Homologuer son SI : comprendre et mettre en œuvre la démarche ANSSI

Date et durée

Code formation : GIT002FR
Durée : 2 jours
Nombre d'heures : 14 heures

Description

Face à la multiplication des cybermenaces et au durcissement réglementaire, l'homologation de sécurité de votre **système d'information (SI)** est incontournable. Cette formation vous permettra de comprendre et de mettre en œuvre une **démarche d'homologation robuste**, conforme aux recommandations strictes de l'ANSSI, pour garantir la maîtrise des risques de votre organisation.
À travers une approche pragmatique alternant théorie et études de cas réels, vous apprendrez à naviguer dans le **cadre réglementaire** complexe. Vous découvrirez comment articuler les responsabilités entre **les différents acteurs (DSI, RSSI, Métiers)** et comment structurer efficacement votre dossier pour qu'il soit à la fois réaliste et juridiquement solide.
À l'issue de ces 2 jours, vous repartirez avec toutes les clés pour constituer un **dossier d'homologation complet** , exploiter les résultats d'une **analyse de risques** (type EBIOS) et préparer une décision formelle qui engage la responsabilité de l'autorité qualifiée en toute sérénité.

Objectifs

À l'issue de cette formation, vous atteindrez les objectifs de compétences suivants :

- comprendre le cadre réglementaire et les enjeux de l'homologation de sécurité ;
- identifier les rôles et les responsabilités des différents acteurs (Autorité, RSSI et DSI) ;
- structurer et constituer un dossier d'homologation conforme aux attentes de l'ANSSI ;
- exploiter les résultats d'une analyse de risques pour définir un plan de traitement adapté ;
- préparer et formaliser la décision d'homologation pour assurer le maintien en conditions de sécurité.

Points forts

- **Conformité ANSSI** : un programme strictement aligné sur les guides et recommandations de l'Agence nationale de la sécurité des systèmes d'information.
- **Expertise terrain** : une animation assurée par des consultants experts en homologation et certifiés ISO 27001.
- **Approche pragmatique** : une alternance d'apports théoriques et d'études de cas inspirées de situations réelles pour une mise en application immédiate.
- **Sécurité juridique** : vous apprendrez à construire une démarche « juridiquement robuste » pour garantir la traçabilité et protéger la responsabilité des décideurs.

Modalités d'évaluation

Travaux Pratiques

Etude de cas

Pré-requis

Suivre cette formation nécessite les prérequis suivants :

- **Connaissances :** une connaissance générale des systèmes d'information et des enjeux de sécurité est recommandée.
- **Expérience :** une première participation à une analyse de risques (méthode EBIOS ou équivalent) est un atout, mais n'est pas obligatoire.

Public

Cette formation s'adresse aux acteurs clés de la sécurité des SI. Le public inclut notamment :

- les **RSSI et responsables informatiques** qui sont chargés de piloter la conformité et la sécurité du SI ;
- les **chefs de projet et auditeurs internes** qui doivent intégrer les exigences d'homologation dans leurs projets ou contrôles ;
- les **décideurs (secteur public/parapublic)** appelés à endosser le rôle d'autorité d'homologation et à signer les décisions.

Programme

Module 1 : appréhender le cadre et les principes de l'homologation

- La définition et les objectifs de l'homologation (maîtrise du risque et traçabilité).
- Le contexte réglementaire, normatif et les différences avec la certification ou l'audit.
- L'approche par les risques et le principe d'acceptation du risque résiduel.
- La présentation des guides et recommandations officiels de l'ANSSI.

Module 2 : identifier les acteurs et structurer la gouvernance

- L'identification des acteurs clés : Autorité d'homologation, Comité, RSSI, DSI et Métiers.
- La définition des responsabilités juridiques et organisationnelles de chaque partie.
- L'articulation entre l'homologation, la gouvernance SI et le management des risques.
- Le cas particulier des systèmes d'information externalisés ou mutualisés.

Module 3 : constituer le dossier d'homologation

- La structure type et le contenu d'un dossier conforme aux standards ANSSI.
- La description du système, la politique de sécurité et la déclaration d'applicabilité.
- L'intégration de l'analyse de risques (EBIOS RM) et du plan de traitement.
- La mise à jour et le maintien en conditions opérationnelles du dossier.

Module 4 : formaliser la décision d'homologation et assurer le suivi

- Le processus de prise de décision et sa formalisation (l'acte d'homologation).
- La gestion de la durée de validité et les conditions de renouvellement.
- Le suivi des plans d'action, des risques et des évolutions du système d'information.
- Les bonnes pratiques pour une homologation pragmatique et durable.

ANSSI (Agence nationale de la sécurité des systèmes d'information) est l'autorité nationale en matière de sécurité et de défense des systèmes d'information (cyber.gouv.fr).
EBIOS® est une marque déposée par le Secrétariat général de la défense et de la sécurité nationale.
ISO/IEC 27001 est une norme internationale de sécurité de l'information publiée par l'ISO (www.iso.org).