

GUIDE DE L'HOMOLOGATION DE SECURITE DES SYSTEMES D'INFORMATION

FICHE METHODE

IDENTIFIER

L'AUTORITE D'HOMOLOGATION

Les fiches méthodes permettent aux responsables de la démarche d'homologation ou au comité d'homologation d'identifier les points essentiels d'attention en fonction de la typologie du système d'information ou des concepts utilisés.

Elles n'ont pas vocation à remplacer les guides techniques de l'ANSSI ou les politiques de sécurité et les réglementations en vigueur qui doivent être appliquées.

QU'EST-CE QU'UNE AUTORITE D'HOMOLOGATION ?

L'autorité d'homologation est un individu de l'organisation dont le niveau hiérarchique est suffisamment élevé pour assumer les responsabilités de l'homologation et assumer des choix stratégiques et financiers.

- Dans le secteur privé, il s'agit généralement d'un membre de la direction générale appelé dans certains cas l'autorité qualifiée de la sécurité du système d'information (AQSSI) ;
- Dans le secteur public, il s'agit de l'AQSSI.

LA DELEGATION D'AUTORITE

Le Directeur Général ou l'AQSSI peut décider de déléguer son autorité via une délégation de signature¹ et donc son pouvoir d'homologation à un représentant de l'autorité d'homologation (AH) qu'elle désigne. Il peut s'agir de l'autorité d'emploi.

L'autorité désignée est chargée de s'engager sur l'acceptabilité de la sécurité pour le Directeur Général ou l'AQSSI. Toutefois, l'autorité première reste juridiquement responsable, notamment en cas de survenance d'un incident.

¹ La délégation de pouvoir est un acte juridique permettant à un dirigeant de transférer une partie de ses responsabilités à un tiers, souvent pour mieux gérer les obligations au sein d'une entreprise.

IDENTIFIER L'AUTORITE D'HOMOLOGATION

Dans les organisations avec une gouvernance complexe matricielle où l'autorité est difficile à identifier, les points suivants permettent d'identifier une autorité compétente :

- Quelle direction métier utilise le système d'information ?
- Qui finance le système d'information ?
- Qui dispose des leviers décisionnels au sein de l'organisation ?
- Qui est la personne morale, juridiquement responsable au nom de l'organisation ?

QUE FAIRE SI PLUSIEURS AUTORITES SONT PRESENTES ?

Pour éviter de diluer les responsabilités, il n'est pas recommandé d'identifier plusieurs autorités pour un système d'information.

Par exemple :

- *le financement du projet est partagé entre des organismes relevant de plusieurs autorités qualifiées différentes ;*
- *une homologation capacitaire² est nécessaire ;*
- *l'équipe support (DSI) est :*
 - *rattachée à une entité commune (ex : co-entreprise ou joint-venture, multinationale, GIE, organisation internationale) ;*
 - *indépendante mais financée par plusieurs entités auxquelles elle rend compte.*

Idéalement le choix d'une seule autorité d'homologation pour le système d'information se fait par concertation ou par décision de direction.

Une responsabilité partagée entre plusieurs AH est un cas de figure rare qu'il convient de ne déployer qu'en dernier recours car elle peut entraîner une dilution des responsabilités.

² ensemble de plusieurs systèmes d'information à homologuer (voir guide de l'homologation)

LES RESSOURCES DISPONIBLES POUR ALLER PLUS LOIN

L'homologation de sécurité	https://cyber.gouv.fr/publications/lhomologation-de-securite-des-systemes-dinformation
Maîtrise du risque numérique – l'atout confiance	https://cyber.gouv.fr/publications/maitrise-du-risque-numerique-latout-confiance
La méthode EBIOS Risk Manager	https://cyber.gouv.fr/la-methode-ebios-risk-manager
Le guide d'hygiène informatique	https://cyber.gouv.fr/publications/guide-dhygiene-informatique