Pourquoi choisir le LNE
comme organisme de certification ?

Le LNE délivre des certificats de système de management depuis de nombreuses années et dispose d'**auditeurs qualifiés et expérimentés dans toutes les industries :** emballage, médical, transport, construction ...

Accrédité par le COFRAC pour la certification ISO 27001, nos activités sont donc évaluées de manière indépendante, ce qui permet d'établir la conformité de nos prestations de certification par rapport à des exigences spécifiées. Le LNE est notifié pour plus de 20 directives européennes.

Le LNE, retenu par l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) en tant qu'organisme d'évaluation pour les référentiels PRIS, PDIS et SECURE CLOUD, en procédure expérimentale :

- délivre sur un large panel de certification (ISO 9001, ISO 14001, OHSAS 18001 etc.),
- travaille avec de grosses structures organisationnelles aussi bien que des PME, PMI,
- propose un accompagnement individualisé dans le processus de certification par un chef de projet certification.

Pour vous accompagner, nous vous proposons **différents outils d'aide à la mise en place de votre système de management :**

- webinar,
- journées d'information technique,
- guides pratiques,
- formation inter/intra,
- accompagnement technique.

LNE

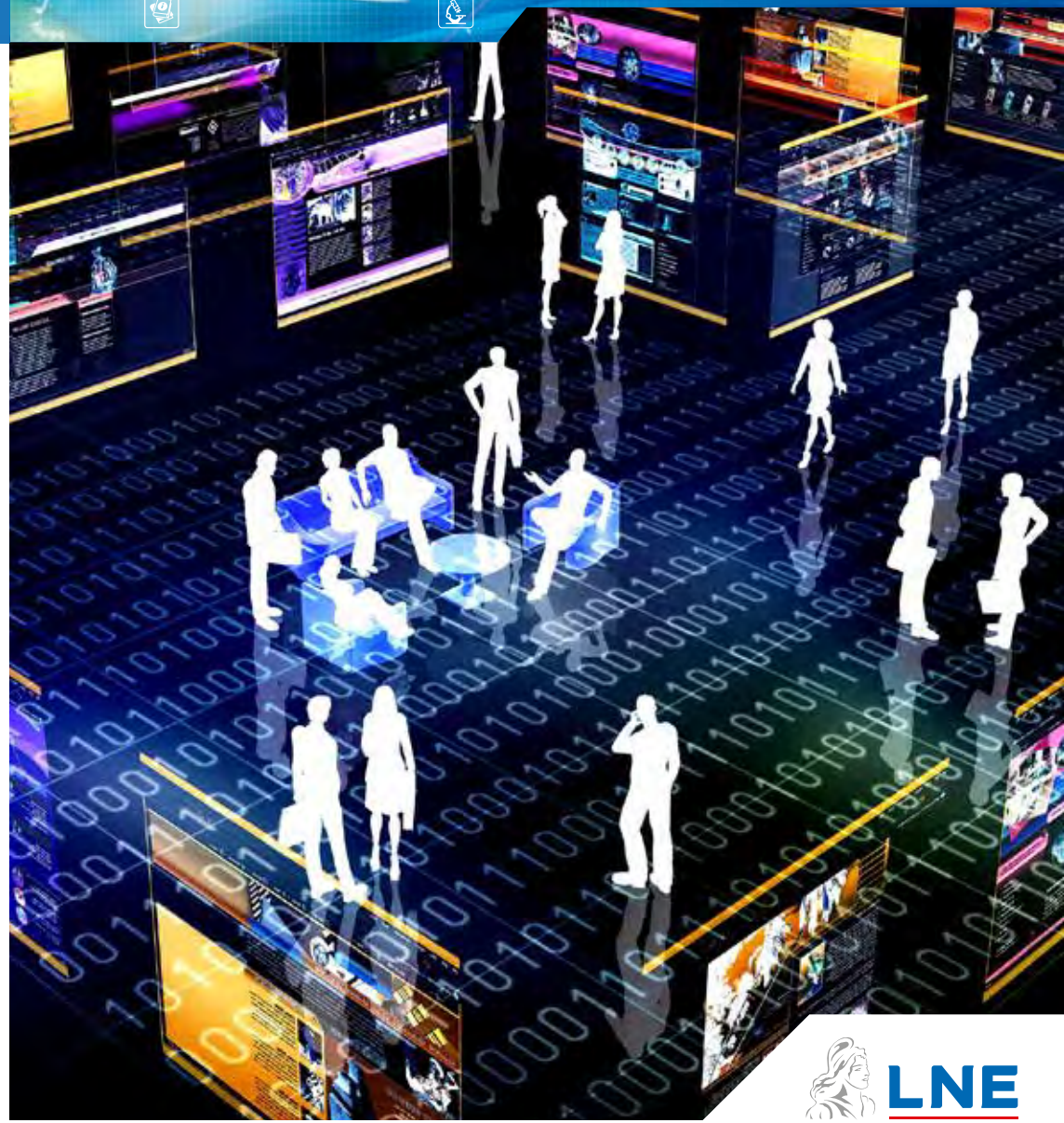
Contact Sécurité de l'Information

LABORATOIRE NATIONAL DE MÉTROLOGIE ET D'ESSAIS
1, rue Gaston Boissier • 75724 Paris Cedex 15
Tél. : 01 40 43 37 00 • E-mail : info@lne.fr
Site Internet : www.lne.fr

Réalisation : Esquif Communication - Crédits photos Istockphoto, Fotolia, X. 11/16

MAÎTRISER LA SÉCURITÉ DE L'INFORMATION

Norme ISO 27001, référentiels ANSSI



LNE

La sécurité de l'information est l'ensemble des mesures adoptées pour empêcher l'utilisation non autorisée, le mauvais usage, la modification ou le refus d'utilisation d'un ensemble de connaissances, de faits, de données ou de moyens. Dans une économie mondialisée et dématérialisée, la sécurité de l'information devient un atout stratégique.

VOS ENJEUX

SÉCURISER vos données et vos échanges

ANTICIPER les risques d'intrusion et de piratage

FIABILISER votre SI

ASSURER la continuité des services stratégiques pour l'économie nationale

Délivrance de **la certification ISO 27001**

Toute entreprise est concernée par la sécurité de son information ou peut être sollicitée sur ce sujet par ses partenaires économiques. **La norme ISO 27001 est un standard international** de la gestion des systèmes d'information s'appuyant sur **la gestion des risques** pour définir une politique, des procédures et des mesures de sécurité appropriées pour gérer ces risques.

La norme ISO 27001 :

- adopte et promeut les bonnes pratiques à tous les niveaux de l'entreprise (méthodologie, outils et processus) ;
- permet une meilleure appréhension des risques de cyber sécurité grâce à l'identification des menaces ;
- est un gage de qualité et de sécurité pour les partenaires économiques (actionnaires, clients, fournisseurs, Etat, assurances, utilisateurs...) ;
- satisfait aux exigences légales, réglementaires et contractuelles ;
- est source de sécurisation et traçabilité ;
- garantit une amélioration continue du SI dans la durée.

Les acteurs de votre information sécurisée

Évaluation des prestations dans le cadre de la qualification ANSSI

Prestataire de Détection des Incidents de Sécurité **(PDIS)**

Ce référentiel démontre la confiance que le commanditaire peut accorder au prestataire de détection d'incidents de sécurité en garantissant la qualité de sa prestation, notamment **en matière de confidentialité, ainsi que les compétences du prestataire et de son personnel.**
Une meilleure détection des incidents de sécurité participe :

- à la prévention de ces incidents,
- à la limitation de l'ampleur de leurs conséquences.

Prestataire de Réponse aux Incidents de Sécurité **(PRIS)**

Ce référentiel démontre la confiance que le commanditaire peut accorder au prestataire de réponse aux incidents de sécurité en garantissant la qualité de ses activités de réponse aux incidents par sa capacité à **adopter une approche globale de l'incident de sécurité et une démarche d'analyse adaptée**, ainsi que les compétences du prestataire et de son personnel. Cette méthodologie structurée de réponse aux incidents permet :

- de qualifier l'étendue de la compromission,
- de préconiser les mesures de remédiation.

Prestataires de services d'informatique en nuage **(Secure Cloud)**

Ce référentiel démontre la confiance que le commanditaire peut accorder au prestataire de *cloud computing* sur la qualité des services fournis **avant de lui confier des données,** ainsi que sur ces compétences. Ce référentiel permet :

- la mise en œuvre d'un cadre de reference pour l'utilisation sécurisée des solutions *Cloud*,
- l'émergence d'offres qualifiées afin de traiter la sécurité de manière globale et efficace.