# Foire Aux Questions

## WEBINAR

# Face à l'enjeu de sécurité de l'information, que vous apporte l'ISO 27001 ?

## 29 janvier 2015



Laboratoire national de métrologie et d'essais - 1, rue Gaston Boissier - 75724 Paris cedex 15 - France
Tél. +33 (1) 40 43 37 00 - Fax +33 (1) 40 43 37 37 - info@lne.fr - www.lne.fr

| | |
|---|---|
| **Q** | L'ISO 27002 peut-elle être appliquée aux produits ? |

| | |
|---|---|
| **R** | L'ISO 27002 est un guide de bonnes pratiques de sécurité des systèmes d'information. Cependant certaines bonnes pratiques sont applicables à des produits. |

| | |
|---|---|
| **Q** | Normaliser la sécurité, n'est-ce pas paradoxalement une vulnérabilité ? |

| | |
|---|---|
| **R** | L'ISO 27001 n'est pas un carcan qui détermine ce qu'on doit faire. L'ISO 27001 permet de s'assurer qu'on atteigne un certain niveau de sécurité, qu'on le maintienne, voir qu'on le dépasse.<br><br>Ce n'est pas la sécurité qui est normée, c'est sa gestion. |

| | |
|---|---|
| **Q** | Nous sommes prestataires pour des laboratoires d'analyses médicaux. Nous leur fournissons un middleware (logiciel de d'interfaçage entre les instruments et le SIL). Quel peut être notre rôle dans la mise en place de cette norme dans le laboratoire? |

| | |
|---|---|
| **R** | Si le laboratoire met en œuvre une démarche ISO 27001, il peut être amené à demander à ses prestataires de leur fournir un service avec un certain niveau de sécurité. Dans le cadre de la fourniture d'un middleware, cela passe par la mise en place d'un SDLC garantissant une application sans faille de sécurité. |

| | |
|---|---|
| **Q** | 27001 versus RGS ? Qui gère ?<br><br>Est-ce que l'ISO 27001 est un RGS +++? |

| | |
|---|---|
| **R** | Le RGS est une obligation réglementaire pour les autorités administratives, dans leur relation avec le public. Il définit six grands principes pour une gestion efficace de la sécurité des systèmes d'information<br><br>• Adopter une démarche globale de sécurisation des systèmes d'information<br>• Gérer les risques SSI<br>• Adapter la SSI selon les enjeux et les besoins de sécurité des autorités administratives<br>• Élaborer une politique de sécurité<br>• Utiliser des produits et prestataires labellisés SSI<br>• Viser une amélioration continue<br><br>Le RGS est donc dans une logique ISO 27001, mais restreint à un type particulier de système. L'ISO 27001 est un système de management de la sécurité qui s'applique à tout système. |



Laboratoire national de métrologie et d'essais - 1, rue Gaston Boissier - 75724 Paris cedex 15 – France
Tél. +33 (1) 40 43 37 00 - Fax +33 (1) 40 43 37 37 - info@lne.fr - www.lne.fr

| | |
|---|---|
| **Q** | Ou pourrons-nous accéder aux différents guides de la famille ISO 27000? |

| | |
|---|---|
| **R** | Sur le site de l'AFNOR ou de l'ISO.<br>Pour information l'ISO 27000 « Vue d'ensemble et vocabulaire » est gratuite, contrairement à toutes les autres. |

| | |
|---|---|
| **Q** | Que peut apporter l'ISO 27001 au niveau de la protection juridique, est-ce une assurance? |

| | |
|---|---|
| **R** | L'ISO 27001 n'est pas une assurance. Elle garantit juste que pour un système donné, des mesures de sécurité adéquates ont été mises en œuvre pour traiter les risques identifiés jusqu'à un niveau acceptable.<br>Si l'ISO 27001 n'apporte aucune garantie juridique ou assurantielle, cela démontre par contre une volonté de mise en œuvre de la sécurité, ce qui peut permettre de baisser une assurance, ou en cas de fuite de données à caractère personnelles de justifier que des moyens adéquats ont été mis en œuvre. |

| | |
|---|---|
| **Q** | Est-ce que l'ISO 27001 s'intègre dans un système QSE ISO 9001? |

| | |
|---|---|
| **R** | L'ISO 27001 s'intègre parfaitement dans un SMQ ISO 9001. Les normes sont conçues sur le même socle concernant le Système de Management. Seules les spécificités changent. De plus, comme présentée dans le Webinar, la sécurité doit s'intégrer dans tous les processus de l'entreprise et ne pas être une surcouche. Il est donc primordial d'intégrer le SMSI dans le SMQ. |

| | |
|---|---|
| **Q** | Combien de temps est- il nécessaire pour mettre en place l'ISO 27001 ? (En moyenne) |

| | |
|---|---|
| **R** | Le temps de mise en œuvre d'un SMSI dépend de la taille du système et du niveau de sécurité initiale. Un projet de certification d'une durée de l'ordre de 12-18 mois est généralement constaté. |



Laboratoire national de métrologie et d'essais - 1, rue Gaston Boissier - 75724 Paris cedex 15 – France
Tél. +33 (1) 40 43 37 00 - Fax +33 (1) 40 43 37 37 - info@lne.fr - www.lne.fr

# CONTACT

**Service clients**
1, rue Gaston Boissier
75724 Paris Cedex 15
+(33) 1 40 43 38 13
info@lne.fr

www.lne.fr