RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

COLLECTION
GESTION DES RISQUES CYBER

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

FICHE METHODE

L'HOMOLOGATION DE SECURITE ET LA NORME ISO/IEC 27001

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'ISO/IEC 27001, DE QUOI S'AGIT-IL ?

La norme internationale certifiante ISO/IEC 27001 définit les exigences à mettre en œuvre et à maintenir pour un système de management de la sécurité de l'information (SMSI). Elle vise à protéger les informations et les processus les plus sensibles d'une organisation contre les menaces numériques. La version de 2022 de la norme couvre les domaines organisationnels, physiques et technologiques du périmètre à certifier.

En s'appuyant sur son annexe A, elle permet à son utilisateur de vérifier que les bonnes mesures de sécurité de l'information sont appliquées.

La certification est prononcée par un organisme accrédité.

L'HOMOLOGATION DE SECURITE, DE QUOI S'AGIT-IL ?

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 (voir la fiche méthode sur l'autorité d'homologation de sécurité).

Une décision d'homologation est un acte formel, pouvant être 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.

QUELS RAPPROCHEMENTS ENTRE LES DEMARCHES D'HOMOLOGATION ET LA NORME 27001 ?

Les deux concepts visent à mettre en œuvre une amélioration continue de la sécurité et nécessitent une revue régulière des périmètres étudiés.

Le tableau suivant énumère les correspondances entre la norme de l'ISO/IEC 27001 et la doctrine d'homologation.

	ISO/IEC 27001	Homologation
Dernière version	ISO27001 version 2022	Homologation version 2.1 (2025)
Organisme porteur	ISO (AFNOR en France)	ANSSI
Domaine d'application	Organisation	Système d'information
Objectif	Mettre en place un cadre afin de protéger l'information : le SMSI	Identifier, traiter et accepter les risques cyber résiduels sur un système d'information
Périmètre	Information	Système d'information
Type	Méthode et norme certifiante	Doctrine et exigence réglementaire
Obligation	Facultatif	Obligatoire (réglementaire) et conseillée (pour les autres)
Décision	Organisme accrédité	Autorité d'homologation (interne ou externe)
Durée	3 ans	Maximum 3 ans
Revue	Revue annuelle de direction Audit de suivi	Revue annuelle des systèmes d'information conseillée
Décision	Audit de certification	Commission d'homologation
Analyse de risque recommandée	ISO27005:2022	EBIOS RM
Fil directeur	Annexe A	Réglementations Politiques de sécurité Analyse de risques
Mesures de sécurité à appliquer	Déclaration d'applicabilité	Mesures réglementaires et nécessaires identifiées lors de l'analyse de risque, audits…
Portée	Internationale	Française
Impact en cas de défaillance	Perte de la certification	Nécessité d'arrêt du système d'information

LES RESSOURCES DISPONIBLES POUR ALLER PLUS LOIN

L'homologation de sécurité	https://cyber.gouv.fr/publications/lhomologation-de-securite-des-systemes-dinformation
ISO/IEC 27001	https://www.iso.org/fr/standard/27001
ISO/IEC 27002	https://www.iso.org/fr/standard/75652.html
ISO/IEC 27005	https://www.iso.org/fr/standard/80585.html
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