Certification ISO 27001 : tir groupé au GHT d'Armor

Pour favoriser la certification désormais obligatoire sur le périmètre de l'hébergement des données de santé, le groupement hospitalier de territoire d'Armor comprenant cinq établissements de médecine, chirurgie et obstétrique a lancé une démarche de certification ISO/CEI 27001 Lead Implementer pour l'ensemble des responsables du système d'information, en lien avec DSIH Formations.
Entretien avec Didier Bonnet, directeur du système d'information du GHT breton.

Pourquoi avez-vous souhaité que tous les référents du système d'information du GHT reçoivent une formation ISO/CEI 27001 ?

Le choix de former tous les managers SI, mais aussi le RSSI et l'ingénieur processus et qualité, s'inscrit dans une logique d'industrialisation de la sécurité de notre système d'information engagée depuis plusieurs années, avec notamment le recrutement d'un RSSI en 2012. Nous avions identifié l'intérêt d'une certification ISO 27000 dès 2014, lors de l'établissement de notre schéma directeur qui intègre la création d'une DSI en mode centre de services, nous faisant passer d'une mobilisation de moyens à un engagement de résultats pour lequel la sécurité est d'autant plus importante qu'elle influe sur la qualité de service.
Aller vers la certification nous permet d'officialiser le niveau de maturité de notre DSI sur la partie sécurité. Elle constitue également un levier d'adhésion complète de l'ensemble des membres de la DSI aux valeurs de sécurité et de confidentialité des données. Les gardiens de l'opérationnalité de la sécurité sont en effet les managers eux-mêmes, ceux qui, au quotidien, mobilisent leurs équipes.
Enfin, la certification va nous permettre d'aborder la question de l'hébergement des données de santé avec une meilleure maîtrise et de choisir plus facilement, à terme, les prestations que nous pourrons externaliser.

Quels autres bénéfices entendez-vous retirer de la certification ?

La certification est bénéfique à plusieurs niveaux. Elle contribue à nouer une relation de confiance entre la direction du système d'information et les utilisateurs, mais aussi entre le patient et l'établissement.
Avec la certification, nous espérons aussi limiter les efforts que nous devons déployer pour attester de notre niveau de sécurité. Nous sommes de plus en plus sollicités dans ce cadre par l'Agence régionale de santé lors de l'audit des prérequis dans le cadre du programme Hôpital numérique, par nos laboratoires de biologie médicale soumis à la certification Cofrac qui nous demandent de démontrer notre maîtrise du processus de sécurité ou encore par le commissaire aux comptes.
La certification nous permet également d'asseoir notre exigence vis-à-vis des prestataires externes qui doivent eux aussi répondre à des niveaux de certification.

Pourquoi avez-vous choisi DSIH Formations pour assurer ces formations ?

Nous avons choisi cet organisme pour le contenu de la formation, mais aussi pour la qualité des intervenants. Il se trouve que nous connaissions déjà l'un d'entre eux pour nous avoir accompagnés dans le dépôt de notre demande d'agrément d'hébergeur de données de santé. Nous n'avions aucun doute sur sa maîtrise du sujet et sa pédagogie.
Une première session à laquelle ont participé trois personnes nous a confortés dans notre choix. Elles ont apprécié les supports et la transmission d'un savoir concret et non conceptuel.
Parallèlement, nous avons pu bénéficier de souplesse dans le financement des formations de Lead Implementer et de Lead Auditor à venir, qui concernent respectivement onze et trois personnes. DSIH Formations nous a également proposé plusieurs dates possibles pour ces formations qui, du point de vue de notre organisation interne, ne peuvent se dérouler que de manière échelonnée.

Comment avez-vous sensibilisé la direction générale à ce projet de formation groupé ?

En 2009, nous avions entrepris d'élaborer une politique de territoire de sécurité du système d'information avec les deux établissements de santé mentale (Espic) et deux cliniques privées. Ces structures ne partageant ni les mêmes contraintes ni les mêmes approches que les établissements MCO, ce projet de territoire a abouti à la mise en œuvre d'une politique de sécurité du SI de groupe pour nos cinq établissements. Ce qui leur a permis d'atteindre d'excellents scores de conformité du SI (de 96 % à 100 %) dans le cadre de la certification 2017 de la Haute Autorité de santé.
Même chose pour Hôpital numérique : tous les prérequis relatifs à la sécurité du SI ont été très largement atteints, et ce dès 2014.
Cette démarche communautaire autour de la sécurité du SI, avec aujourd'hui une réelle conscience des utilisateurs des risques y afférents, est donc particulièrement visible par les directions qui s'en sont emparées. Nous n'avons plus besoin d'en démontrer l'intérêt.

Propos recueillis par Pierre Derrouch