle ou pérenne à une ou plusieurs autres personnes au sein d'une entité. Cette délégation peut être prononcée en vue de faciliter l'industrialisation des homologations, notamment pour les systèmes aux besoins de sécurité moins élevés. Pour cela, **la délégation doit être formalisée par écrit sans contrainte de forme (ex. mail, note).**

Dans le cas d'un système sous la responsabilité de plusieurs entités, le rôle d'autorité d'homologation doit revenir à l'entité ayant la responsabilité principale du système (ex. conception, déploiement, hébergement, financement, etc.).

Exemples d'autorité d'homologation ou de délégation :

Au sein d'une collectivité

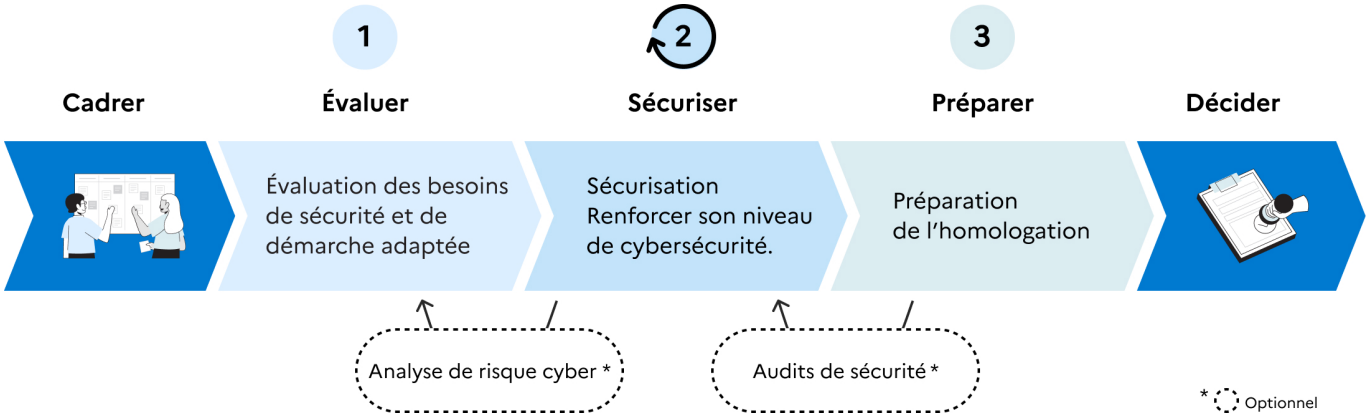
- Le ou la Maire pour une commune
- Le ou la DGS par délégation.

Au sein d'une administration ou d'une entité privée

- Le ou la DG d'une direction publique ou d'une agence publique
- Par délégation, un adjoint ou une adjointe, un chef de service ou une cheffe de service, un sous-directeur ou une sous-directrice voire pour les systèmes et services / besoins de sécurité aux besoins de sécurité les plus faible, un ou une chef(fe) de division.

LES GRANDES ÉTAPES VERS L'HOMOLOGATION

La décision d'homologation est la dernière étape d'une démarche en 3 grandes étapes.



Préalable à la sécurisation et l'homologation d'un système, une phase de **cadrage** est nécessaire afin de définir les objectifs du projet, son périmètre, les parties prenantes concernées.

Étape 1 - Évaluer

L'évaluation des besoins de sécurité d'un système consistant à évaluer sa criticité et son exposition aux sources de risques. Cette étape est indispensable en vue de proportionner l'effort de sécurisation et la profondeur de la démarche d'homologation.

Dans le cas où les besoins de sécurité identifiés seraient modérés (voir « Identifier la démarche adaptée », **la réalisation d'une analyse de risques rapide est recommandée** en vue d'affiner la compréhension des risques et identifier à l'étape suivante des mesures additionnelles susceptibles d'être mises en œuvre. **Pour les systèmes aux besoins de sécurité avancés ou élevés, la réalisation d'une analyse de risque approfondie est indispensable.** L'analyse de risque peut également conduire à réévaluer à la hausse les besoins de sécurité identifiés.

Étape 2 - Sécuriser

La sécurisation du système par la mise en œuvre, dès le début du projet de mesures de sécurité adaptées aux risques identifiés et contre lesquels l'entité souhaite se protéger. Plus l'effort de sécurisation sera mené dès le début du projet (« *by design* ») plus celui-ci sera performant et réduira les coûts ultérieurs. La réalisation d'une analyse de risque peut permettre de préciser les risques pour un système et de prioriser leur traitement. Dans le cadre du plan d'action de renforcement de la sécurité du système, il convient toujours de prioriser les actions ayant le plus d'impact et permettant de réduire les risques les plus critiques.

Dans le cadre d'une démarche d'homologation renforcée adaptée aux systèmes aux besoins de sécurité avancés et élevés (voir « identifier la démarche adaptée »), une **évaluation du niveau de sécurité** effectif (audits) du système doit être réalisée avant toute décision d'homologation **via la réalisation *a minima* de tests de sécurité automatiques ou d'audits plus approfondis, adaptés aux besoins de sécurité et aux caractéristiques d'un système** (ex. audit de configuration, d'architecture, de code, test d'intrusion, etc.). **La fréquence des audits ultérieurs doit répondre à la même logique.**

Étape 3 - Préparer

La démarche d'homologation en tant que telle, consistant à préparer l'ensemble des éléments permettant à l'autorité d'homologation de prendre sa décision, incluant à *minima* la définition du périmètre de l'homologation, la constitution d'un « dossier d'homologation », la collecte des avis – notamment du comité d'homologation – et la préparation de la commission d'homologation.

Décider

La décision d'homologation est prise par l'autorité d'homologation ou par délégation :

1. **Sur la base d'un dossier d'homologation** dont la profondeur varie en fonction du niveau de démarche et de l'avis du comité d'homologation.
2. **À l'issue d'un contrôle** de la matérialité des mesures mises en œuvre pour les démarches de niveau intermédiaire ou approfondi (voir « Identifier la démarche adaptée »).
3. **Lors d'une « commission d'homologation » pouvant prendre la forme :**

Lors d'une réunion réunissant les différentes parties prenantes, pouvant être consacrée à une seule décision ou mutualiser plusieurs décisions.

Dématérialisée, notamment dans le cadre d'une démarche initiale ou intermédiaire.

Dans le cadre d'une réunion, une ou plusieurs décisions d'homologation peuvent être prises simultanément.

IDENTIFIER LA DÉMARCHE ADAPTÉE

L'effort de sécurisation et la démarche d'homologation doivent être proportionnés aux besoins de sécurité d'un système d'information. Plus la criticité et l'exposition au risque d'un système sont élevés, plus l'effort de sécurisation sera important et la démarche d'homologation exigeante.

Évaluer les besoins de sécurité d'un système

Afin d'identifier l'effort de sécurisation nécessaire et la démarche d'homologation adaptée, les besoins de sécurité d'un système doivent être évalués en mettant en regard deux enjeux :

1. La criticité du système, établie sur la base d'une évaluation des impacts pour l'organisation d'une atteinte à la confidentialité, à l'intégrité ou à la disponibilité d'un système. Ces impacts peuvent être par exemple de nature juridique, financier, réputationnel. Ces impacts pouvant être identifiés dans le cadre de l'analyse de risques.

2. L'exposition aux sources de risques d'un système, incluant mais ne se limitant pas à son exposition depuis Internet.

Dans ce dernier cas de figure, 4 niveaux d'exposition sont identifiés :

a. Nul : aucune connexion réseau (« *stand alone* »), accès aux seules personnes habilitées.
b. Faible : ouverture à des réseaux maîtrisés, accessibles à des personnes habilitées
c. Important : indirectement ouvert à des réseaux non maîtrisés, accès nomades limités.
d. Total : ouverture complète sur internet.

La rencontre entre ces deux critères permet d'identifier **les besoins de sécurité du système,** à savoir les enjeux de sécurité de ce dernier et l'effort de sécurisation qui devra être mis en œuvre en conséquence.

	Exposition nulle	**Exposition faible**	**Exposition importante**	**Exposition totale**
Criticité maximale	Besoins de sécurité **avancés**	Besoins de sécurité **élevés**	Besoins de sécurité **élevés**	Besoins de sécurité **élevés**
Criticité importante	Besoins de sécurité **modérés**	Besoins de sécurité **modérés**	Besoins de sécurité **avancés**	Besoins de sécurité **avancés**
Criticité modérée	Besoins de sécurité **basiques**	Besoins de sécurité **basiques**	Besoins de sécurité **modérés**	Besoins de sécurité **modérés**
Criticité faible	Besoins de sécurité **basiques**	Besoins de sécurité **basiques**	Besoins de sécurité **basiques**	Besoins de sécurité **basiques**

Ainsi, dans le cas extrême ou la criticité d'un système serait maximale et son exposition absolument nulle, ses besoins de sécurité seraient considérés comme « seulement » avancés. Exemples de systèmes d'information selon les besoins de sécurité :

Besoins de sécurité basiques


Site vitrine d'une collectivité


Site de réservation de la médiathèque d'une commune


Système d'information bureautique d'une petite organisation

Besoins de sécurité modérés


Portail familles


Service de stockage des documents de travail en ligne


Système d'information bureautique d'une organisation de taille moyenne (Ex. PME <250 personnes)

Besoins de sécurité avancés


Service numérique d'envergure nationale traitant de données personnelles


Système de gestion d'opérations financières ou bancaires


Système ou service de gestion d'identité et de signature électronique

Besoins de sécurité élevés


Système d'information d'un grand groupe emportant des enjeux de sécurité spécifiques (R&D, processus industriel...)

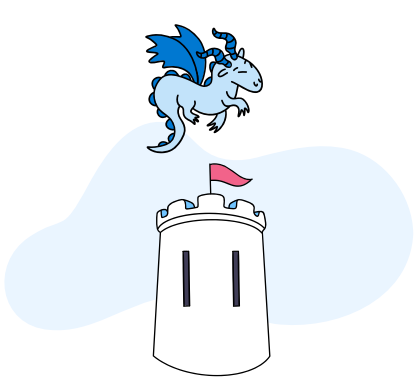

Système d'information traitant de données classifiées de défense


Système d'information sous-tendant des activités d'importance vitale

En déduire la démarche de sécurisation et d'homologation adaptée

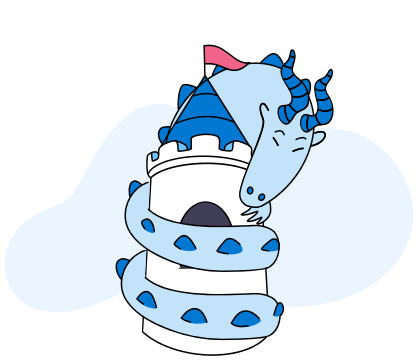
3 niveaux de démarches doivent être mis en œuvre en fonction des besoins de sécurité identifiés.

Démarche
Simplifiée



Besoins de sécurité **basiques**

Démarche
Intermédiaire

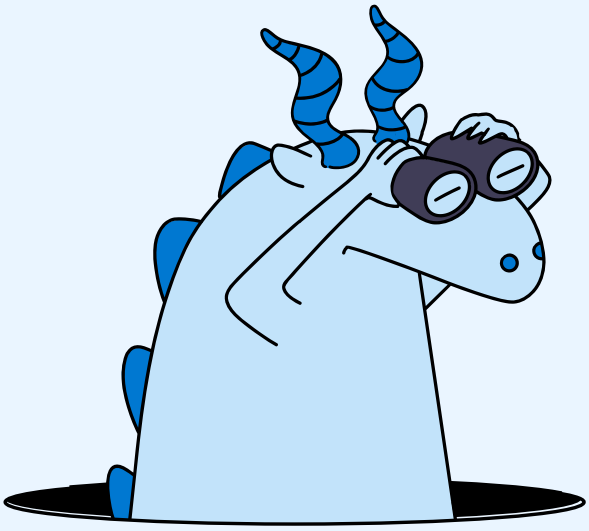


Besoins de sécurité **modérés**

Démarche
Renforcée

Besoins de sécurité **avancés** **élevés**

Quand bien même les besoins de sécurité d'un système auraient été identifié à un certain niveau (ex. élémentaire, modéré), **une organisation peut toujours librement choisir de mettre en œuvre une démarche de sécurisation et d'homologation plus exigeante.**



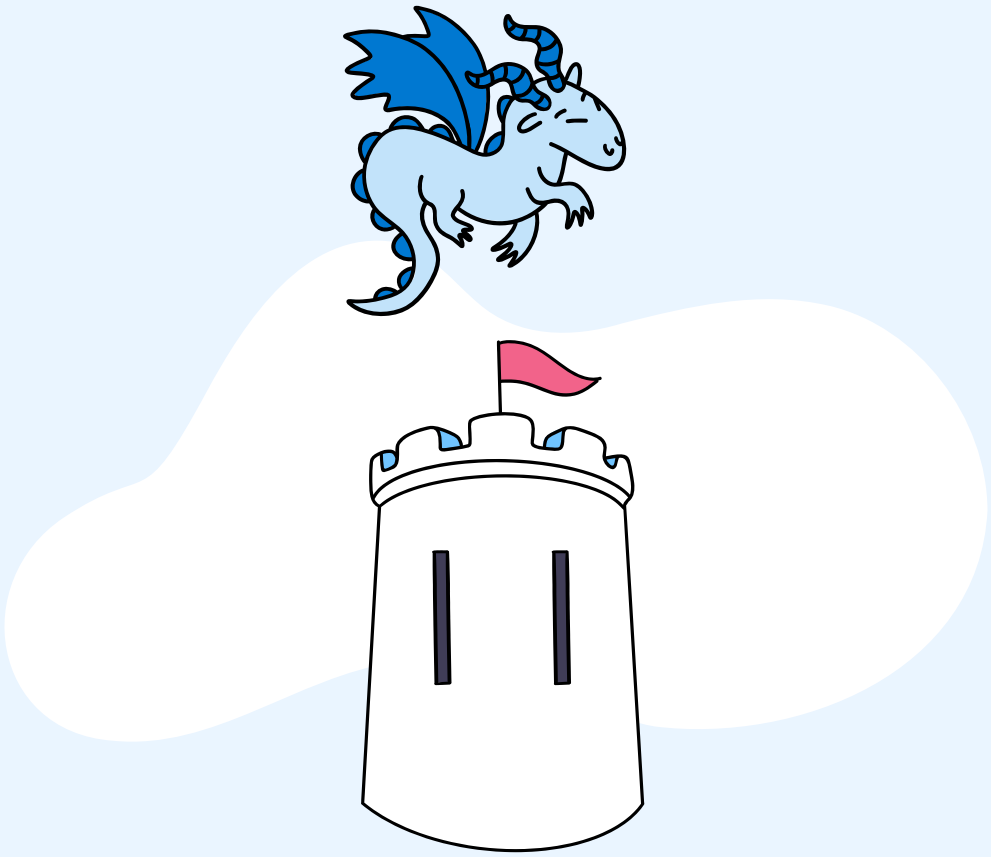
PROPORTIONNER CONCRÈTEMENT LA DÉMARCHE

Une fois le cadrage de la démarche et l'étape 1 d'évaluation des besoins de sécurité réalisés, plusieurs actions clés doivent être mises en œuvre à chaque niveau de démarche.

La liste proposée ci-dessous est indicative et ne vise pas à se substituer à des procédures déjà en vigueur qui auraient fait la preuve de leur efficacité **et de leur capacité à « industrialiser » l'homologation.**

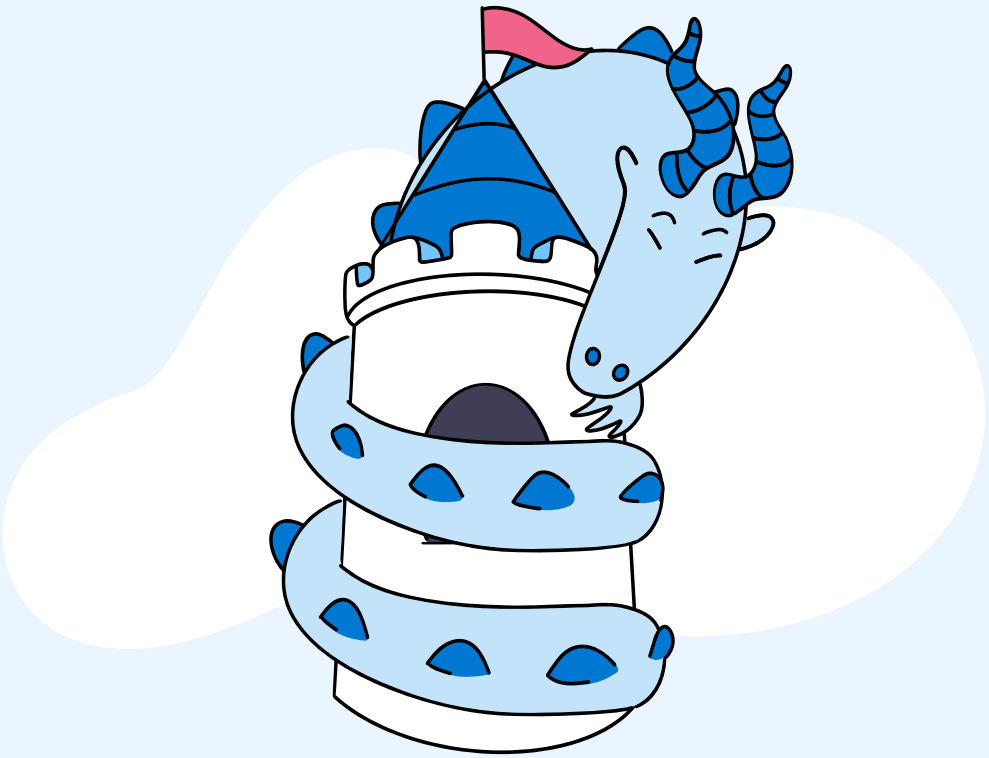
DÉMARCHE SIMPLIFIÉE		BESOINS DE SÉCURITÉ BASIQUES
1 ÉVALUATION DES BESOINS DE SÉCURITÉ	Réaliser une évaluation rapide des besoins de sécurité du système en fonction de sa criticité et de son exposition aux risques	☑
2 SÉCURISATION	Respect d'un socle de mesures de sécurité (hygiène informatique et mesures prévues dans la réglementation applicable).	☑
ÉVALUATION DE LA SÉCURITÉ (AUDIT)	/	
3 HOMOLOGATION	**Dossier d'homologation** succinct incluant l'historique du projet, la liste des mesures de sécurité mises en oeuvre et le plan d'action.	☑
	Contrôle : le dossier est considéré recevable sur la base des seules déclarations de l'équipe (auto-déclaration sur l'application des mesures de sécurité). Pas de vérification de la mise en oeuvre effective des mesures de sécurité listées dans le dossier.	☑
	Commission d'homologation : réunion non nécessaire, le processus exclusivement dématérialisé possible (ex. mail, parapheur, signature électronique).	☑
	Décision d'homologation par l'autorité ou par délégation	☑

☑ Action indispensable ☑ Action possible



DÉMARCHE INTERMÉDIAIRE		BESOINS DE SÉCURITÉ MODÉRÉS
1 ÉVALUATION DES BESOINS DE SÉCURITÉ	Réaliser une évaluation rapide des besoins de sécurité du système en fonction de sa criticité et de son exposition aux risques.	☑
ANALYSE DE RISQUE	Réalisation d'une analyse de risque rapide (complémentaire à l'évaluation des besoins de sécurité) pour préciser les risques à traiter et identifier des mesures de sécurité complémentaires à mettre en oeuvre.	☑
2 SÉCURISATION	Respect d'un socle de mesures de sécurité (hygiène informatique et mesures prévues dans la réglementation applicable).	☑
ÉVALUATION DE LA SÉCURITÉ (AUDIT)	Tests de sécurité automatiques	☑
	Tests d'intrusion, autres audit.	☑
3 HOMOLOGATION	**Dossier d'homologation** succinct incluant l'historique du projet, la liste des mesures de sécurité mises en oeuvre,le plan d'action (plan de traitement des risques) et de toutes les informations nécessaires.	☑
	Contrôle des informations fournies dans le cadre de la preparation de l''homologation	☑
	Commission d'homologation : réunion ou processus dématérialisé uniquement (ex. parapheur, signature électronique).	☑
	Décision d'homologation par l'autorité la plus élevée ou par délégation	☑

☑ Action indispensable ☑ Action possible



DÉMARCHE RENFORCÉE		BESOINS DE SÉCURITÉ AVANCÉS	BESOINS DE SÉCURITÉ ÉLEVÉS
1 EVALUATION DES BESOINS DE SÉCURITÉ	Analyse des risques cyber.	☑	
ANALYSE DE RISQUE	Réalisation d'une analyse de risque approfondie pour préciser les risques et identifier des mesures complémentaires à mettre en oeuvre.	☑	
2 SÉCURISATION	Respect d'un socle de mesures de sécurité (hygiène informatique et mesures prévues dans la réglementation applicable).	☑	
	Identification et mise en oeuvre de mesures additionnelles en matière de défense et de résilience.	☑	
EVALUATION DE LA SÉCURITÉ (AUDIT)	Tests de sécurité automatiques.	☑	
	Audit de sécurité complet au regard des besoins d'audit (ex. test d'intrusion audit de configuration, d'architecture, de code, physique...)	☑	
3 HOMOLOGATION	Formalisation (au plus tôt) d'un document d'accompagnement (présentation du système d'information dans son contexte et justification de la sélection de la démarche)	☑	
	Constitution d'un comité d'homologation	☑	☑
	Dossier d'homologation **complet** incluant des PJ détaillées (dossier d'architecture, plans MCO/MCS, plan de résilience, audits, etc.).	☑	
	Contrôle : revue de l'ensemble des mesures de sécurité listées dans le dossier.	☑	
	Commission d'homologation : réunion recommandée. La décision peut néanmoins toujours être adoptée de manière dématérialisée (ex. parapheur, signature électronique)	☑	
	Décision d'homologation par l'autorité la plus élevée ou par délégation.	☑	

☑ Action indispensable ☑ Action possible

PÉRIMÈTRE ET STRATÉGIES D'HOMOLOGATION POSSIBLES

Le périmètre d'homologation doit être défini

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 son responsable en a la maîtrise.

Le périmètre est défini librement

Le périmètre d'une homologation est défini au cas par cas par l'organisation. Néanmoins, pour des raisons de simplification, il peut sembler opportun de regrouper plusieurs systèmes d'information ayant une mission commune ou de les scinder.

Il n'existe donc pas *a priori* de « bonne manière » de définir le périmètre d'une homologation.

Plusieurs approches possibles

On peut, à titre d'exemple, évoquer plusieurs approches possibles en matière de définition d'un périmètre d'homologation.

- **L'homologation d'un système d'information dans ses différentes dimensions,** par exemple, l'homologation d'un service numérique tel qu'un site web ainsi que de l'infrastructure l'hébergeant et les services tiers participant à son fonctionnement (ex. service de mailing).
- **L'homologation d'un « socle » commun à plusieurs systèmes d'information d'une part puis séparément de chaque système d'information prenant appui sur le socle.** Par exemple, l'homologation de l'infrastructure d'hébergement, distinct des homologations des applicatifs prenant appui dessus. Cette approche permet d'accélérer les homologations de chaque brique prenant appui sur le socle.
- **L'homologation simultanée de plusieurs systèmes d'information distincts rassemblés dans une même « capacité » partageant la même finalité.** Par exemple, l'homologation d'un système complexe réunissant plusieurs systèmes et dont la mise en service doit être décidée simultanément.
- **L'adoption d'une décision homologation de « référence » consistant en l'homologation d'un système d'information pouvant être dupliqué en vue d'accélérer l'homologation d'autres systèmes d'information** partageant les mêmes caractéristiques et besoins de sécurité.
- **L'homologation d'un environnement technique et organisationnel « global » pouvant être modifié (ajout de nouvelles briques) sans nécessité d'homologation systématique à chaque ajout, sous réserve que :**
  - Les besoins de sécurité soient similaires.
  - La brique additionnelle se conforme aux mesures de sécurité communes à l'ensemble des applicatifs et services gérés dans l'environnement.
  - Cet ajout ne suscite pas de vulnérabilités nouvelles ou une plus grande exposition à des sources de risques.

Contraintes sur le périmètre de l'homologation

La profondeur de l'homologation dépend du niveau de maîtrise du système concerné. Dans le cas des systèmes d'information hébergés, le périmètre de l'homologation est condition au niveau de responsabilité du contractant.

Responsabilité	SaaS	PaaS	LaaS	*On premise*
Données	X	X	X	X
Ordinateurs (PC et mobile)	X	X	X	X
Annuaires d'identité		X	X	X
Application (dont MCO)		X	X	X
Système (OS, MCS)			X	X
Virtualisation (machine, réseau)			X	X
Machines physiques (+hyperviseur)				X
Réseau physique				X
Local informatique				X

Dans le cas extrême des systèmes hébergés en SaaS, l'entité adoptant la décision d'homologation doit concentrer son effort à deux niveaux :

- **Avant la sélection du fournisseur de service,** en évaluant ou en fixant les garanties de sécurité offertes (pouvant prendre la forme d'un « plan d'assurance sécurité ») et en se penchant sur plusieurs offres afin d'identifier le choix le plus sûr.
- **Une fois le fournisseur sélectionné en concentrant l'effort d'homologation sur les dimensions du projet sur lesquels l'entité contractante dispose d'une marge de manœuvre sur laquelle doit se concentrer l'effort de sécurisation et l'homologation :** ex. : identification des données à protéger, configuration du système en vue d'en renforcer la sécurité ; sécurisation de l'environnement informatique d'utilisateur du système, etc.

CAS SPÉCIFIQUES

Le cas de l'homologation des services publics mutualisés

Un système d'information ou un service numérique proposé par une entité publique à d'autres entités publiques ne doit être homologué qu'une seule fois par l'entité proposant, en premier, lieu le service. Il est, ce faisant, recommandé à l'entité homologuant le service :

- D'impliquer un panel d'entités utilisatrices du service, lors de la commission d'homologation.
- De baser l'homologation sur un cadre d'emploi prédéfini.

Les entités publiques utilisatrices du service peuvent alors bénéficier de l'homologation mutualisée, dès lors que le service est utilisé conformément au cadre d'emploi défini. Dans l'hypothèse où ces entités utiliseraient le service en-dehors de ce cadre d'emploi, une décision d'homologation spécifique devrait être adoptée.

Le cas de l'homologation des systèmes développés de manière agile

Les deux principales différences entre des systèmes conçus de manière agile – souvent des services numériques – et les systèmes d'information développés selon une approche planificatrice résident :

- Au démarrage, dans le fait qu'un système agile est le plus souvent mis en production dans **une version préliminaire (*« minimum viable product »*)** auprès d'un périmètre d'utilisateurs restreint en vue de vérifier son potentiel d'impact et l'adhésion des utilisateurs. Lors de cette phase, les risques sont souvent significativement amoindris par la très faible exposition du système.
- Tout au long de la vie du système, compte tenu du fait **qu'un système développé de manière agile évolue en continue** – parfois de manière quotidienne – et avec lui les besoins de sécurité, pouvant nécessiter une fréquence de ré-homologation plus élevée que pour un système classique tout en étant vigilant à ce que toute nouvelle « mise en production » ne soit pas conditionnée à une décision d'homologation, au risque de stopper la dynamique itérative.

En s'inscrivant dans une logique de sécurisation en continu, il convient de veiller à :

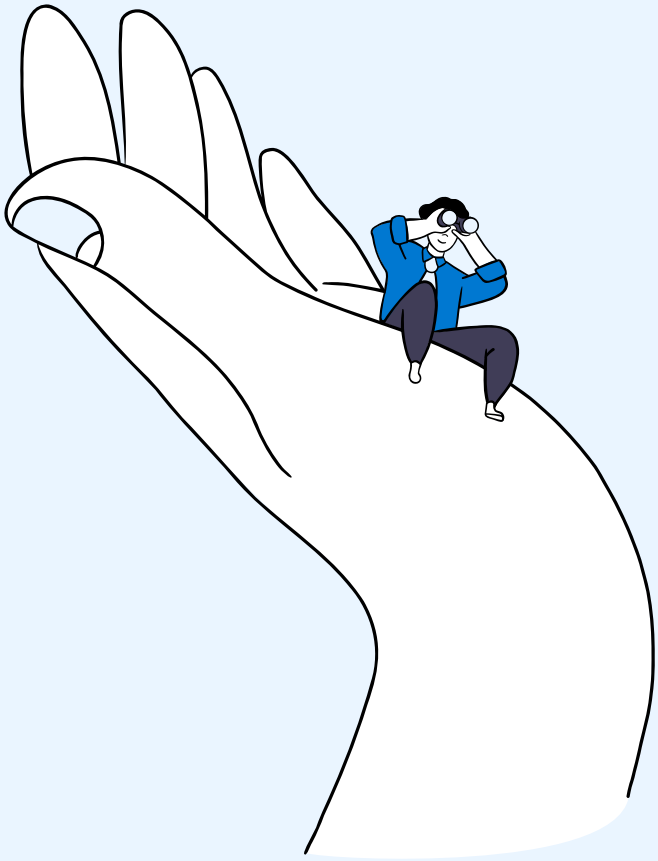
1. **Intégrer la sécurité dès la première ligne de code.**
2. **Évaluer et réévaluer régulièrement les besoins de sécurité en continu et proportionner l'effort de sécurisation** en fonction de ces derniers en vue d'identifier le besoin d'une ré-homologation.

À titre d'exemple, un service numérique d'envergure nationale qui serait tout d'abord déployé auprès d'un petit nombre d'utilisateurs, l'effort de sécurisation devrait être proportionné au risque actuel (faible) et non au risque cible (potentiellement très important). À mesure que le service accélèrera, sa sécurité devra être renforcée et de nouvelles homologations envisagées.

S'il est aussi obligatoire, comme pour tout système d'information, d'être homologué avant la première mise en production du service numérique, **la décision d'homologation peut être prise – dans le cadre des projets agiles, sur la base d'une démarche accélérée** ayant permis d'identifier les besoins de sécurité du système et de s'assurer que l'équipe a minima identifié les mesures de sécurité indispensables à mettre en œuvre.

En phase de test (Beta), il peut, par ailleurs, être envisagé de planifier l'adoption de la décision d'homologation dans un délai raisonnable après la mise en service du produit afin de permettre à l'équipe de se concentrer sur ce dernier plutôt que sur son homologation alors que le projet pourrait être rapidement décommissionné, tout en étant attentive, dès le départ, au respect d'un socle de mesure de sécurité adaptées.

LES FACTEURS CLÉS DE SUCCÈS



Les erreurs à ne pas commettre

Plusieurs idées peuvent nuire au succès de la démarche de sécurisation et d'homologation et son passage à l'échelle au sein d'une organisation :

1. **Considérer que seuls les spécialistes cyber peuvent s'approprier les enjeux de sécurité** et en sont responsables. « D'un côté les spécialistes de l'autre les métiers ».
2. **Considérer la sécurité comme une « étape » souvent postérieure à la construction d'un système ou d'un service.** « Avant on construit ou on achète, ensuite on sécurise ».
3. **Percevoir l'homologation comme un point final** au-delà duquel la sécurité n'aurait plus besoin d'être suivie et renforcée. « Avant on homologue, ensuite on passe à autre chose ».

3 grands principes à respecter

Sécuriser dès que possible

Prendre en compte la sécurité au plus tôt dans les projets et s'inscrire dans une logique de renforcement en continu de la sécurité est essentielle et facilite la prise de décision d'homologation. La sécurité peut être prise en compte :

- Dès les phases d'idéation sur le projet de système ou de service numérique.
- Au moment de la mise en concurrence de prestataires d'équipements et/ou de services, au travers d'exigences de sécurité dans le cahier des charges.
- Tout au long du développement d'un système d'information

L'intégration de la sécurité au plus tôt dans le design du produit permet des gains d'efficacité importants sur l'ensemble de la durée de vie du produit.

Collaborer dès que possible

Impliquer au plus tôt l'ensemble des personnes susceptibles de contribuer au renforcement de la sécurité d'un système ou d'un service est un facteur de succès de la démarche de sécurisation et facilite l'homologation :

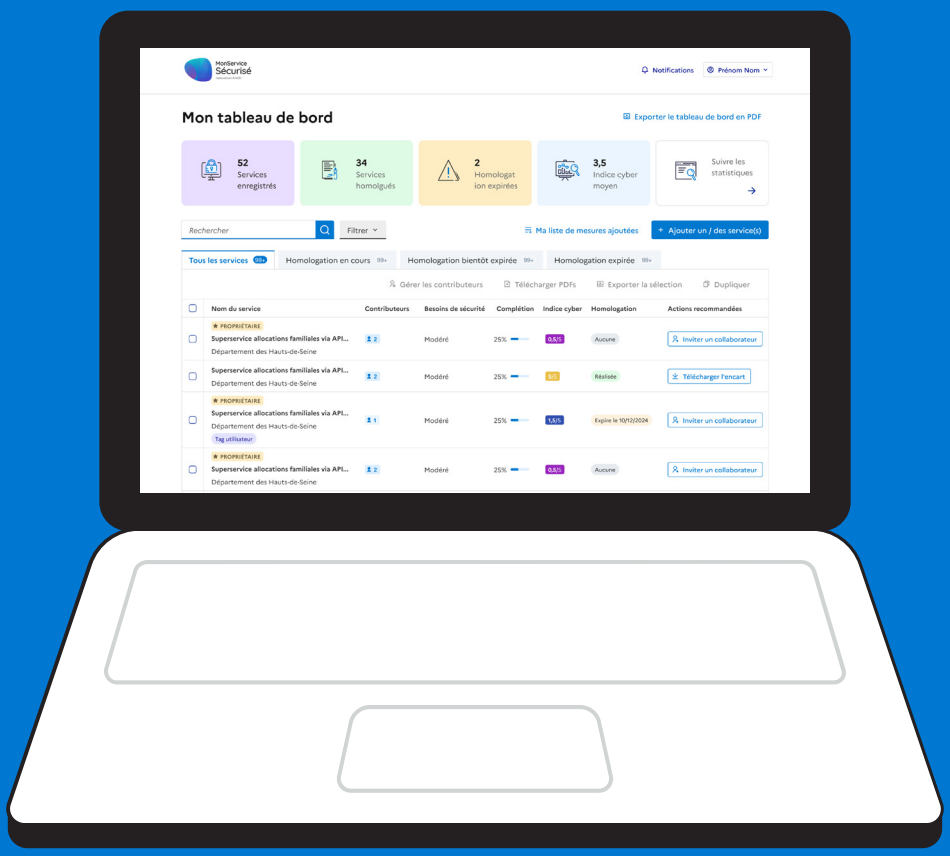
- Responsables métiers
- Responsables informatiques
- Responsables de la sécurité des systèmes d'information
- Délégués à la protection des données
- Equipes projets (admin, design, dev, bizdev, etc.).

Proportionner l'effort à chaque étape

Les systèmes d'information et les services numériques sont divers de par leur nature, les risques auxquels ils sont soumis et in fine leurs besoins de sécurité. L'effort nécessaire, à chaque étape de l'homologation, doit être proportionné aux besoins de sécurité du système en termes :

- D'effort humain à mobiliser dans la constitution du dossier permettant une décision d'homologation (ex. nombre de réunions préparatoires).
- De niveau de profondeur des actions à mener.
- De temps alloué à la commission d'homologation.

NOS SOLUTIONS POUR VOUS AIDER



Découvrez MonServiceSécurisé

Entités publiques, pilotez en équipe **la sécurité de tous vos services numériques** et **homologuez-les** rapidement avec **MonServiceSécurisé.**
Un service adapté aux services aux **trois niveaux de démarches d'homologation** pour des systèmes aux besoins de sécurité basiques, modérés et avancés.

Découvrez le guide de l'homologation de sécurité des systèmes d'information

Le guide complet de l'homologation de sécurité. Découvrez également le guide de la méthode d'analyse de risque EBIOS Risk Manager.