CyberOne

CYBER SECURITY

THALES
Building a future we can all trust

L'Homologation de Sécurité

Pourquoi et comment homologuer vos systèmes d'information ?

Jeudi 29/01/2026

www.thalesgroup.com

THALES
Building a future we can all trust

MÜLLER Christophe

Responsable la Sécurité des Systèmes d'Information

Réseaux d'affaires SYSTEMES TERRESTRES ET AERIENS

christophe.muller@thalesgroup.com

SOMMAIRE

1 - Pourquoi parler d'homologation ?

> Comprendre pourquoi homologuer

> Découvrir qui est concerné, ce que l'on veut protéger, et comment faire

Les Systèmes d'information (SI), ce que l'on veut protéger

> les systèmes d'information (SI), ce ne sont pas que des ordinateurs ….

- **c'est tout ce qui permet à votre organisation de fonctionner avec des données**
  - **Des matériels** (serveurs, ordinateurs, smartphones),
  - **Des logiciels** (applications, sites web, bases de données),
  - **Des données** (fichiers clients, emails, documents sensibles),
  - **Des personnes** (utilisateurs, administrateurs)

> Selon les organisations, différentes valeurs sont à protéger contre différents risques

Type d'organisation	Exemple de SI à homologuer	Risque si non sécurisé
Collectivité	Site de déclaration d'impôts locaux	Fuite de données fiscales des citoyens
Hôpital	Dossier médical électronique	Piratage des données patients
Entreprise	Plateforme de paiement en ligne	Fraude + perte de confiance des clients
École	Portail de notes des élèves	Modification malveillante des résultats

Parler d'homologation dans un contexte de guerre cyber

> Contexte lié aux Cyber attaques

- En 2023, UNE organisation sur TROIS en France a subi une cyberattaque (Source ANSSI)
- En 2024, c'est +25% par rapport à 2023
- Les cyberattaques peuvent paralyser toute une organisation pour déstabiliser, saper, voler, rançonner, espionner ….
  - Risques de perte de **disponibilité** (D), **d'intégrité** (I), de **confidentialité** (C) des données
  - Impacts à différents niveaux : **financiers, humains, d'image, juridiques, opérationnels**

> Revue Nationale Stratégique (RNS) orientée conflit majeur

- Propositions faites au Gouvernement (site – Secrétariat Général de la Défense et de la Sécurité Nationale)
- Se concentrer sur le prioritaire pour lutter contre une menace tangible inscrite et permanente
- Postulat d'un scénario de conflit majeur au cœur de l'Europe en 2030
- Objectif de résilience cyber de 1er rang en France et en Europe
- Risque de « tempête parfaite »
  - Avec des acteurs prépositionnés
  - Cibler ce qui est le plus critique
  - Objectif de saturer et baisser la confiance des citoyens dans les institutions

Les incidents/crises majeurs identifiées

> International année 2025

- **Groupe Jaquar Land Rover**
- **Collins Aerospace**
- **Providers de services Cyber mondiaux**
- **Oracle Business Suite**
- **Salesforce**
- **…. Et des tentatives contre Thales et ses fournisseurs // la France**

> Et aussi

- **Barrage Norvège** 2024 (perte confiance population)
- **Réseau électrique en Pologne** 2026 (shutdown)
- **APT28**
- **Storm1516** (guerre informationnelle)
- …

> France en décembre 2025

- **La Poste** : Paralysie d'infrastructure critique via attaque DDoS
- **Mondial Relay & Colis Privé** : Exfiltration de 25 millions d'enregistrements de données personnelles
- **Ministère de l'Intérieur** : Accès non autorisé aux fichiers, affectant potentiellement 16,4 millions d'individus
- **Ministère des Sports, Jeunesse et Vie Associative** : Compromission affectant 3,5 millions de foyers
- **CNRS** : Exfiltration de données techniques / espionnage scientifique
- **Ville de Lens** : Intrusion informatique compromettant les services municipaux
- **Duick — Brasserie Jenlain** : Compromission d'infrastructure critique du secteur agroalimentaire
- **Ministère de l'Agriculture et de l'Alimentation** : Exfiltration de 61 Go de données
- **THT Bio Science** : Laboratoire pharmaceutique compromis, données techniques exfiltrées

Parler d'homologation pour se défendre : un peu de GRC

> L'Homologation de Sécurité, c'est votre assurance contre ces risques & impacts

- Elle est de plus en plus souvent obligatoire
- Les principales sources réglementaires de l'homologation de sécurité incluent :
  - **Le référentiel général de sécurité** (RGS) pour l'Etat, les **établissements publics, les collectivités**
    - Ainsi que le **décret n°2022-513 du 8 avril 2022** qui étend l'obligation à l'ensemble de leurs SI et systèmes de communication
  - **l'Instruction Interministérielle 901** (II 901) pour les SI traitant **d'informations restreintes** publiques ou privées
  - **l'Instruction Générale Interministérielle 1300** (IGI 1300) pour les SI traitant **d'informations classifiées** liées au secret de la défense nationale
    - **l'Instruction Générale Interministérielle 2102** (IGI 2102) pour l'Union Européenne
    - **l'Instruction Interministérielle 2100** (II 2100) pour l'OTAN
  - **La loi de Programmation Militaire** (LPM) pour les **SI d'Importance Vitale** (SIIV) au sein d'Opérateur d'Importance Vitale (OIV)
  - **La directive européenne NIS2** : pour augmenter la sécurité des réseaux et des systèmes d'Information des infrastructures critiques et le renforcement de la cybersécurité des **Entités Essentielles** et des **Entités Importantes**

> Défense des organisations informatiques simples et complexes

- Protéger la chaine de valeur des **clients** et des **fournisseurs**
- Approche par **Gouvernance, Risques et Conformité** (GRC)

Qu'est-ce qu'une homologation ?

> Une homologation de sécurité est un acte formel qui engage l'autorité qui la prononce

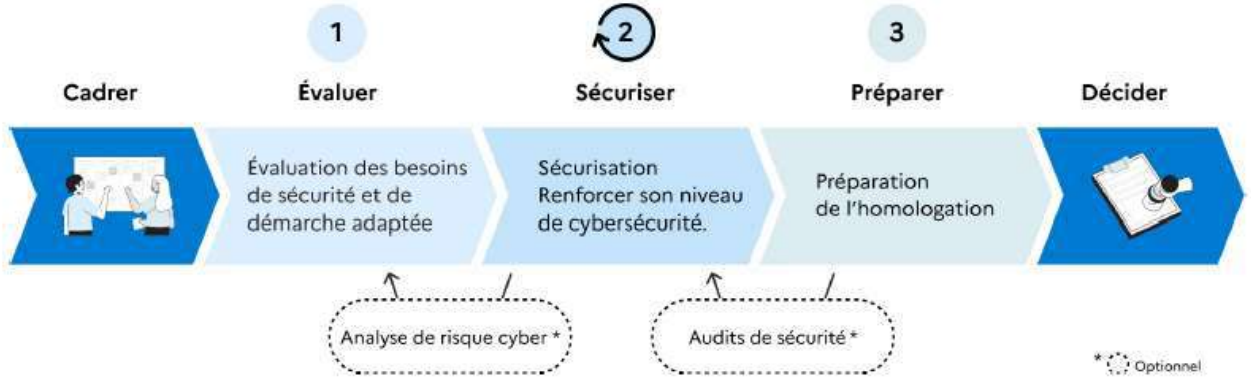
- Décision officielle attestant la bonne appropriation des risques cyber (identifiés, maîtrisés et acceptés)
- Elle est obligatoire pour les organismes publics et entreprises liées aux services vitaux et essentiels pour la France

> C'est comme un « contrôle technique d'une voiture » pour votre organisation autour du SI

- elle vérifie que les protections sont en place avant qu'il ne soit trop tard
- renforce son niveau de sécurité et permet de renforcer la confiance de ses usagers, clients et partenaires quand à son utilisation.

> Elle s'organise comme un projet

- Un début, une fin, des acteurs, un objectif …



Les rôles clés de l'homologation

> L'homologation est une équipe : chacun a un rôle pour garantir la sécurité

- Tout le monde est concerné, que vous soyez maire, directeur d'hôpital, ou responsable IT

Rôle	Qui ?	Mission
Opérationnel	Équipes techniques (développeurs, architectes)	Mettre en œuvre les mesures de sécurité.
Fonctionnel	RSSI, DPO, consultants cyber	Conseiller et superviser les actions.
Contrôle	Auditeurs, comité d'homologation	Vérifier que tout est conforme avant décision.

- Exemple pour le site web d'une mairie

Acteur	Rôle dans l'homologation	Exemple
Direction générale	Prend la **décision finale** d'homologuer.	Le maire signe l'homologation du site web.
Responsable métier	Définit les **besoins** (ex. : quelles données protéger ?).	Le DRH identifie les données RH sensibles.
RSSI / DPO	Conseille sur les **risques et mesures de sécurité**.	Le RSSI propose des chiffrement des données.
Équipes techniques	Met en œuvre les **protections** (ex. : pare-feu).	Les développeurs corrigent les failles.
Auditeurs	Vérifie que tout est **conforme** avant décision.	Un prestataire teste la résistance aux attaques.

Déclinaison et enjeux chez Thales depuis les années 2010

> Recensement de tous les Systèmes d'Information

- Les SI des différentes **DSI** du Groupe : le cœur de l'informatique centralisée
- Plus de **5500 SI** sous responsabilité « **métier** » décentralisés : R&D, Dev, Usine (Fab, Manuf..), IVVQ (Intégration, Validation, Qualification..), Démonstration, Services aux client (formations, jumeaux physiques ou numériques, maintenance …), Management IS/IT, Surveillance, Médical ….
- Identifier les éléments de SI et les liens technologiques avec les fournisseurs, partenaires et clients

> Identification de la Gouvernance = référencement de plusieurs milliers d'acteurs

- les **« propriétaires responsables »** de ces SI (« IS owners ») en charge d'atteindre le bon niveau de sécurité des SI
- Les **« acteurs techniques »** (technical contacts) : architectes techniques, administrateurs, techniciens
- Les **« contacts sécurité »** (security managers) : personnel cyber mis à contribution pour assurer la conduite des homologations
- La **« chaine Sécurité des SI »** : responsables et officiers de sécurité des SI qui conseillent, préconisent et contrôlent
- Les **« Autorités d'Homologation » internes et externes** : qui valident l'acceptation des risques résiduels et le plan de traitement

> Des politiques de sécurité et des processus d'homologation des SI

- Déployer et faire adopter les principes et processus IS/IT à toutes les parties prenantes
- Utiliser différents niveaux de validation selon différents critères (sensibilité, exposition, soumis à la règlementation ….)
- Impliquer tous les acteurs

2 - Les 5 étapes vers l'homologation

> Un processus structuré en 5 phases, adapté à la complexité de votre système

Les 3 niveaux de criticité

> Tous les systèmes ne nécessitent pas le même niveau de sécurité.

> L'ANSSI propose 3 niveaux pour adapter l'effort /// 3 niveaux également pour l'IGI1300

Niveau	Pour quel système ?	Exemple	Démarche
Simplifié	Système peu critique.	Site vitrine d'une PME.	Checklist basique + bonnes pratiques.
Standard	Système important (données sensibles).	Portail patients d'un hôpital.	Analyse de risques + audits légers.
Renforcé	Système **critique** (vie humaine, État).	Système de gestion des urgences.	Analyse approfondie + tests intrusifs.

> Comment choisir ?

- Aider la décision avec un questionnaire d'évaluation pondéré
  - **A quel niveau le SI est-il exposé sur des réseaux** : isolé ? intranet ? Internet ?
  - **Quel est le niveau de complexité du SI** : 1 seul équipement ? Inférieur à 10-20 équipements ? Plus de 10-20 équipements ?
  - **Quel est le niveau de diversité technique** : Moins de 5 technos utilisées ? De 5 à 10 technos ? Plus de 10 technos
  - **Quel est l'impact financier si le service s'arrête** : Moins de xx Keurs ? Entre xx et yy Keurs ? Plus de yy Keurs
  - **Quelles sont les typologies de données manipulées** : Personnelles ? Santé ? Diffusion restreinte ? Special France ? Classifiées ?
  - **Quel est le niveau de maturité cyber des personnes en charge** : faible ? Moyen ? Élevé ?
  - ….

Étape 1 : Cadrer

> Objectif

- Définir quoi sécuriser et pourquoi

> Questions à se poser

- "Quel est le périmètre ?" (ex. : seulement le site web, ou aussi les serveurs ?)
- "Quels sont les enjeux ?" (ex. : données personnelles, service critique comme les urgences)

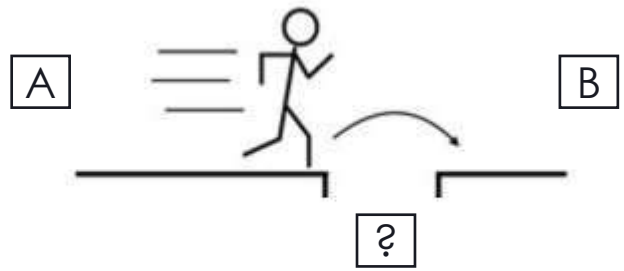
> Exemple : Une école cadre l'homologation de son portail élèves

- **Périmètre** : site web + base de données des notes
- **Enjeu** : éviter la modification frauduleuse des résultats

> Exemples de valeurs apportées par cette étape

- Référencer les SI et identifier les personnes en charge
  - Eviter le « shadow » et « hidden » IT
- Inventorier les SI et maitriser son parc informatique
  - Eviter de devoir en urgence parcourir tout le parc informatique pour savoir si on est concerné par telle ou telle alerte de sécu

Étape 2 : Évaluer les risques

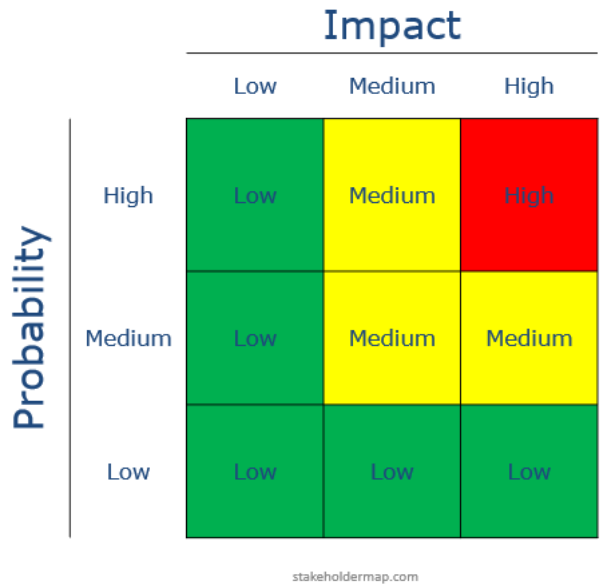


> Objectif

- Identifier ce qui pourrait mal se passer et à quel point c'est grave

> Méthode

- Utiliser des grilles d'évaluation (ex. : risque faible/moyen/élevé)
- Se demander :
  - "Que se passe-t-il si le système tombe en panne ?" (ex. : arrêt des urgences)
  - "Que se passe-t-il si les données fuient ?" (ex. : amende RGPD)



> Outils

- EBIOS Risk Manager (lien dans le document) pour les systèmes critiques
- Questionnaire simplifié pour les petits projets

> Exemples de valeurs apportées par cette étape

- Identifier les « angles morts », les « zones grises », les « cônes d'ombre »
- Eviter de conserver des risques cyber au niveau opérationnel, sans les formaliser, et sans que la chaine managériale soit au courant

Étape 3 : Sécuriser

> Objectif

- Mettre en place des protections concrètes contre les risques identifiés

> Mesures types

- **Basique** : Antivirus, mises à jour régulières, mots de passe robustes, sauvegarde des données
- **Avancé** : Chiffrement des données, authentification à 2 facteurs

> Exemple : Pour un site web

- **Basique** : Installer un certificat SSL (🔒 dans la barre d'URL)
- **Avancé** : Limiter le nombre de tentatives de connexion (anti-bruteforce)

> Exemples de valeurs apportées par cette étape

- Suivre les bonnes pratiques de sécurité (en profondeur, en zero-trust …)
- Eviter l'illusion de croire qu'on est protégé contre toutes les sources de menaces alors qu'on n'en traite qu'une seule

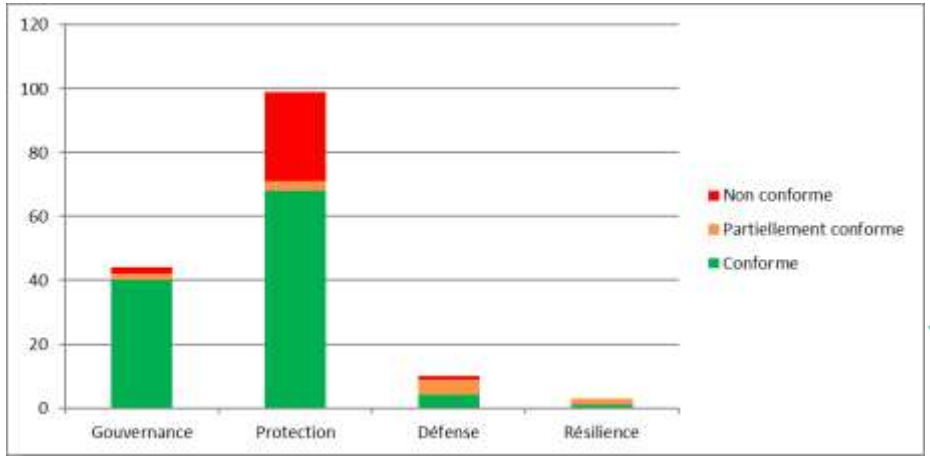
Étape 4 : Préparer la décision

> Objectif

- Rassembler les preuves que tout est sécurisé pour convaincre l'autorité

> Contenu du dossier d'homologation

- Description du système : inventaire et cartographie
- Plan de traitement des risque : liste des risques cyber et mesures appliquées
- Résultats des audits : vérifications, tests de pénétration
- **Recommandation** : Ne pas cacher les risques résiduels
  - ex. : « On n'a pas encore corrigé X, mais voici le plan »



> Exemple : Le dossier pour un site web inclut

- Les preuves des sauvegardes automatiques
- Le rapport d'audit montrant que les failles critiques sont corrigées

> Exemples de valeurs apportées par cette étape

- Mettre en place des politiques de maintien en condition d'homologation (et de sécurité) par amélioration continue
- Être proactif, éviter de traiter au coup par coup uniquement suite aux contrôles …. Ou en pleine crise cyber

Étape 5 : Décider

> Objectif

- L'autorité valide ou refuse l'homologation, avec une durée limitée

> Qui décide ?

- **Pour une mairie** : le maire.
- **Pour une entreprise** : le Directeur Général, ou l'Autorité Qualifiée pour Sécuriser les Systèmes d'Information (AQSSI)

> Durée

- De 6 mois à maximum 3 ans (car les menaces évoluent)
  - Comme un contrôle technique pour une voiture : à renouveler régulièrement !

> Cas de refus :

- Si les risques sont trop élevés, l'autorité peut demander des corrections avant de signer

> Exemples de valeurs apportées par cette étape

- Embarquer les parties prenantes au bon niveau de reesponsabilité
- Avoir le sponsoring adéquat

Les pièges à éviter

> L'homologation n'est pas un sprint, mais un marathon. Évitez ces erreurs courantes !

Erreur	Conséquence	Solution
1. "On sécurise après le déploiement."	Coûts élevés pour corriger en urgence.	Intégrer la sécurité **dès la conception**.
2. "C'est l'affaire des informaticiens."	Risques mal évalués (ex. : oubli des aspects métiers).	Impliquer **tous les services** (RH, juridique...).
3. "On cache les risques résiduels."	Décision d'homologation **invalide**.	**Transparence** : lister les risques restants + plan d'action.
4. "Une fois homologué, c'est fini."	Le système devient vulnérable avec le temps.	**Surveillance continue** (audits annuels).

Conclusion & Ressources

Conclusion

> L'homologation est un investissement, pas une dépense : elle protège votre organisation et vos parties prenantes

> En synthèse

- **Pourquoi** : Obligation légale et/ou démarche de réduction des risques cyber
- **Qui** : Tous les acteurs (pas seulement les experts cyber). Le contact à privilégier en premier est le RSSI
- **Comment** : 5 étapes structurées + maintenir une amélioration continue et éviter les pièges

> Ressources utiles :

- Le référentiel général de sécurité (RGS) — ANSSI
- MonServiceSécurisé
- Tout savoir sur l'homologation de sécurité | MonServiceSécurisé
- Homologation de sécurité — ANSSI
- Guide d'homologation de l'ANSSI : ce qu'il faut savoir en 2025
- Homologation sécurité : expériences partagées
- Processus de démarche d'homologation - armement.defense.gouv.fr
- MonEspaceNIS2 - Directive NIS 2

THALES
Building a future we can all trust

Questions ?

www.thalesgroup.com

THALES
Building a future we can all trust

Merci

www.thalesgroup.com

Les attaques notables en France en Décembre 2025

- **La Poste (22-26 décembre)** : Paralysie d'infrastructure critique via attaque DDoS
- **Mondial Relay & Colis Privé (novembre-décembre)** : Exfiltration de 25 millions d'enregistrements de données personnelles
- **Ministère de l'Intérieur** (décembre) : Accès non autorisé aux fichiers, affectant potentiellement 16,4 millions d'individus
- **Ministère des Sports, Jeunesse et Vie Associative** (19 décembre) : Compromission affectant 3,5 millions de foyers
- **Centre National de la Recherche Scientifique** (décembre 2025) : Exfiltration de données techniques relatives à l'instrument NectarCam, constituant un acte d'espionnage scientifique
- **Ville de Lens** (24-25 décembre) : Intrusion informatique compromettant les services municipaux
- **Duick — Brasserie Jenlain** (décembre) : Compromission d'infrastructure critique du secteur agroalimentaire
- **Ministère de l'Agriculture et de l'Alimentation** (28 décembre) : Exfiltration de 61 Go de données incluant journaux de connexion, bases SQL et configurations critiques
- **THT Bio Science** (26 décembre) : Laboratoire pharmaceutique compromis, données techniques exfiltrées