Une Gouvernance de la sécurité de l'information adaptée à vos risques

Service Offer

La sécurité de vos informations n'est pas qu'une question technique. Leur protection repose avant tout sur une gouvernance basée sur ISO 27'001 et adaptée à votre organisation et aux risques auxquels elle est confrontée.

Comprendre les menaces, évaluer les risques, adapter l'organisation, sélectionner et implémenter les contrôles adéquats, ainsi que mettre en œuvre un système de management sont les activités qui s'imposent pour instaurer une gouvernance proactive de la sécurité qui donnera à la Direction et aux clients l'assurance d'un dispositif efficace pour gérer vos risques.

Une exposition aux risques croissante

La multiplication des données internes et externes, ainsi que l'augmentation des plateformes digitales de gestion, de collaboration et de partage exposent les organisations à des risques croissants au niveau de leurs informations.

Si la presse relaie un nombre grandissant de cyberattaques, des menaces subsistent au sein même des organisations. La méconnaissance par les collaborateurs de la sensibilité des informations, leur accès trop large aux actifs critiques ou une application hétérogène des règles de sécurité constituent autant de risques d'altérer la confidentialité, l'intégrité et la disponibilité des informations.

Une gouvernance nécessaire et stratégique

En réaction à cette situation, les Directions, les clients, les partenaires et les régulateurs développent des exigences croissantes en termes de sécurité de l'information qui, dans certains cas, vont jusqu'à la nécessité de faire état d'une certification reconnue.

La sécurité de l'information devient ainsi capitale pour les organisations et l'adoption d'un système de management de la sécurité constitue une décision stratégique de la Direction. Car la complexification des écosystèmes exige une vision et une gouvernance transverses pour s'assurer de dispositifs sécuritaires adaptés aux risques.

Une indispensable compréhension des risques

La gouvernance de la sécurité doit être adaptée à vos exigences et à vos objectifs. Elle est indissociable des menaces et vulnérabilités auxquelles votre organisation et son activité sont exposées. C'est l'ensemble de ces éléments qui orientera votre dispositif sécuritaire.

Une composante de la structure de management

Pour soutenir sa dimension stratégique, il est important que le système de management de la sécurité fasse partie intégrante de la structure de management de l'organisation.

Les processus de sécurité et les contrôles qui seront instaurés auront pour but de réduire les vulnérabilités mais ils devront aussi fournir une vision opérationnelle ainsi que des indicateurs pour permettre un pilotage efficace.

Ce que nous offrons

Nous vous proposons une approche structurée et modulable basée sur vos risques spécifiques et qui repose sur le référentiel ISO 27'001. Notre accompagnement peut inclure une démarche de certification ou simplement permettre la mise en place d'une gouvernance de la sécurité efficace.

Cette approche se décline selon les quatre étapes suivantes :

› L'**appréciation de vos risques** de sécurité, de conformité ou de réputation, basée sur l'analyse de votre organisation, de votre activité, de vos exigences et des menaces auxquelles vous faites face.

› L'**établissement du périmètre** d'intervention et la sélection des contrôles opérationnels requis pour satisfaire vos exigences et réduire les risques. La documentation de ce périmètre par la déclaration d'applicabilité (SoA) servira de base à une certification éventuelle. Elle sera dans ce cas soumise à votre auditeur.

Une Gouvernance de la sécurité de l'information adaptée à vos risques

Service Offer

Une approche structurée et modulable fondée sur la gestion des risques

Étapes	Appréciation des risques	Établissement du périmètre	Analyse des écarts et planification	Mise en œuvre du système de management
Thèmes	Organisation, objectifs, menaces et exigences	Sélection des contrôles opérationnels	Écarts et priorisation	Processus, politiques, contrôles et indicateurs
Livrables	Ambitions, politique générale, risques	Déclaration d'applicabilité	Plan de traitement des risques	Gouvernance, traitements et amélioration continue

› L'**analyse des écarts** et la **planification** et priorisation du traitement des risques qui servira de référence pour la mise en œuvre de l'amélioration continue.

› La mise en œuvre du **système de management** de la sécurité. Elle inclut les processus, les contrôles, la sensibilisation de vos collaborateurs, la diffusion d'une culture de sécurité, mais aussi la mise en place de tableaux de bord et d'indicateurs qui vous permettront de vous assurer de l'efficacité de vos investissements dans vos dispositifs de sécurité et du suivi des menaces.

Cette dernière étape réalisée, votre système de management de la sécurité peut être soumis à un audit annuel pour l'obtention d'une certification.

renouvelable

ISO 27'0000

Ce cadre constitue une famille de référentiels se référant au système de management de la sécurité ISMS. ISO 27'001 fournit les exigences et traitements de la sécurité incluant notamment la sécurité physique et logique, les aspects organisationnels et légaux.

Vos bénéfices

› Une démarche alignée sur vos objectifs stratégiques, vos exigences sécuritaires et votre tolérance aux risques.

› Une gouvernance reposant sur une organisation, des processus, des politiques, des contrôles et des indicateurs calibrés pour répondre aux menaces auxquelles vous êtes exposé.

› Des dispositifs de sécurité efficients en adéquation avec la gouvernance souhaitées.

› Une meilleure protection de vos actifs informationnels.

› La réduction des risques et vulnérabilités de sécurité.

› La capacité de valoriser vos dispositifs de sécurité auprès de votre organisation et de vos partenaires, p.ex. par le biais d'une certification ISO 27'000.

Notre approche de la sécurité de l'information