
Prévention
CYBER

40 %

des attaques CYBER touchent les TPE et PME

AXA a une réelle capacité à accompagner l'ensemble de ses assurés...

... en accompagnant toutes entreprises, quels que soient l'activité, la taille et le besoin.

Source : ANSSI, Rapport 2023 (Agence nationale de la sécurité des systèmes d'information)

L'accompagnement en cyber sécurité

AXA accompagne le client
pour le protéger des menaces Cyber

En savoir plus ❯

L'accompagnement en cyber résilience

AXA accompagne le client
dans la mise en place
d'une Cyber résilience réussie

En savoir plus ❯

DISPOSITIF DE CYBER RÉSILIENCE ❯

NOTRE DISPOSITIF PRÉVENTION ❯

Cyber sécurité

AXA accompagne le client pour le protéger des menaces Cyber

Aspects Organisationnels & Conformité

- Analyse des risques
- Audits Gouvernance - Risques - Conformité

Aspects Techniques

- Scan externe (Inclus dans le contrat)
- Board of Cyber - Security Rating® (Inclus dans le contrat)
- Les audits techniques : Tests d'intrusion, audits d'architecture ou de code
- Docaposte – Pack Tremplin Cyber

Aspects Facteurs humains

- Formation - Test de phishing (Inclus dans le contrat)
- Plateforme de sensibilisation Kamaé (Inclus dans le contrat)

Aspects Organisationnels & Conformité

Analyse des risques

L'analyse des risques est une étape essentielle d'une démarche de gestion des risques cyber qui est très largement préconisée aussi bien dans les normes et référentiels de bonnes pratiques de cybersécurité que dans la réglementation.

Objectifs visés, à titre d'exemples, selon les besoins

- Mettre en place ou renforcer un processus de management du risque cyber au sein de l'entreprise.
- Prendre en compte la cybersécurité dans le cadre d'un projet numérique.
- Définir le niveau de sécurité à atteindre pour un produit ou un service selon les cas d'usage envisagés.

Méthode

La méthode d'analyse est celle préconisée par l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'information), à savoir EBIOS Risk Manager. Très opérationnelle, modulaire et alignée avec les normes en vigueur, c'est la boîte à outils indispensable pour toute réflexion de sécurité des systèmes d'information (SSI). Pour plus d'information : **La méthode EBIOS Risk Manager – Le guide | Agence nationale de la sécurité des systèmes d'information (ssi.gouv.fr)**

Livrables

Les livrables correspondent aux résultats de tout ou partie des cinq ateliers de cette méthode, selon les objectifs définis au préalable.

Durée

À définir selon le type d'analyse à effectuer.

Coût

Sur devis, tarif préférentiel pour les assurés AXA IARD Entreprises.

Aspects Organisationnels & Conformité

Audits Gouvernance - Risques - Conformité

Les audits Gouvernance – risques – Conformité sont complémentaires aux audits techniques. Ils investiguent les aspects managériaux, organisationnels, humains de la cyber sécurité, ainsi que la conformité à la réglementation applicable et/ou aux bonnes pratiques.

Ils sont possibles aussi bien sur le système d'information de gestion que sur le système d'information industriel.

Objectifs visés

- Identifier les forces et faiblesses du système de management de la cybersécurité en place.
- Analyser les vulnérabilités et l'efficacité des moyens de prévention et de protection face aux risques cyber.
- Définir des actions d'amélioration pour renforcer le niveau de cybersécurité.

Méthode

Selon la taille de l'entreprise et ses besoins, trois types d'audits sont proposés : diagnostic flash, audit de maturité cyber, audit approfondi de cybersécurité.

	Méthode	Livrables	Durée	Coût
Diagnostic flash	Prestation réalisée sur le site de l'entreprise. Référentiel : guide d'hygiène de l'ANSSI	Rapport avec préconisations priorisées sous la forme d'un plan d'actions.	½ journée sur site	Sur devis, tarif négocié pour les assurés AXA IARD Entreprises
Audit de maturité cyber	Prestation réalisée sur le site de l'entreprise. Référentiels : guide d'hygiène de l'ANSSI	Rapport avec préconisations priorisées sous la forme d'un plan d'actions.	1 journée sur site	
Audit de cybersécurité	Prestation réalisée sur le site de l'entreprise. Référentiels : ISO 27001, NIST, …	Rapport avec préconisations priorisées sous la forme d'un plan d'actions.	À définir selon le périmètre et la granularité de la mission	

Aspects Techniques

Le scan externe

Le scan de vulnérabilités indique les faiblesses sur le périmètre internet de la société correspondant à des points d'attaques exposés et potentiellement exploitables par les attaquants pour s'introduire dans le système d'information.

Objectifs visés selon les besoins

- Connaître en permanence l'exposition Web de l'entreprise et ses vulnérabilités.
- Évaluer indirectement le niveau de maturité en cyber sécurité d'une organisation.
- Suivre dans le temps sa dynamique d'amélioration continue.
- Évaluer potentiellement l'écosystème de l'entreprise.

Méthode

Le scan de vulnérabilité consiste en une évaluation automatisée, continue et reproductible sur la base de données observables publiquement de l'empreinte de l'entreprise sur internet.

Livrables

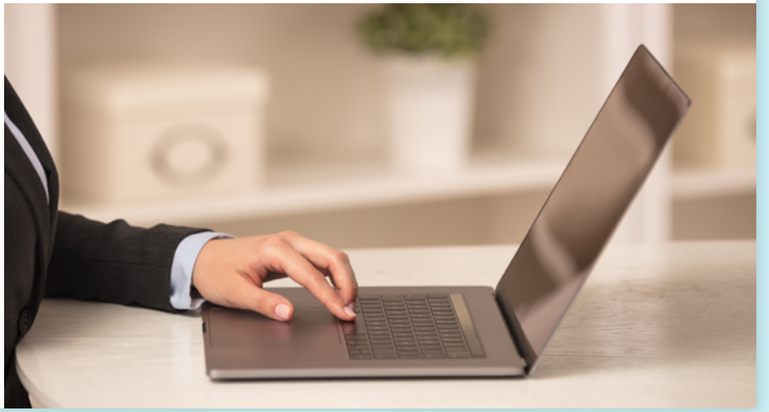
Deux livrables sont fournis: un rapport synthétique à destination de la Direction de l'entreprise et un rapport détaillé à destination de l'équipe informatique.

Durée

À définir selon le type d'analyse à effectuer.

Coût

Offert pour les clients d'AXA détenteurs d'un contrat d'assurance cyber.



Cyber sécurité

Board of Cyber - Security Rating®

Board of Cyber est une Société française spécialisée dans la cybersécurité, labélisée « France Cybersecurity 2024 ».

Inclus dans l'offre Global Cyber Secure

board of cyber

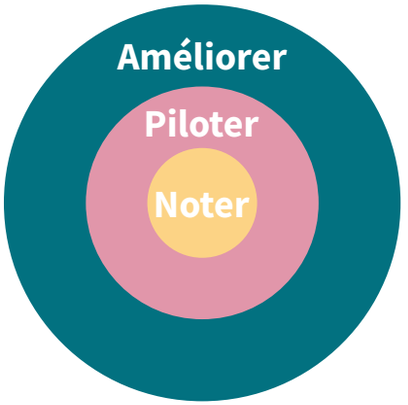
FRANCE CYBER SECURITY

Security Rating® propose d'évaluer la performance et la maturité en cybersécurité de votre organisation.

Notation hebdomadaire

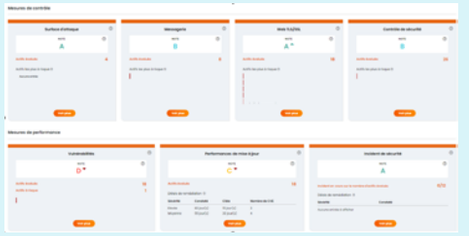
Notation non intrusive

Notation 100 % automatisée



Noter

Noter votre maturité cyber à travers **7 axes d'analyse**.



Piloter

Suivre en continu l'évolution de votre maturité cyber grâce à un tableau de bord.

Améliorer

Améliorer votre performance grâce au rapport détaillé avec les observables et les recommandations.

Comment accéder à l'offre ?

- Contactez votre Agent Général AXA pour fournir les informations nécessaires à l'ouverture des services. Ensuite, accédez aux services via votre espace client Ma Protection Entreprise, onglet « Prévention ».

Les audits techniques : Tests d'intrusion, audits d'architecture ou de code

Les audits techniques sont complémentaires des audits Gouvernance – Risques – Conformité. Ils sont possibles aussi bien sur le système d'information de gestion que sur le système d'information industriel.

Plusieurs types d'audits sont réalisables :
- Les tests d'intrusion (pentest)
- L'audit d'architecture
- L'audit de code

Objectifs visés, à titre d'exemples, selon les besoins

- Mettre en place ou renforcer un processus de management du risque cyber au sein de l'entreprise.
- Prendre en compte la cybersécurité dans le cadre d'un projet numérique.
- Définir le niveau de sécurité à atteindre pour un produit ou un service selon les cas d'usage envisagés.

Livrables

Les livrables correspondent aux résultats de tout ou partie des cinq ateliers de cette méthode, selon les objectifs définis au préalable.

Durée

À définir selon le type d'analyse à effectuer.

Coût

Sur devis, tarif préférentiel pour les assurés AXA IARD Entreprises.

Cyber sécurité

Aspects Techniques

Service à partir de 9,99 € HT/mois/poste

DOCAPOSTE

BIENTÔT DISPONIBLE

Docaposte - Pack Tremplin Cyber

Le pack tremplin Cyber de Docaposte s'appuie sur l'expertise des meilleures solutions technologiques du marché.

Sécurisez votre entreprise avec un pack technologique permettant de traiter les principaux aspects de la protection cyber.

★ Découvrez le pack de services Docaposte

Docaposte propose un portail unique et une combinaison gagnante de **3 solutions complémentaires et essentielles :**

Protection de vos équipements

Dispositif de détection, blocage et analyse des cyberattaques (EDR managé).

Protection de vos données

Sauvegarde sécurisée de vos données **(jusqu'à 50 Go par utilisateur)** : chiffrement des sauvegardes, interdiction des modifications et accès authentifié

Protection de votre messagerie

Filtrage des mails contre les courriers indésirables et les malwares.

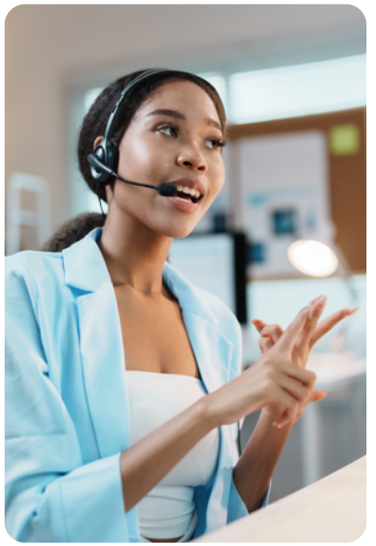
Service en option

★ Bénéficiez d'un accompagnement personnalisé

Un interlocuteur unique : Mise en œuvre coordonnée par Docaposte

- Un modèle simple et abordable directement piloté depuis un espace client
- Accompagnement dans l'installation des agents EDR et sauvegardes (vidéos, tutos, FAQ, support téléphonique et visio)

Un support téléphonique et mail est disponible pour toute question



★ Bénéficiez d'une offre à tarif préférentiel AXA

- Contactez votre Agent Général AXA pour savoir comment bénéficier de l'offre.

Aspects Facteurs Humains

La formation – le test de phishing

La très grande majorité des cyber attaques exploitent les vulnérabilités humaines, notamment par l'envoi d'un mail de phishing.

La formation des utilisateurs aux bonnes pratiques d'hygiène informatique représente donc un enjeu essentiel de cybersécurité.

Objectifs visés

- Faire des utilisateurs la première ligne de défense du dispositif de cybersécurité.
- Maintenir et améliorer en continue la robustesse de cette première ligne de défense.

Méthode

- Actions de sensibilisation et de formation en distanciel ou en présentiel.
- Organisation de campagnes tests de phishing.

Livrables

Tableau de bord de suivi des sessions de formation et des résultats obtenus.

Fréquence ou Périodicité

À définir selon les objectifs de l'entreprise.

Coût

Offert pour les clients d'AXA détenteurs d'un contrat d'assurance Cyber. Possibilité d'aller plus loin avec une offre approfondie à un tarif préférentiel (demande à faire à notre partenaire via sa plateforme).

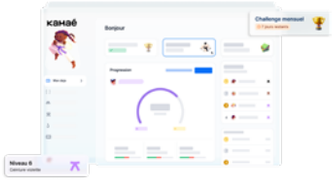
Plateforme de sensibilisation Kamaé

Inclus dans l'offre Global Cyber Secure

Engagez vos collaborateurs à se protéger face aux risques cyber.

Augmentez l'engagement de vos équipes et diminuez vos risques cyber grâce à une plateforme simple, attractive et gamifiée.

Vos collaborateurs s'entraînent avec des micro-learnings interactifs, gagnent des points et passent progressivement leurs ceintures, comme au judo.



Visualisez facilement leur progression en temps réel grâce à des tableaux de bord.

Offert avec votre contrat Cyber Secure d'AXA

Micro-learnings et challenges
5 modules d'entrainement sur les fondamentaux
+ 1 challenge sous forme de mini quiz

Tests de phishing
2 tests de phishing par an

Kit de prévention
Des fiches réflexes à télécharger pour sensibiliser en dehors de la plateforme

Pilotage et suivi
Suivi ludique grâce à des classements individuels et **par équipe** ainsi qu'un **reporting global**

Comment accéder à l'offre Kamaé ?

- Contactez votre Agent Général AXA pour fournir les informations nécessaires à l'ouverture du service. Ensuite, accédez au service via votre espace client Ma Protection Entreprise, onglet « Prévention ».

Envie d'aller plus loin ? Profitez d'une offre à tarif préférentiel AXA

- Formation approfondie sur les fondamentaux
- Campagnes de tests de phishing en illimité
- Accompagnement dédié

Cyber résilience

AXA accompagne le client dans l'anticipation d'une Cyber attaque réussie

Audit

- Diagnostic Cyber résilience

Aspects Organisationnels

- PCA
- PCI
- PRA SI
- PCA Cyber

Exercice de crise

- Gestion de crise

Audit

L'audit diagnostic de cyber résilience

Objectifs visés

- Identifier les points forts et les points d'améliorations possibles de l'environnement informatique de l'entreprise.
- Proposer des recommandations opérationnelles face aux risques cyber.

Méthode

La démarche est fondée sur les bonnes pratiques (retour d'expérience, recommandations de l'ANSSI) ainsi que les standards ISO 27001 et ISO 22301.

Livrables

Rapport avec préconisations priorisées sous la forme d'un plan d'actions.

Durée

À définir selon le type d'analyse à effectuer.

Coût

Sur devis, tarif préférentiel pour les assurés AXA IARD Entreprises.

État des lieux SI/SSI

Analyse et préconisation

Le Plan de Continuité d'activité (PCA)

L'entreprise peut être confrontée à un événement majeur impactant tout ou partie de ses ressources vitales :

Indisponibilité du site et d'équipements
(incendie, inondation, perte d'utilités...)

Indisponibilité des ressources humaines
(mouvement social, pandémie...)

Indisponibilité de l'informatique
(arrêt du SI, cyber attaques...)

Indisponibilité de fournisseurs stratégiques
(sous-traitants, fournisseurs prestataires...)

Objectifs visés, selon les besoins de l'entreprise

- Identifier les points forts et les points d'améliorations possibles du dispositif de continuité d'activité existant.
- Concevoir et mettre en œuvre un dispositif de continuité d'activité.
- Accompagner l'entreprise à l'obtention de la certification ISO 22301 (norme sur la continuité d'activité).

Modes dégradés

La démarche est fondée sur le standard international ISO 22301.

Livrables

Selon les objectifs visés.

Durée

À définir selon le type d'accompagnement à effectuer.

Coût

Sur devis, tarif préférentiel pour les assurés AXA IARD Entreprises.

Service PCA Entreprise

Le Plan de Continuité Informatique (PCI)

Le plan de continuité informatique est l'un des éléments essentiels constituant la politique de sécurité du système d'information qui vise à faire face à un évènement majeur susceptible d'impacter le système informatique.

Destruction ou arrêt d'une salle de machine

Interruption du système d'information et des applications

Interruption de la téléphonie

Défaillance de prestataires/ de fournisseurs stratégiques

★ Livrables

Selon les objectifs visés.

★ Durée

À définir selon le type d'accompagnement à effectuer.

★ Coût

Sur devis, tarif préférentiel pour les assurés AXA IARD Entreprises.

★ Objectifs visés, selon les besoins de l'entreprise

- Identifier les points forts et les points d'améliorations possibles du dispositif de continuité informatique existant.
- Concevoir et mettre en œuvre un dispositif de continuité informatique.

★ Méthode

La démarche est fondée sur les standards internationaux ISO 22301, ISO 27001-27002, et ISO 24762.

Phasage du projet ❯

Élaboration du PCI ❯

Aspects Organisationnels

Plan de Reprise des Activités du SI (PRA SI)

La reprise de votre SI est fondée sur les 4 piliers suivants :

Actifs critiques

Sauvegardes

Bascule

Reconstruction

Parmi les dispositifs de continuité (PCA/PCI), le Plan de Reprise des Activités du SI est essentiel pour anticiper et atténuer les risques liés aux interruptions des processus, à la perte ou à la détérioration des actifs critiques.

Le plan de reprise des activités du SI est défini par l'Afnor FD Z 90-004, associé à l'ISO 22301 (PCA / PCI) et l'ISO 27001 (SSI) afin d'assurer la continuité opérationnelle de l'entreprise face à des évènements tels que les cyber attaques, défaillances matérielles ou catastrophes naturelles...

L'objectif du PRA SI est de garantir la disponibilité, l'intégrité et la confidentialité des données, en renforçant la résilience de l'entreprise.

★ Mise en œuvre d'un PRA du SI

Prise en compte de l'existant
- Identification des actifs critiques et de l'infrastructure SI existante
- Identification des besoins métiers (RTO/RPO)
- Etude du plan de sauvegarde et des procédures de restaurations existantes
- Etude des risques et menaces
- Etude du plan de tests

Ebauche du PRA SI
- Identification des scénarios de risques
- Vérification de la complétude des données
- Réalisation du chronogramme de reconstruction et /ou bascule en priorisant les étapes
- Rédaction des procédures manquantes et consolidation des procédures existantes (plan de test inclus)
- Préparation du plan d'actions

Test du PRA SI
- Evaluation des capacités d'ordonnancement de la reprise du SI
- Réalisation d'un test sur tout ou partie du SI (Test de bascule, Test sur site secondaire, Test de simulation, etc.)
- Réalisation de tests d'intégrité (actifs métiers et dépendances)
- Retour d'expérience et mise à jour du plan d'actions

Aspects Organisationnels

Le Plan de Continuité d'Activité Cyber (modes dégradés métiers)

L'entreprise peut être confrontée à une cyber attaque paralysante :

Indisponibilité prolongée de l'informatique
(cyber attaque, cryptolocker, ransomware...)

Temps long de reconstruction du SI
(multiples levées de doute, remédiations ardues et incertaines...)

Pas de perspective de retour à la normale avant plusieurs jours, voire plusieurs semaines

Paralysie de l'activité, arrêt de production, perte d'exploitation, impact image et réputation, défaut de conformité

★ Objectifs visés, selon les besoins de l'entreprise

- Identifier les points forts et les points d'améliorations possibles du dispositif de continuité d'activité « métiers » existant lors de l'indisponibilité du système d'information.
- Concevoir et mettre en œuvre un dispositif de continuité d'activité cyber (modes dégradés métiers).

★ Modes dégradés

La démarche est fondée sur le standard international ISO 22301.

★ Livrables

Selon les objectifs visés.

★ Durée

À définir selon le type d'accompagnement à effectuer.

★ Coût

Sur devis, tarif préférentiel pour les assurés AXA IARD Entreprises.

Accompagnement PCA Cyber ❯

Exercice de crise

La gestion de crise cyber

Objectifs visés, selon les besoins de l'entreprise

- Concevoir et mettre en œuvre une structure de gestion de crise cyber.
- Organiser un exercice de gestion de crise cyber.

Méthode

La démarche est fondée sur les standards internationaux ISO 22301, ISO 27001-27002, et les bonnes pratiques de l'ANSSI.

Livrables

Selon les objectifs visés.

Durée

À définir selon le type d'accompagnement à effectuer.

Coût

Sur devis, tarif préférentiel pour les assurés AXA IARD Entreprises.

Mise en place de la gestion de crise Cyber

Préparation et animation d'un exercice de crise Cyber

Glossaire

ANSSI : Agence nationale de la sécurité des systèmes d'information

DRP : Traduction en anglais du Plan de Reprise après sinistre (ou PRA)

PCA : Plan de continuité d'activité

PCI : Plan de continuité informatique

PRA : Plan de reprise des activités

PSSI : Politique de Sécurité des Systèmes d'Information

RPO : Recovery Point Objective (Traduction en anglais de la durée maximum d'enregistrement des données qu'il est acceptable de perdre lors d'une panne)

RTO : Recovery Time Objective (Traduction en anglais de la Durée maximale d'interruption admissible d'une ressource informatique)

SLA : Service-level agreement

AXA vous répond sur :

Réf. 2003968 02 2025 - Crédit photos : Shutterstock, Getty Images