



Audit Sécurité de l'Information

Mesurer votre degré de maîtrise en sécurité

Défendre les systèmes d'information qui soutiennent votre performance est une exigence forte dans un contexte d'échanges croissants d'information. Seule une organisation efficace concentrée sur les risques majeurs est capable de faire face aux multiples risques informatiques. Pour y parvenir, il est fondamental de mesurer l'exposition de vos ressources, l'efficacité de vos dispositifs de réponse et l'étendue des risques couverts [continuité d'activité, physique, informatique et réseaux, organisation & réglementation].

Notre intervention d'analyse répond à vos préoccupations :

- Identifier les risques extrêmes non couverts
- Mesurer l'impact des sinistres informatiques sur vos métiers
- Aligner votre démarche sécurité sur la stratégie de votre organisation
- Améliorer l'efficacité de votre action de prévention et de réduction des risques

L'information cruciale de mes métiers est-elle protégée ?

Mon organisation maîtrise-t-elle les enjeux de sécurité ?

Mes dispositifs de sécurité sont-ils vraiment adaptés à mes risques ?

Comment nous situons nous par rapport aux bonnes pratiques ?

Pour mieux protéger vos ressources critiques

Spécialisé dans l'audit et l'accompagnement de la fonction informatique, **audéa** a développé une méthodologie et des outils adaptés à la mesure et à l'amélioration de votre organisation en sécurité des SI.

Dans le cadre d'une démarche de contrôle interne, d'anticipation des risques ou d'amélioration permanente, nos auditeurs réalisent un diagnostic, en toute indépendance.

Pragmatiques et économiques, nos recommandations s'appuient sur un référentiel reconnu : les normes ISO de la famille 27000.

Les normes de la famille ISO 27000 (dont 27002, l'ancienne ISO 17799) ont été conçues pour :

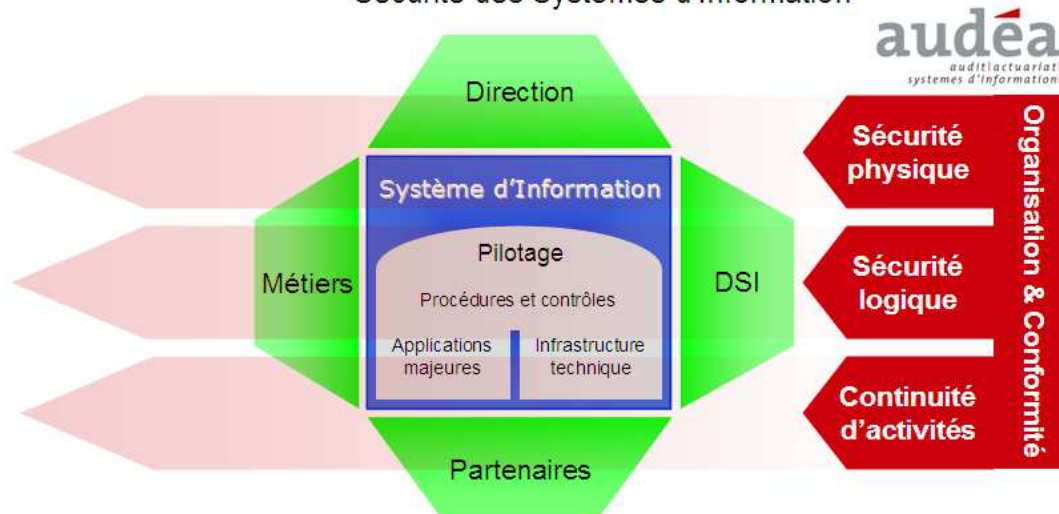
- Mettre en place une organisation sécurité cohérente et efficace
- Effectuer une analyse des risques sécurité
- Assurer la prise en compte de ces risques transversaux par l'organisation
- Adapter les mesures de sécurité aux capacités humaines, techniques et financières

audéa les enrichit par l'apport :

- D'une méthodologie « orientée client »
- D'outils d'analyse technique et organisationnelle
- De bonnes pratiques efficaces, validées sur le terrain



Notre démarche d'audit Sécurité des Systèmes d'Information





Exemple de réalisation

Mission Audit de sécurité informatique

Client Compagnie d'assurance

■ Nature des travaux

Dans le cadre de la refonte des Systèmes d'Information de la compagnie, nous avons réalisé l'audit-diagnostic de la fonction Sécurité des Systèmes d'Information.

Nos travaux ont consisté à :

- ▶ Analyser la fonction sécurité des systèmes d'information suivant les normes ISO :
 - Organisation et conformité,
 - Sécurité physique,
 - Sécurité logique (informatique et réseaux),
 - Continuité d'activités,
- ▶ Identifier l'émergence de risques nouveaux,
- ▶ Vérifier que le serveur de données des dirigeants n'est pas accessible du réseau interne,
- ▶ Synthétiser les constats effectués,
- ▶ Proposer des pistes d'amélioration adaptées aux besoins et classées par priorité.

■ Résultats

▶ Constats

La refonte des Systèmes d'Information a provoqué une forte tension sociale au sein de l'organisation.

Nos analyses ont permis d'identifier plusieurs zones de risque majeur :

- Les utilisateurs appliquent des règles anciennes sans conscience des enjeux et négligent des risques évidents (ils ne transportent pas de documents confidentiels sur leur ordinateur portable, mais n'effacent pas leur clé USB et jettent les versions papier sans destruction).
- L'outil de prise en main à distance utilisé par le support technique peut être utilisé à l'insu de l'utilisateur « supporté ». La fonctionnalité qui signale ce fait à l'utilisateur n'est simplement pas activée.
- Il n'est pas possible de se connecter aux bases de données des dirigeants mais il est possible de copier leurs fichiers de stockage par les partages Windows (et de les exploiter sur une autre machine). Les droits d'accès ne sont pas suffisamment durcis.

▶ Plan d'action

Note client a concentré ses efforts sur la réduction des risques les plus pressants identifiés lors de l'audit. Ces travaux ont conduit à :

- Modifier les droits d'accès aux fichiers du serveur des dirigeants pour en interdire la consultation aux administrateurs et aux autres utilisateurs,
- Organiser des séances de sensibilisation sécurité sur la bonne gestion des documents, des clés USB et former chacun au respect des règles de protection de ces outils,
- Renforcer les protections et la traçabilité de l'outil de prise en main à distance des postes de travail utilisés par le support technique,
- Installer des broyeuses de documents performantes dans les locaux et promouvoir leur usage.