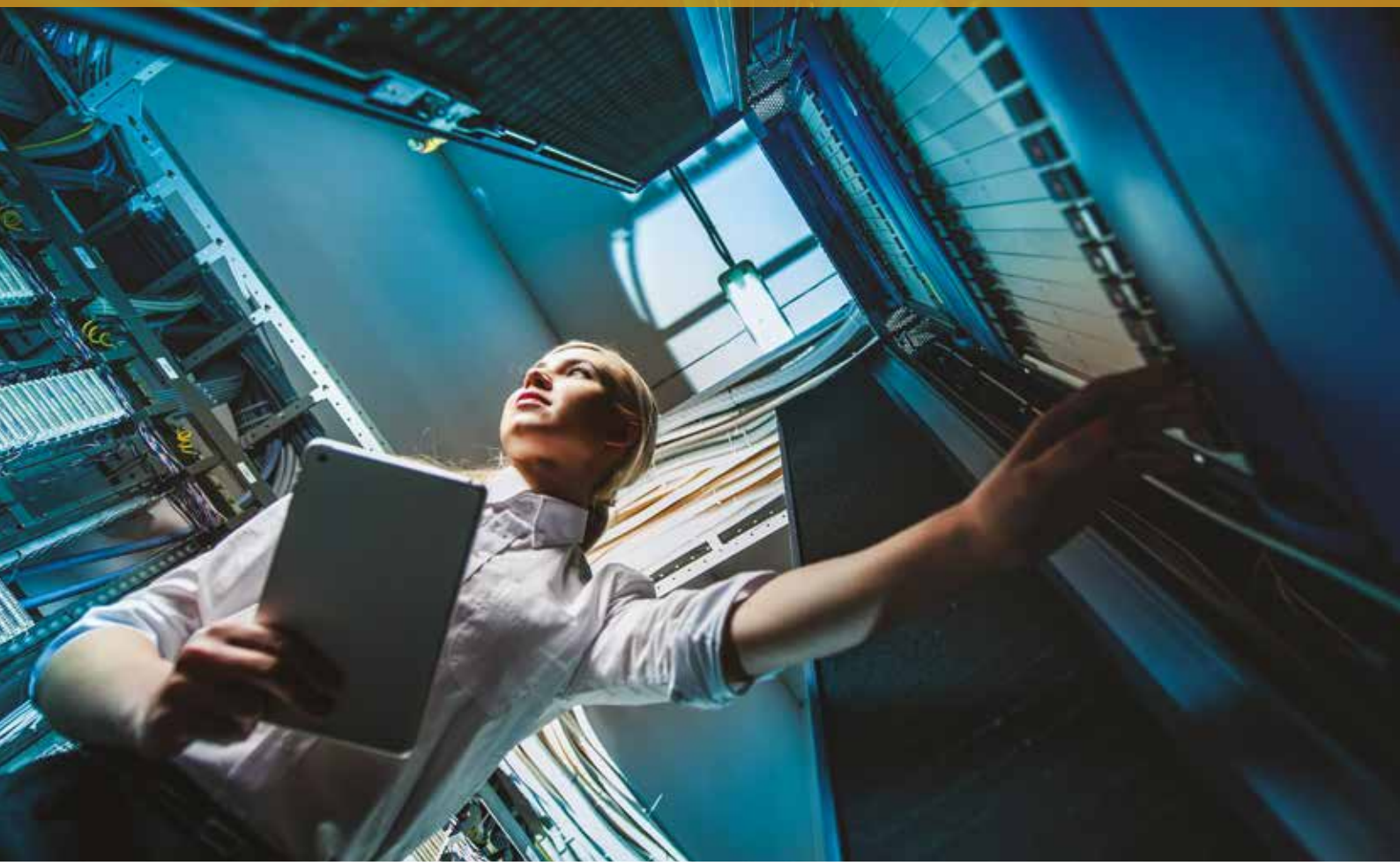
Lloyd's Register
LRQA

Améliorer la performance,
réduire le risque

Sécurité des informations

Protégez votre organisation contre les coûteuses cyber-attaques

Conformité réglementaire · Évaluation et certification des systèmes de management · Formation et diagnostic sur mesure



La cyber-sécurité est plus que jamais à l'ordre du jour des conseils d'administration.

Tandis que près de 50 % des organisations ont fait face à un examen public suite à une violation de sécurité en 2016[1], les entreprises reconnaissent que leur exposition potentielle aux cyber-menaces fait apparaître la nécessité d'un cadre de cyber-sécurité solide basé sur des processus efficaces.

[1] Source : Cisco 2017 Security Capabilities Benchmark Study

Il ne s'agit pas de savoir « **si** », mais « **quand** »

Si les organisations sont soumises à des réglementations comme le Règlement général sur la protection des données (RGPD) de l'Union européenne (UE), alors la conformité aux lois et meilleures pratiques en matière de sécurité des informations est un prérequis pour exercer leurs activités.

Les cyber-risques ne se limitent plus à notre vision traditionnelle des ordinateurs et incluent désormais les smartphones, les tablettes et l'Internet des objets, notamment les véhicules et les appareils ménagers, ce qui élargit la portée des pirates à un territoire inexploré pour la plupart des organisations.

Par conséquent, un manque d'investissement dans la prévention, la détection et la formation est dommageable pour les organisations, quels que soient leur taille, leur secteur et leur position géographique. En effet, 50 % de l'ensemble des cyber-attaques visent des petites entreprises, précisément parce qu'elles sont considérées comme étant généralement moins bien protégées.

Une violation de sécurité des informations peut s'avérer extrêmement coûteuse et avoir des conséquences désastreuses sur la réputation d'une organisation. Cependant, malgré l'importance de la sécurité des informations, seulement 37 % des organisations possèdent un plan de réponse aux cyber-incidents[2].

Les mesures de cyber-sécurité ne sont plus une option ; elles sont indispensables au bon fonctionnement des entreprises.

Les petites entreprises sont un gros marché pour les pirates informatiques

50 % de l'ensemble des cyber-attaques visent des petites entreprises. Les pirates informatiques se basent sur l'idée répandue selon laquelle les petites entreprises ne possèdent pas le même niveau de cyber-défense que les grandes organisations.

[2] Source : PwC Global Economic Crime Survey 2016

Améliorez la cyber-résilience de votre organisation

Grâce à l'ampleur des spécialisations de LRQA, combinée à l'expérience de nos partenaires technologiques, nous pouvons vous soutenir et vous guider pour que votre organisation soit en mesure non seulement de réagir aux cyber-attaques, mais aussi de les maintenir à distance avec nos services.

« Lorsque nous avons décidé de nous soumettre à la certification ISO 27001, notre but n'était pas uniquement de valider la certification. Nous voulions renforcer notre entreprise en pleine croissance et ses activités, pour offrir les niveaux de résilience, d'assurance et de confiance que les clients utilisant nos services attendaient. »

John Hall
PDG de MyLife Digital

Cyber-sécurité et sécurité du cloud

LRQA peut fournir à votre organisation l'approche adéquate en matière de gestion des risques et le cadre de sécurité des informations approprié pour prendre en charge les infrastructures, les données et les applications professionnelles face à de nouvelles menaces en perpétuelle évolution provenant de l'utilisation de services dans le cloud et les plates-formes informatiques mobiles.

En ligne de mire

De nombreuses cyber-attaques et intrusions ne sont pas détectées immédiatement. Certaines sont ainsi identifiées des mois, voire des années, plus tard[3]. Avec l'entrée en vigueur du RGPD de l'UE à compter de mai 2018, les organisations devront signaler auprès de l'autorité de contrôle compétente les violations de sécurité dans les 72 heures suivant leur détection. L'éventail des services de sécurité des informations de LRQA peut apporter de la visibilité quant aux événements de sécurité dans votre organisation, pour vous permettre de garder une longueur d'avance sur les cyber-menaces et de réagir rapidement en cas d'incident.

Des défenses plus solides

Les pirates volent des informations car ces dernières sont précieuses. Il est donc essentiel de sécuriser les données et éléments de propriété intellectuelle de votre organisation. LRQA propose des services d'évaluation, de certification, de formation et d'amélioration opérationnelle, qui contribuent non seulement à renforcer votre capacité à empêcher les cyber-attaques et à réagir si elles surviennent, mais aussi à limiter les risques de sécurité associés à un manque de cyber-sensibilisation et de cyber-hygiène chez les employés. Nous pouvons également vous aider à développer un plan de continuité efficace pour les activités de votre organisation afin de réduire l'impact d'éventuelles violations de sécurité.

[3] Source : World Economic Forum Global Risks Report 2016

LRQA, votre partenaire de confiance pour la protection de votre organisation contre les cyber-menaces

ISO 27001

La norme internationale en matière de systèmes de management de la sécurité de l'information (SMSI) ISO 27001 (Technologies de l'information – Techniques de sécurité – Systèmes de management de la sécurité de l'information – Exigences) fournit aux organisations un modèle de meilleures pratiques permettant d'identifier, d'évaluer et de mettre en œuvre des contrôles pour gérer les risques de sécurité de l'information et protéger l'intégrité des données stratégiques des entreprises.

La certification ISO 27001 présente notamment les avantages suivants :

- Seule norme internationale définissant les exigences d'un SMSI et pouvant faire l'objet d'un audit, pour une conformité garantie aux obligations juridiques, contractuelles et réglementaires
- Flexibilité permettant d'intégrer la norme ISO 27001 dans d'autres grands systèmes de management comme ISO 9001 et ISO 14001, étant donné que la dernière version de la norme est alignée sur la structure générale de l'Annexe SL
- Mise en place d'un cadre de management pour toutes les organisations, quels que soient leur taille, leur secteur et leur localisation, comme point de départ pour gérer les cyber-risques
- Acquisition d'un avantage concurrentiel et amélioration de la capacité de votre organisation à remporter de nouveaux contrats et à conserver ses clients existants
- Réduction des coûts associés à la planification d'audits clients répétés et protection contre les pertes financières liées aux violations de données
- Amélioration de la cyber-sensibilisation dans toute l'organisation, pas seulement le service informatique, grâce à une définition claire des cyber-risques dans le travail quotidien des employés

« Nous avons toujours utilisé des centres de données conformes Cyber Essentials et ISO 27001 pour héberger notre plate-forme, et nous nous sommes conformés à des procédures internes exigeant des niveaux élevés de sécurité des informations. Cette accréditation renforce encore notre position de partenaire de confiance. »

David Cocks
PDG de CloudTrade

RGPD de l'UE

Le Règlement général sur la protection des données (RGPD) de l'UE est une nouvelle réglementation qui entrera en vigueur en mai 2018. Ce règlement renforce la confidentialité des données pour les individus, établit des lois plus strictes quant à la manière dont les entreprises utilisent les données personnelles et impose des amendes plus lourdes aux organisations exposées à des violations. Les organisations implantées hors de l'Union européenne qui ont des activités dans l'Union européenne avec les données personnelles de citoyens de l'Union européenne doivent se préparer à se conformer à ce règlement. Les organisations fournissant des produits ou des services à des clients de l'Union européenne ou traitant leurs données s'exposent à des conséquences juridiques si un incident est signalé.

ISO 37001

La norme ISO 37001:2016 (Systèmes de management anti-corruption – Exigences et recommandations de mise en œuvre) a récemment été publiée par l'Organisation internationale de normalisation (ISO) pour aider les organisations à lutter contre la corruption et à promouvoir une culture commerciale éthique.

ISO/IEC 20000-1

La norme ISO/IEC 20000-1:2011 (Technologies de l'information – Gestion des services – Partie 1 : Exigences du système de management des services) est une norme relative aux systèmes de management des services (SMS) qui spécifie les exigences pour le fournisseur de services dans le cadre de la planification, de la mise en place, du déploiement, de l'exploitation, de la surveillance, de la révision, de la mise à jour et de l'amélioration d'un SMS. Les exigences incluent la conception, la transition, la distribution et l'amélioration de services pour répondre aux exigences de service convenues.

ISO 22301

La norme ISO 22301:2012 (Sécurité sociétale – Systèmes de management de la continuité d'activité – Exigences) est la norme internationale concernant la continuité de l'activité. Elle spécifie les exigences dans le cadre de la planification, de la mise en place, du déploiement, de l'exploitation, de la surveillance, de la révision, de la mise à jour et de l'amélioration continue d'un système de management documenté pour se protéger contre des incidents perturbateurs, réduire leur probabilité, se préparer et réagir à de tels incidents, et rétablir un fonctionnement normal après ces événements.

ISO/IEC 27032:2012*

La norme ISO/IEC 27032:2012 (Technologies de l'information – Techniques de sécurité – Lignes directrices pour la cyber-sécurité) fournit des recomtmandations pour améliorer l'état de la cyber-sécurité, en tenant compte des aspects uniques de cette activité et de ses relations de dépendance avec d'autres domaines de sécurité, comme la sécurité des informations, la sécurité des réseaux, la sécurité Internet et la protection des infrastructures d'information critiques.

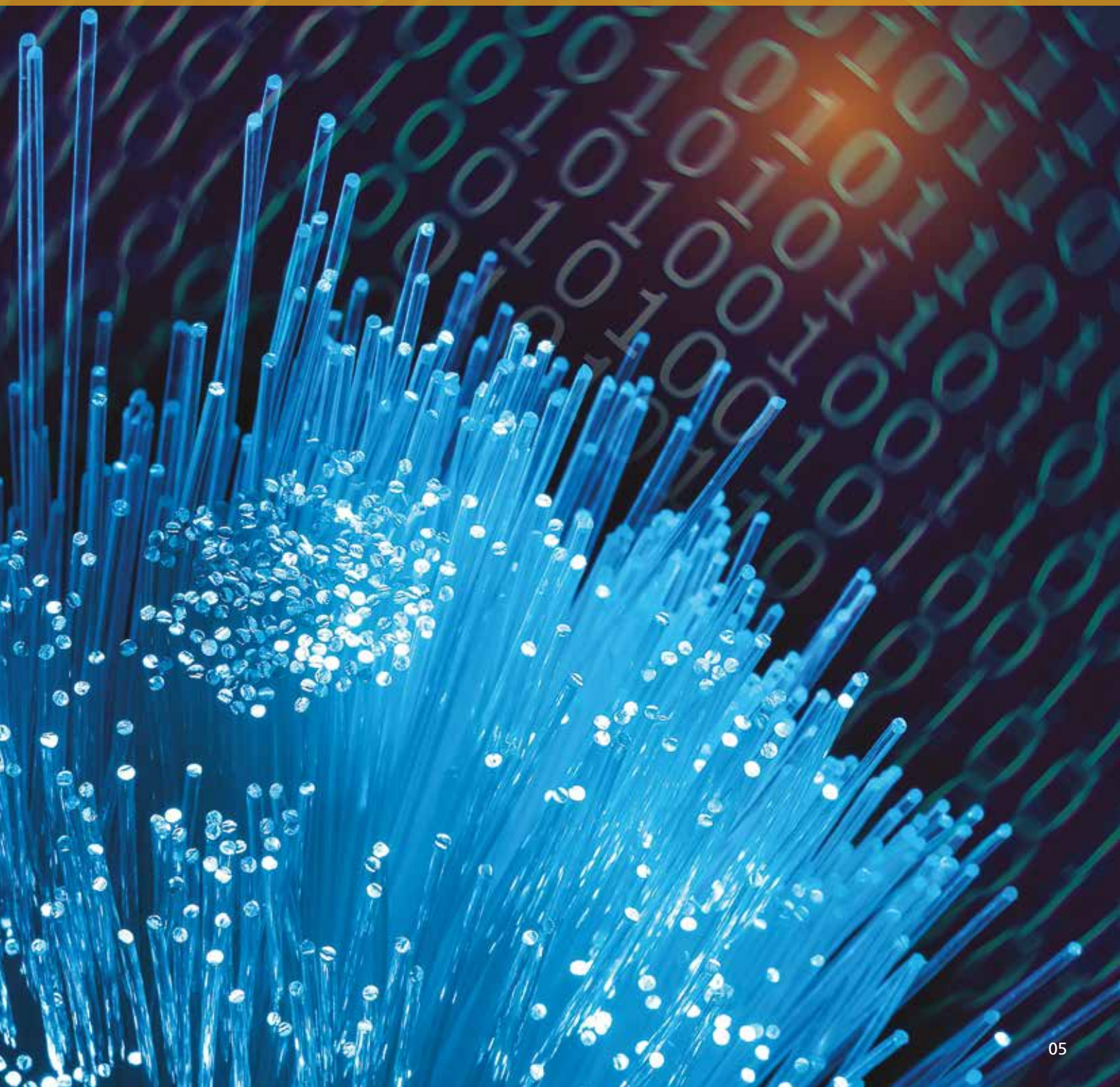
ISO/IEC 27017:2015*

La norme ISO/IEC 27017:2015 (Technologies de l'information – Techniques de sécurité – Code de pratique pour les contrôles de sécurité de l'information fondés sur l'ISO/IEC 27002 pour les services du nuage) fournit des recommandations pour les contrôles de sécurité de l'information applicables à la prestation et à l'utilisation de services cloud en proposant des conseils de mise en œuvre supplémentaires pour les contrôles pertinents spécifiés dans ISO/IEC 27002 et des contrôles supplémentaires avec des conseils de mise en œuvre qui se rapportent spécifiquement aux services cloud.

ISO/IEC 27018:2014*

La norme ISO/IEC 27018:2014 (Technologies de l'information – Techniques de sécurité – Code de bonnes pratiques pour la protection des informations personnelles identifiables (PII) dans l'informatique en nuage public agissant comme processeur de PII) spécifie les recommandations basées sur ISO/IEC 27002, en tenant compte des exigences réglementaires pour la protection des PII susceptibles de s'appliquer dans le contexte des environnements de risques de sécurité de l'information d'un fournisseur de services de cloud public.

*LRQA sera en mesure de fournir des services de certification accréditée pour ces normes d'ici fin 2017.



Notre expertise

Les informations sont parmi les ressources les plus précieuses et les plus stratégiques de n'importe quelle organisation. Dans le monde hyperconnecté qui est le nôtre aujourd'hui, les organisations sont exposées à des menaces de sécurité à grande échelle pour leurs informations et à des cyber-attaques destructrices, et ce quels que soient la taille, le secteur et la localisation des entreprises.

Si les systèmes de sécurité de l'information ne sont pas correctement gérés et mis à jour, les organisations courent le risque de subir de lourdes pertes financières et d'importantes atteintes à leur réputation.

Vérifier que votre organisation a mis en place les contrôles adéquats pour réduire les risques sérieux pour les données et éviter que les failles du système ne soient exploitées n'est plus une simple option.

Ces précautions sont encore plus incontournables depuis la publication du Règlement général sur la protection des données de l'UE, qui impose des exigences plus strictes et des amendes et sanctions plus lourdes aux organisations en cas de violation de données.

La société LRQA est pionnière en matière d'élaboration de normes et s'est très tôt engagée dans les domaines de la certification et de l'évaluation des systèmes de management de la sécurité de l'information (SMSI).

De nombreux clients prestigieux dans des secteurs aussi divers que la finance, les télécommunications, l'édition de logiciels, la navigation sur Internet, le conseil, la justice et l'administration font confiance à LRQA pour leur fournir des évaluations de grande qualité, cohérentes et impartiales, assorties de services exhaustifs d'assistance spécialisée.

Nos évaluateurs regroupent des experts en systèmes de management, spécialisés en sécurité de l'information et dans d'autres aspects de l'informatique, dont la vision objective renforcera votre confiance dans vos propres mesures de sécurité estimées à l'aune des meilleures pratiques en vigueur dans le secteur.

La méthodologie d'évaluation unique de LRQA vous aide à gérer vos systèmes et vos risques afin d'améliorer et de protéger les performances actuelles et futures de votre entreprise.

À propos de LRQA

LRQA est une société reconnue comme étant le leader mondial des services de certification professionnelle. Nous sommes spécialisés dans la conformité des systèmes de management, ainsi que dans les avis d'experts pour un large éventail de normes, référentiels et services d'amélioration opérationnelle, incluant des programmes de formation et d'assurance sur mesure. Nous sommes reconnus par près de 50 organismes d'accréditation et nos clients sont répartis dans plus de 120 pays.

Notre méthodologie d'évaluation unique permet de faire passer vos systèmes de management de la conformité à la performance. Ainsi, nous réduisons le risque pour votre entreprise tout en favorisant l'efficacité, l'efficience et l'amélioration continue de vos systèmes de management.

LRQA est membre du groupe Lloyd's Register, lui-même détenu par une organisation caritative. Contrairement à la plupart des entreprises, qui agissent pour faire du profit, au sein de Lloyd's Register nous faisons du profit pour agir. Une part de nos bénéfices étant reversés à la LR Foundation, chaque fois que vous choisissez LRQA, non seulement vous bénéficiez des meilleurs services de certification professionnelle, mais vous contribuez aussi à faire une différence dans le monde.

Avec sa large gamme de formations et de services d'évaluation, LRQA facilite pour les organisations du monde entier la transition vers les normes ISO nouvelles et révisées.
Nous proposons une gamme de services d'audit, ainsi que des formations publiques et en interne, afin de veiller à ce que les organisations du monde entier migrent en douceur vers les nouvelles normes.

Nos services d'évaluation et de formation en matière de sécurité de l'information

Nous proposons une gamme de services d'évaluation en ligne et en face à face adaptés aux organisations, quelles que soient leur taille et leur localisation, et nous pouvons vous aider à tirer le meilleur parti des normes.

Formation

Les packs et services de formation sur mesure de LRQA peuvent aider n'importe quelle organisation à répondre à ses besoins professionnels spécifiques.

Notre gamme de cours de formation inclut notamment les cours suivants :

- **Présentation de la norme ISO 27001:2013**
- **Mise en œuvre de la norme ISO 27001:2013**
- **Auditeur interne et auditeur en chef ISO 27001:2013**
- **Présentation du RGPD de l'UE (en face à face, en interne ou via l'apprentissage électronique)**

Gap Analysis

Nos audits nous offrent l'occasion de faire ressortir les zones de faiblesse ou à risque de votre organisation afin de mettre au point un système certifiable. Elle peut également examiner les systèmes ou les processus de management existants et leur utilisation au sein de la norme sélectionnée.

Que l'installation de votre système de management n'en soit qu'à ses débuts ou que vous procédiez à une « répétition » avant l'évaluation proprement dite, vous pouvez décider du périmètre de « l'analyse des écarts » en accord avec votre responsable du développement ou avec l'évaluateur seul, de façon à bénéficier d'une plus grande souplesse au moment de déterminer le champ d'application et la durée du processus.
Nous proposons des audits :
ISO 31000, Business continuity, Audit de vulnérabilité, Penetration Test, Risk Management, ISA/IEC 62443

Certification

Généralement, ce processus comprend deux étapes, une appréciation du système et une évaluation initiale, dont la durée dépend de la taille et de la nature de votre entreprise.

Votre responsable du développement des activités concevra une solution capable de répondre à vos besoins spécifiques tandis que nos évaluateurs, ouverts à toutes les options, vous assisteront et adopteront une approche pratique. Il s'agit là d'une des nombreuses manières d'enrichir réellement le processus d'évaluation.

Surveillance

Une fois votre SMSI approuvé, nous effectuons régulièrement des visites de surveillance afin de vérifier l'efficacité de la solution. Vous avez ainsi l'assurance, ainsi que vos dirigeants, que les systèmes de management restent opérationnels et continuent de s'améliorer.

Audit RGPD

Nous proposons des analyses d'impact relatives à la protection des données pour les organisations souhaitant se mettre en conformité avec les nouvelles exigences du RGPD de l'UE. Les entreprises désireuses de combiner leur système de management avec un système existant (gestion de la qualité, par exemple) peuvent également profiter d'un programme coordonné d'évaluation et de surveillance. Ce service est en constant développement.

Pour découvrir comment LRQA peut vous aider dans le cadre de la conformité aux exigences liées à la **sécurité des informations**, rendez-vous sur **www.lrqa.fr,** envoyez un message à l'adresse **lrqa-lyon@lrqa.com** ou appelez le **04 72 13 31 41**.

LLOYD'S REGISTER QUALITY ASSURANCE FRANCE S.A.S.
Tour Swiss Life - 1, bd Vivier Merle
69443 LYON Cedex 03
Tél. : 04 72 13 31 41

France

E-mail : lrqa-lyon@lrqa.com

Suivez-nous
sur les réseaux
sociaux :

www.lrqa.com

Lloyd's Register et LRQA sont des marques commerciales du Groupe d'entités Lloyd's Register.
Les services sont fournis par des membres du Groupe Lloyd's Register.
Pour en savoir plus, rendez-vous sur www.lr.org.

Lloyd's Register Quality Assurance est un membre du Groupe Lloyd's Register.
Siège social : 71 Fenchurch Street, Londres EC3M 4BS, Royaume-Uni
Numéro d'inscription au registre : 1879370

Nous veillons à ce que toutes les informations fournies soient exactes et à jour. Toutefois, Lloyd's Register LRQA décline toute responsabilité en cas d'inexactitude ou de modification des informations. Lloyd's Register et ses variantes sont des marques commerciales de Lloyd's Register Group Limited et de ses filiales et sociétés affiliées. Copyright © Lloyd's Register Quality Assurance Limited, 2017. LRQA est membre du groupe Lloyd's Register.