RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

COLLECTION
GESTION DES RISQUES CYBER

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

FICHE METHODE

L'HOMOLOGATION POUR LES DECIDEURS

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.

L'HOMOLOGATION : DE QUOI S'AGIT-IL ?

L'homologation est l'étape qui autorise ou non la mise en route ou le maintien d'un système d'information au sein d'une organisation. C'est une décision qui doit être prise par un responsable hiérarchique de l'organisation (l'autorité d'homologation) et qui peut impliquer une responsabilité légale de la personne qui la prend.

L'homologation est rendue obligatoire par un grand nombre de textes réglementaires[1].

QUELS BENEFICES ?

Au-delà de certaines obligations réglementaires, homologuer permet à un dirigeant de connaître le niveau de cybersécurité des systèmes d'information qui contribuent au fonctionnement de leur organisation et les impacts sur leur fonctionnement en cas d'une attaque réussie, initiée par une source malveillante.

L'homologation doit être appréciée comme un outil de prise de conscience pour les dirigeants des risques qui pèsent sur leur organisation et qui dépassent largement les aspects techniques. Cette démarche permet également aux dirigeants de piloter l'équilibre des investissements en cybersécurité au regard des enjeux des systèmes concernés.

[1] voir le guide de l'homologation de sécurité des systèmes d'information, chapitre « identifier les réglementations applicables »

QUAND DOIT ON HOMOLOGUER ?

Une homologation n'est pas permanente et doit être reconduite au maximum tous les trois ans (tous les deux ans pour les systèmes d'information avec un classification de niveau secret ou plus).

Un système d'information doit être homologué avant sa mise en exploitation, à chaque fin de période d'homologation et à chaque changement notable ayant un impact sur les risques qui pèsent sur l'utilisation du système d'information.

L'homologation peut être réalisée même dans le cas d'une mise en exploitation rapide d'un système d'information.

COMMENT HOMOLOGUER ?

Une homologation est décidée par l'autorité lors d'échanges électroniques ou au cours d'une réunion (la commission d'homologation) pour les systèmes d'information les plus critiques ou les plus exposés aux risques numériques

Durant cette réunion qui ne doit pas excéder une heure, l'autorité d'homologation doit avoir les éléments pour comprendre :

- le contexte et les enjeux dans lequel évolue le système d'information ;
- le taux de conformité par rapport aux textes réglementaires auxquels il s'applique ;
- les actions qui ont été menées pour prendre en compte les risques qui pèsent sur le système d'information et celles qui seront prises pendant son exploitation ;
- les risques résiduels qui demeurent une fois ces actions prises.

Le comité d'homologation qui instruit le dossier doit présenter une proposition d'avis et de durée d'homologation.

Celle-ci peut être suivie ou discutée.

NOTE :

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

ET APRES ?

Une revue annuelle de suivi des systèmes d'information doit être menée par les équipes opérationnelles et un compte rendu adapté doit être remis à l'autorité d'homologation. Cette revue permet de s'assurer du maintien ou de l'amélioration de la sécurité des systèmes d'information.

A chaque fin de période d'homologation, d'un grand changement d'un incident de sécurité, une ré-homologation doit être initiée. Le contexte, les nouvelles menaces, « l'histoire » du système d'information et de tout élément pouvant influer sur les risques doivent être étudiés.

L'homologation s'arrête lorsque le système d'information est démantelé. Le dirigeant doit en être notifié.

LES RESSOURCES DISPONIBLES POUR ALLER PLUS LOIN

L'homologation de sécurité	https://cyber.gouv.fr/lhomologation-de-securite
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
Mon Service Sécurisé	https://monservicesecurise.cyber.gouv.fr