SEQUAL
by MEANQUEST

AUDIT - PROTECTION DES DONNÉES ET SÉCURITÉ DE L'INFORMATION

OÙ EN ÊTES-VOUS AVEC VOTRE CONFORMITÉ LPD ?

IDENTIFIEZ VOS LACUNES ET GAGNEZ EN SÉRÉNITÉ

La LPD a été créée pour **protéger la vie privée des individus et règlementer la manière dont les entreprises gèrent les données personnelles.** Afin de savoir si votre entreprise est conforme aux règlementations, voici une liste de questions à se poser :

- Est-ce que vous appliquez toutes les bonnes pratiques en matière de sécurité de l'information ?
- Est-ce que ces pratiques sont documentées et bien communiquées ?
- Votre plan de réponse aux incidents est-il à jour ?
- Avez-vous prévu tous les cas de figure, tels que les sauvegardes de données ou la protection des postes de travail et des serveurs ?

L'audit est un examen approfondi visant à **évaluer la conformité de votre organisation à la LPD et la sécurité de votre système d'information,** mettant en lumière d'éventuelles failles ou dysfonctionnements pouvant compromettre vos activités.

POURQUOI RÉALISER UN AUDIT ?

Établir un état des lieux de la **conformité de votre organisation à la LPD**

Évaluer votre niveau de **sécurité de l'information**

Identifier les potentielles vulnérabilités présentes au sein de votre entreprise

Soumettre des recommandations afin d'atteindre un niveau de risque acceptable

DOMAINES AUDITÉS

- **Gouvernance de la sécurité de l'information**
- **Système d'information**
- **Ressources humaines**

ÉTAPES DE NOTRE AUDIT DE SÉCURITÉ

A. ANALYSE ET COMPRÉHENSION DU CONTEXTE DE VOTRE ORGANISATION

- Identification de vos attentes et besoins au travers d'interview de la Direction
- Entretiens avec les responsables de vos infrastructures IT et RH

B. ÉTAT DES LIEUX ET ANALYSE

- Analyse du niveau de conformité et de maturité de la gouvernance de la sécurité de l'information (rôles et responsabilités, plan de continuité et de reprise des activités, etc.)
- Analyse du niveau d'exposition cyber lié à vos systèmes d'information (gestion du parc informatique, vulnérabilités, accès, logiciels malveillants, etc.)
- Analyse du niveau de conformité de la gestion des RH ainsi que de l'exposition cyber liée au risque humain (recrutement, formations & sensibilisations, fin de la collaboration)

C. RAPPORT D'AUDIT ET RECOMMANDATIONS

- Rapport comprenant une analyse des risques et des recommandations de traitement des risques identifiés
- Séance de présentation du projet de rapport d'audit
- Transmission d'un rapport final par le biais d'une plateforme sécurisée

CONFIDENTIALITÉ

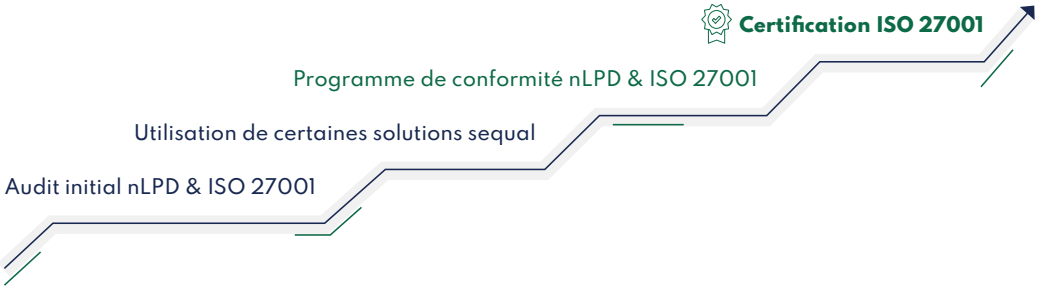
Les auditeurs s'engagent à traiter de manière confidentielle, et à garder le secret sur toutes les données, accès, informations et documents concernant l'Entreprise.

INFORMATIONS COMPLÉMENTAIRES

- Exclusion des modèles de document
- Possibilité de correction d'éventuelles failles de sécurité détectées (voir offre de services)
- Le nombre d'heures allouées aux tests définira l'exhaustivité des recherches effectuées

UNE OFFRE ÉVOLUTIVE :

JUSQU'OÙ SOUHAITERIEZ-VOUS ALLER ?



Cet audit est qualifié d'audit initial/gap analysis ou encore d'audit interne. À la suite de celui-ci, nos équipes seront en mesure de vous accompagner pour la suite du processus en vue de l'obtention de la certification ISO 27001.

NOS POINTS FORTS ?

La protection des données et la sécurité de l'information sont notre cœur de métier

Nous sommes nous-mêmes une organisation certifiée ISO 27001

Nos experts certifiés bénéficient d'une expérience de terrain au sein d'entités de différentes tailles et natures

Notre équipe vous accompagne tout au long de votre processus de sécurisation des données pour vous permettre d'atteindre vos objectifs de conformité et de sécurité.

Vous souhaitez en savoir plus sur notre offre ?
Contactez-nous par mail : ventes@meanquest.ch
ou au +41 58 810 00 00

meanquest.ch/sequal/audit