RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

COLLECTION
GESTION DES RISQUES CYBER

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

FICHE METHODE

ORGANISER UNE REVUE DES SYSTEMES D'INFORMATION

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 REVUE DES SYSTEMES D'INFORMATION ?

Il s'agit d'un 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.

NOTE :
La revue des systèmes d'information est semblable à une revue de direction dans le cadre d'une certification ISO/IEC 27001.

QUI DOIT ASSISTER A LA REVUE DES SYSTEMES D'INFORMATION ?

Des représentants de la première et seconde ligne de maîtrise[1] doivent assister à la revue des systèmes d'information. Il est conseillé que les autorités d'homologation assistent à la revue. Elle doit être animée par le responsable de la sécurité des systèmes d'information.

[1] voir guide de l'homologation (mettre en place une gouvernance de sécurité)

A QUELLE FREQUENCE DOIT AVOIR LIEU LA REVUE DES SYSTEMES D'INFORMATION ?

Une revue des systèmes d'information doit être planifiée au moins une fois par an.

COMMENT DOIT SE DEROULER LA REVUE DES SYSTEMES D'INFORMATION ?

La revue des systèmes d'information doit être composée de deux parties et à minima permettre de couvrir les points suivants :

Partie 1 : revue globale

1. Information sur le contexte et les risques globaux qui pèsent sur les SI de l'organisation.
   Le niveau des risques identifiés (KRI), le contexte économique et stratégique, les changements organisationnels doivent être abordés durant ce point.

2. Revue des indicateurs[2] globaux de sécurité :
   Les indicateurs doivent être globaux et conformes à la stratégie de l'organisation. *Par exemple, nombre d'évènements de sécurité sur le site, nombre de personnel en charge de la cyber sécurité…*

3. Revue des changements depuis la dernière revue et suivi du plan d'action :
   Le plan d'action validé lors de la précédente revue doit être analysé. Les écarts par rapport au plan doivent être présentés.

[2] Chaque indicateur doit être mesuré par rapport à une cible décidée par l'organisation. *Par exemple, la cible est de ne pas avoir plus de dix évènements de sécurité par an*. Tout dépassement doit être justifié et donner lieu à une ou plusieurs actions.

Partie 2 : revue détaillée

4. Revue des systèmes d'information :

   L'ensemble[3] des systèmes d'information doit être revu.

   La date d'homologation ou de fin d'homologation de chaque système d'information doit être identifiée. Les systèmes d'information dont la date d'homologation est proche doivent être clairement identifiés et un planning de réalisation présenté.

   Même si le système est homologué, un indicateur doit permettre d'identifier les systèmes d'information pour lesquels une action spécifique de sécurité ou d'homologation est à mener. Ces actions devront être exposées lors de la revue.

La revue des systèmes d'information doit se terminer par l'établissement et la validation d'un plan d'action permettant aux équipes en charge des systèmes d'information et de leur sécurité de se réaligner par rapport aux objectifs de sécurité.

La date de la prochaine revue doit être définie en fin de réunion.

[3] 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.

EXEMPLE DE REVUE DE SUPPORT POUR UNE REVUE DES SYSTEMES D'INFORMATION

Les tableaux ci-dessous sont fournis à titre d'exemple et ne correspondent à aucune donnée réelle.

Les échelles et niveaux de risque sont donnés à titre indicatif pour illustrer l'exemple.

Partie 1 : revue globale

1. Point d'information général sur le contexte

Niveau de risque	Période précédente	Période actuelle	Commentaires
Changements organisationnels	Faible	↘ Moyen	Délocalisation de l'équipe de maintenance informatique.
Changements physiques	Moyen	↗ Faible	Le gardiennage a été renforcé le mois dernier.
Changements technologiques	Faible	↘ Moyen	L'outil permettant la virtualisation a été racheté par une société étrangère et les coûts de maintenance ont fortement augmentés
…			

Par exemple, les points qui peuvent être abordés :

- Quels sont les changements organisationnels, physiques, technologiques qui ont eu lieu depuis la dernière revue ?
- Quelle est l'évolution de la menace[4] sur l'entité et sur le secteur ?
- Quels sont les évènements majeurs impactant la sécurité globale de l'année passée ?

[4] Voir panorama de la menace de l'ANSSI

2. Indicateurs globaux

Indicateurs	Période précédente	Période actuelle	Cible
Nombre d'évènements de sécurité	7	5	10
Revue mensuelle des comptes utilisateurs par rapport aux informations RH	12	4	10
Personnel en charge de la SSI	4	4	4
…			

La présence d'indicateurs anormaux (rouge) doit être justifiée.

3. Non avancement des plans d'actions

Quelles sont les actions qui pèsent sur l'ensemble des SI par rapport à l'année précédente ?

Nom de l'action	Détail	Propriétaire	…	Statut n-1	Statut n	Commentaire
Sensibilisation	Sensibiliser lors de e-learning 100% des employés et prestataires	RSSI		En cours (60%)	En cours (80%)	Plainte concernant la longueur du e-learning. Beaucoup d'employés ne terminent pas la sensibilisation.
Revue physique	Mise en place de revue de sécurité physique mensuelle du site	Services Généraux		En cours (75%)	Terminé	Les revues sont effectuées tous les premiers lundis du mois
Embauche d'un RSSI adjoint	Besoin de renfort de l'équipe cyber	RH / RSSI		Prévu fin d'année	En retard	Manque de candidat correspondant à la demande
…						

… et revue des changements durant la période

Changement	Impact	Propriétaire
Doublement de la liaison internet	Augmentation de la performance et de la résilience du site par rapport aux connexions internet	DSI
Changement de la méthode d'accès à la salle machine	Les clés ont été remplacées par un système à badge permettant de tracer les entrées et sorties en salle	Services Généraux
…		

Partie 2 : revue détaillée

4. Revue des systèmes d'information

Nom du SI	…	Statut d'homologation	Date de fin d'homologation	Statut du plan d'action	Informations complémentaires
SI Alpha		Homologué	Mars 2027	Suivi	RAS
SI Bravo		Homologué	Septembre 2025	Suivi	Chantier de ré-homologation a débuté – Date de commission à définir
SI Charlie		Non homologué	/	La démarche est en cours	Grosse pression du métier pour démarrer au plus vite
SI Echo		Non homologué	/	Aucun plan connu	Attention le SI est employé, mais pas homologué. Action à mener.
…					

LES RESSOURCES DISPONIBLES POUR ALLER PLUS LOIN

L'homologation de sécurité	https://cyber.gouv.fr/publications/lhomologation-de-securite-des-systemes-dinformation
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
Panorama de la menace	https://cyber.gouv.fr/le-panorama-de-la-cybermenace