claranet
helping our customers do amazing things

La certification ISO/IEC 27001:2013 permet de renforcer la confiance de vos clients et constitue un avantage concurrentiel réel pour certaines offres de vos services.

Claranet, société spécialisée en réseau et hébergement d'applications critiques, a été certifiée conforme à la norme ISO/IEC 27001:2013 par BSI Group France. Alexandre LAUGA, CISO / Head of Security & Compliance, répond à nos questions au sujet de cette certification.

BSI Group : Organisme de normalisation et de certification qui aide les organisations à faire de l'excellence une habitude partout dans le monde. Nous le réalisons grâce à une gamme unique de produits et de services, qui vous permet en premier lieu de comprendre en quoi consiste la meilleure pratique, comment y arriver et finalement intégrer l'excellence comme une habitude constante au sein de votre organisation.

Notre intégrité, notre expertise et l'expérience client que nous offrons, répondent aux besoins des organisations pour inspirer de la confiance et améliorer leur activité.

Claranet : Fondé en 1996, Claranet est un Managed Service Provider, spécialisé en réseau et hébergement d'applications critiques. Le groupe Claranet comprend 18 bureaux et 35 centres d'hébergement. Comptant 1 200 collaborateurs répartis sur 7 pays, Claranet est devenu un acteur majeur des services managés en Europe (238 M€ de CA) et opère des solutions réseau et hébergement pour plus de 5 700 clients managés de tous secteurs d'activités, notamment Sarenza, Le Printemps, MyMajorCompany, Veolia Environnement et Airbus.

Claranet rassemble les meilleures compétences, technologies et procédures pour fournir des services managés flexibles, sécurisés et économiques, capables de garantir les performances réseaux et applicatives. Les entreprises peuvent se concentrer sur leur cœur de métier, pas sur la gestion de leur IT. Claranet est certifié ISO 27001, ISO 9001, PCI DSS et est agrée Hébergeur de Donnée de Santé à caractère personnel. Claranet est le premier leader du Magic Quadrant Gartner, catégorie « Managed Hybrid Cloud Hosting, Europe 2016 » à être certifiée AWS Premier Consulting Partner.

bsi.

...making excellence a habit.™

Pour quelles raisons vous a-t-il paru important de vous certifier ISO/IEC 27001 ?

La mise en place d'un SMSI permet de structurer la démarche sécurité d'une entreprise et de mettre en place une gouvernance pérenne. La certification ISO 27001 est la garantie par un tiers extérieur, expert sur ce domaine, que le SMSI est conforme aux exigences de la norme et qu'il le reste dans le temps.
Claranet est certifiée ISO 27001 depuis 2011 sur ses activités cœur de métier : cette certification nous permet de renforcer la confiance de nos clients et constitue un avantage concurrentiel réel pour certaines offres de services.

En quoi l'ISO 27001 est utile pour une entreprise dans l'hébergement et l'infogérance, comme Claranet ?

Contrairement à une entreprise « classique », le système d'information à protéger n'appartient pas à l'hébergeur mais à son client. L'ISO 27001 permet donc d'établir une relation de confiance entre les deux parties tout au long du projet d'externalisation : identification des besoins de sécurité, appréciation des risques, mise en œuvre de mesures de sécurité adaptées, contrôles d'efficacité et audits par le client, gouvernance et reporting sécurité.
D'une manière plus globale, l'ISO 27001 permet de gérer la conformité du SMSI par rapport à des référentiels choisis. Cette conformité est alors réévaluée chaque année dans le cadre de l'audit interne et lors des audits externes de certifications.
Initialement fondée sur le standard ISO 27002, la déclaration d'applicabilité (SoA) du SMSI de Claranet comprend également aujourd'hui le standard PCI-DSS et le formulaire P6 lié à l'agrément hébergeur de données de santé à caractère personnel (AHDS). L'ajout de ces standards au sein de notre SMSI permet de nous assurer du maintien continue de la conformité tout en optimisant les coûts associés (processus mutualisés, audit interne multi standards...).
En réponse aux évolutions de la réglementation et aux demandes de nos clients, nous envisageons d'ajouter de nouveaux standards à notre déclaration d'applicabilité en 2017 : ISO 22301, ISO 27017, ISO 27018 et RGPD.

Pourquoi avez-vous choisi BSI ?

Lorsque nous avons démarré notre démarche de certification ISO 27001 en 2011, BSI nous a été vivement recommandé par d'autres filiales du Groupe Claranet à l'échelle européenne.
Compte tenu de la qualité des audits réalisés et du retour constructif et adapté des auditeurs BSI, nous n'avons ni regretté ni remis en cause ce choix.

Comment avez-vous implémenté la norme et par quelles étapes avez-vous du passer ?

Le SMSI ayant l'appui de la Direction, le projet de mise en œuvre aura duré environ un an :
- formalisation des processus du SMSI,
- mise en place de la gouvernance sécurité,
- analyse d'écart ISO 27002 et première appréciation des risques,
- mise en œuvre des mesures de sécurité et collecte des premiers indicateurs,
- mesure des performances et audit interne,
- premier audit de certification.

Depuis 2011, le périmètre du SMSI n'a cessé d'augmenter : extension à de nouvelles offres de service, extension à de nouvelles filiales, ajout de nouveaux référentiels à la déclaration d'applicabilité...
En 2015, nous avons profité de la révision de la norme ISO 9001 pour mettre en place un Système de Management Intégré construit sur le framework de l'annexe SL. Ce système de management permet de fédérer et de mutualiser les processus 27001:2013 et 9001:2015.

Comment avez-vous impliqué les salariés dans la mise en place et le maintien de la certification ?

Le périmètre du SMSI englobant initialement près de quatre-vingts pourcents des effectifs de Claranet, il était utopique d'avoir l'adhésion de tous les collaborateurs dès le début du projet. Nous avons donc suivi les principes de la norme et commencé par une implication top-down. Une fois le Middle Management suffisamment impliqué, nous avons élargi les actions de sensibilisation et de responsabilisation à l'ensemble des collaborateurs.
Le maintien dans le temps de cette implication repose sur une sensibilisation et une responsabilisation constante des collaborateurs :
- amélioration au fil des ans du processus de sensibilisation interne,
- contrôle permanent de l'équipe Sécurité et Conformité,
- campagnes d'audit interne tout au long de l'année,
- nombre croissant des audits externes sur site (audits clients et audits de certification).

Pour vous, quels sont les bénéfices issus de la mise en place d'un système de management ISO/IEC 27001 ?

Les bénéfices immédiats issus de la mise en place d'un SMSI sont, d'une part, la responsabilisation du Management à tous les niveaux de l'organisation et, d'autre part, la formalisation et la mise en œuvre obligatoire des processus et procédures nécessaires à la production d'enregistrements auditables.
A moyen terme, le SMSI devient le pilier de la démarche conformité et permet d'adresser des problématiques aussi bien réglementaires qu'organisationnelles, auprès des clients comme auprès des fournisseurs.

Qu'est-ce que les audits de BSI vous apportent ?

Les audits réalisés par BSI apportent une vision extérieure, factuelle et constructive sur la mise en œuvre du SMSI et des mesures de sécurité au sein de Claranet :
- extérieure, car l'auditeur se positionne en tiers de confiance : il a accès à toutes les informations internes de l'entreprise et engage sa responsabilité dans la délivrance du certificat ;
- factuelle, car l'auditeur fonde son constat sur les faits et s'appuie exclusivement sur les exigences de la norme pour identifier des écarts ;
- constructive, car l'auditeur s'appuie sur l'expérience qu'il a acquis pour identifier des opportunités d'amélioration adaptées au contexte de l'entreprise.

Les audits de BSI peuvent également s'avérer être un soutien important pour les décisions et recommandations portées par l'équipe Sécurité et Conformité auprès des équipes internes de Claranet.

Votre direction s'implique dans le système de management ? Si oui, de quelle manière ?

La Direction a un rôle crucial au sein du SMSI de Claranet : elle redéfinit chaque année les éléments stratégiques du SMSI (périmètre, métriques liées à l'appréciation des risques, objectifs de sécurité), valide les choix de traitement des risques et accepte les risques résiduels.
La Direction alloue de plus les moyens et ressources nécessaires à la mise en œuvre des plans d'actions (plan de traitement des risques et plan d'amélioration) et doit, le cas échéant, arbitrer les décisions.

Quels conseils donneriez-vous à des institutions ou aux entreprises qui aujourd'hui se posent des questions sur la norme ISO 27001 ?

La mise en place d'un Système de Management de la Sécurité de l'Information représente souvent un changement dans la culture de l'entreprise. Il faut donc être pédagogue et persévérant, afin de fédérer l'ensemble des parties prenantes autour de l'approche. Il ne s'agit pas seulement de créer le SMSI à un instant, mais de maintenir les efforts dans la durée pour s'inscrire dans une réelle démarche d'amélioration continue.
Ce projet peut paraitre complexe mais le retour sur investissement est appréciable rapidement. La certification permet quant à elle d'aller jusqu'au bout de la démarche, et la maintenir dans le temps permet de garantir l'engagement constant de l'entreprise.

bsi.

bsi. ISO/IEC 27001:2013 Information Security Management

Pour plus d'informations sur la norme ISO/IEC 27001:2013, contactez BSI au **01 55 34 11 40** ou rendez-vous sur **bsigroup.fr**