BDO ADVISORY | RISK ADVISORY | THIRD PARTY ASSURANCE

CONFORMITÉ EN MATIÈRE DE CYBERSÉCURITÉ

ALORS QUE LES MENACES AUGMENTENT EN NOMBRE ET EN COMPLEXITÉ, VOTRE ORGANISATION MET-ELLE TOUT EN ŒUVRE POUR SE PROTÉGER ET POUR RASSURER VOS PARTENAIRES ET CLIENTS SUR VOTRE GESTION DE LA CYBERSÉCURITÉ ?

LES RISQUES DE CYBERSÉCURITÉ EN TÊTE DES PRIORITÉS DES ENTREPRISES EN 2022

Les menaces se multiplient dans le monde entier. Elles deviennent de plus en plus complexes et touchent des organisations de toutes tailles et de tous secteurs. Un problème de cybersécurité peut donner lieu à des pertes financières, des perturbations opérationnelles, des conséquences juridiques et à une atteinte à la réputation de l'entreprise. Pourtant, de nombreuses organisations indiquent qu'elles ne sont pas préparées à ces risques. Environ 20% des dirigeants d'entreprises interrogés dans le cadre de notre **Global Risk Landscape 2021** ont indiqué que la cybercriminalité est le domaine de risque dans lequel ils sont le moins préparés. Les chiffres sont encore plus inquiétants pour les entreprises du marché intermédiaire : selon la **Middle Market Digital Transformation Survey** effectuée par BDO en 2021, près de la moitié des dirigeants d'entreprises estiment que les risques liés à la cybersécurité et à la confidentialité des données constituent leur principal défi en matière de résilience informatique, et 34% d'entre eux affirment que les cyberattaques et les atteintes à la vie privée constituent leurs principales menaces numériques.

DANS QUELLE MESURE VOTRE ORGANISATION – ET VOS FOURNISSEURS – SONT-ILS PRÉPARÉS AUX PROBLÈMES CYBERNÉTIQUES ?

Partout dans le monde, le risque de cybersécurité est une préoccupation pour les dirigeants d'entreprises et les conseils d'administration. Ce risque doit être géré non seulement si l'infrastructure informatique est *gérée* par une entreprise elle-même, mais aussi lorsque l'infrastructure et les services informatiques sont *externalisés* – ce qui est de plus en plus courant aujourd'hui.

L'externalisation (partielle) de l'informatique - ou de toute autre fonction essentielle de l'entreprise, d'ailleurs - comporte une couche supplémentaire de risques. Même lorsque l'informatique ou d'autres services sont externalisés, ce sont toujours les données commerciales de votre entreprise et votre réputation qui sont en jeu si votre fournisseur est victime d'une violation de données ou ne fournit pas le service attendu. Si vous êtes vous-même une organisation de service ou un fournisseur, inutile de vous dire qu'il est essentiel que vous soyez en mesure de fournir une transparence sur les (cyber)contrôles en place au sein de votre organisation pour rassurer vos clients.

> VOUS POUVEZ EXTERNALISER LES PROCESSUS ET L'INFRASTRUCTURE DE VOTRE ORGANISATION, MAIS VOUS NE POUVEZ PAS EXTERNALISER LE RISQUE.

DÉMONSTRATION DE LA CONFORMITÉ EN MATIÈRE DE CYBERSÉCURITÉ

Il existe un certain nombre d'options qui permettent à votre organisation de créer (en tant que prestataire de services ou vendeur) ou d'obtenir (en tant que client) une plus grande confiance et transparence en matière de cybersécurité dans votre chaîne d'approvisionnement. Voici deux des normes les plus fréquemment appliquées :

- la norme **ISO/IEC 27001:2013** – Gestion de la sécurité de l'information et la norme ISO/IEC 27002:2022 récemment révisée ; et
- la norme **SOC 2** – Rapport sur les contrôles au sein d'une organisation de service concernant la sécurité, la disponibilité, l'intégrité du traitement, la confidentialité ou la vie privée.

Bien qu'il existe des différences entre les deux normes au niveau de l'approche, elles ont des objectifs similaires et peuvent se compléter pour vous aider dans votre démarche de mise en conformité.

FICHE D'INFORMATION

SOC 2

1. Rapport d'attestation fourni par un cabinet d'experts-comptables agréé
2. Sujets : 5 Critères potentiels de Services Fiduciaires et les points d'attention y liés
3. Focus sur les Organisations de Service et le service fourni
4. Principal livrable : rapport d'audit détaillé
5. Cadre flexible vous permettant de vous concentrer sur les Critères de Services Fiduciaires pertinents et les contrôles identifiés spécifiques à votre organisation
6. Renouvellement annuel de l'attestation

ISO27001

1. Certification fournie par un Organisme de Certification accrédité
2. Sujets : 7 clauses sur la définition et le maintien de votre SMSI (Système de Management de la Sécurité de l'Information) et l'Annexe A avec référence aux contrôles et à leurs objectifs
3. Toute organisation peut demander une attestation de la sorte et se concentrer sur l'ensemble ou une partie de l'organisation
4. Principaux livrables : SMSI détaillé et certificat
5. Cadre rigide détaillant la manière dont un SMSI doit être conçu et exploité. Tous les domaines de contrôle de l'Annexe A doivent être traités, sauf indication contraire dans votre déclaration d'applicabilité (Statement of Applicability - SoA)
6. Audit de surveillance annuel et audit de recertification triennal

COMMENT BDO PEUT VOUS AIDER

BDO croit en la complémentarité des deux normes, qui permettent aux prestataires de services et aux organisations de progresser à leur propre rythme dans leur processus de mise en conformité de la sécurité de l'information.

SOC 2 ATTESTATION

Partant des Critères de Services Fiduciaires, la norme SOC 2 vous permet de définir et de mettre en œuvre des contrôles (également connus sous le nom de « Description du Système ») qui sont pertinents pour votre organisation. L'évaluation de la Description du Système par BDO vous permet de démontrer votre conformité avec les principes clés de la sécurité de l'information et de répondre aux besoins d'assurance des parties prenantes internes et externes dans un délai relativement court.

ISO 27001 IMPLEMENTATION

La conception et la mise en œuvre d'un SMSI ISO 27001 nécessitent plus de temps et de ressources. Sur base des contrôles prévus dans le cadre de l'attestation SOC 2, nous pouvons aider votre organisation à tirer profit de cette expérience et à formaliser votre façon de travailler dans un ensemble de politiques et de procédures de sécurité de l'information détaillant la maintenance continue de votre programme de sécurité de l'information.

SOC 2+ ISO27001 ATTESTATION

Après avoir mis en œuvre les principes clés de la norme ISO 27001, votre rapport SOC 2 peut être transformé en un SOC 2+. Cela vous permettra d'établir un rapport sur le statut de votre programme ISO 27001 sans passer par une certification formelle par un organisme de certification.

ISO27001 CERTIFICATION

Comme dernière étape de votre processus de mise en conformité, nous pouvons vous aider à obtenir la certification ISO 27001 par l'intermédiaire de l'un de nos partenaires, un Organisme de Certification officiel.

Vous vous demandez comment vous pouvez améliorer l'approche de votre organisation en matière de cybersécurité ? N'hésitez pas à nous contacter.

CHRISTOPHE DAEMS
Senior Manager

E-mail : christophe.daems@bdo.be
Tel. : +32 474 90 78 51

FRANCIS OOSTVOGELS
Senior Manager

E-mail : francis.oostvogels@bdo.be
Tel. : +32 474 92 08 00

NICK HUYSMANS
Advisor

E-mail : nick.huysmans@bdo.be
Tel. : +32 486 31 90 45

▶ Follow us

▶ www.bdo.be

BDO Advisory BV/SRL, a company under Belgian law in the form of a cooperative company with limited liability, is a member of BDO International Limited, a UK company limited by guarantee, and forms part of the international BDO network of independent member firms. BDO is the brand name for the BDO network and for each of the BDO Member Firms.