



ISO 27001

INFORMATION SECURITY MANAGEMENT

CERTIFIED BY



ISO/IEC 27001 – Système de management de la sécurité de l'information

La sécurité de l'information implique la protection des informations et systèmes d'information contre leur accès, utilisation, divulgation, perturbation, modification ou destruction par des personnes non autorisées. Depuis plus de vingt ans, la sécurité de l'information a pour principes majeurs la confidentialité, l'intégrité et la disponibilité de l'information (confidentiality, integrity, availability ou "triade CIA"). Un système de management de la sécurité de l'information (SMSI) fait partie du système global de management des entreprises et renforce la sécurité des informations dans le cadre de la gestion du risque.

Your tailor-made solution

Le concept clé d'un SMSI pour une organisation est la conception, la mise en œuvre et le maintien d'un ensemble cohérent de processus et systèmes visant à gérer efficacement l'accessibilité de l'information. Comme tout processus de management, un SMSI doit demeurer efficace et efficient sur le long terme et doit être adapté aux changements intervenant dans l'organisation interne et l'environnement externe. ISO/IEC 27001 intègre la fameuse roue de Deming « Plan-Do-Check- Act » (Planifier – Réaliser – Vérifier – Agir) dans une optique d'amélioration continue.

ISO/IEC est la norme reconnue dans le domaine critique de la gestion du risque. Elle est actuellement de plus en plus utilisée par les clients du secteur privé et du secteur public afin d'évaluer les performances de leur système de sécurité de l'information.

Your result

Une certification ISO/IEC 27001 vous aidera à gérer et protéger vos actifs informationnels précieux. Elle vous aidera à gagner la confiance de toutes les parties intéressées et en particulier de vos clients.

Par le biais d'une approche systématique, la norme garantit la continuité des activités, réduit au minimum les pertes d'activité et permet de définir les actifs critiques. Elle améliore la compréhension des aspects de l'entreprise et vous donne l'assurance d'avoir fait les bons investissements en matière de sécurité de l'information. Nous vérifions de manière indépendante que les risques inhérents à votre organisation ont été correctement identifiés via l'évaluation des risques d'entreprise.

Le processus d'évaluation régulière vous aide à accroître l'efficacité de vos activités et à améliorer vos obligations en termes d'assurances. Plus important encore : cette norme vous donne confiance, motive le management et permet également de promouvoir la qualité de votre sécurité auprès de vos clients.

Please note

Législations

- - Droits de propriété intellectuelle
 - Protection des informations concernant l'organisation
 - Protection des données et respect des informations personnelles
 - Prévention de l'utilisation abusive des équipements de traitement de l'information
 - Réglementation des contrôles cryptographiques

Normes et standards

ISO/IEC 27001:2013 Technologies de l'information – Techniques de sécurité - Systèmes de management de la sécurité de l'information - Exigences.

In which situation?

Base pour la famille 27k :

- ISO/IEC 27002 Technologies de l'information – Techniques de sécurité – Code pour la sécurité de l'information
- ISO/IEC 27003 Guide de mise en œuvre
- ISO/IEC 27004 Mesurages SMSI
- ISO/IEC 27005 Approche de la gestion du risque
- ISO/IEC 27006 Processus de certification
- ISO/IEC 27007 Système d'audit
- ISO/IEC 27008 Contrôles des audits
- ISO/IEC 27011 Lignes directrices pour l'industrie des télécommunications
- ISO/IEC 27013 Intégration avec les SMSTI
- ISO/IEC 27014 Gouvernance
- ISO/IEC 27015 Secteur de la finance et de l'assurance
- ISO/IEC 27031 Continuité des affaires
- ISO/IEC 27032 Cyber sécurité
- ISO/IEC 27033 Sécurité du réseau IT
- ISO/IEC 27034 Sécurité des applications