ISO/IEC 27001:2013

Questionnaire d'auto-évaluation

Êtes-vous prêt ?

Ce document a été établi pour évaluer la disposition de votre entreprise à passer une évaluation de certification relative au système de management de la sécurité de l'information ISO/IEC 27001:2013. En renseignant ce questionnaire, vos résultats vous permettront d'auto-évaluer votre organisation et d'identifier où vous en êtes dans le processus en rapport avec les principales exigences de la norme.

Contexte de l'organisation

- Avez-vous déterminé les enjeux externes et internes propres à l'objectif de votre organisation et affectant votre capacité à atteindre les résultats escomptés de votre système de management de la sécurité de l'information (Information Security Management System - SMSI) ?
- Avez-vous un moyen de revoir et contrôler régulièrement les modifications apportées à ces enjeux ?
- Avez-vous déterminé les besoins et attentes des parties intéressées en ce qui a trait à votre SMSI et les revoyez-vous régulièrement ?
- Avez-vous pris en compte l'impact que les parties intéressées ou toute autre structure en lien avec votre organisation peuvent avoir sur votre SMSI ?
- Les enjeux internes et externes risquant d'avoir un impact sur l'SMSI ont-ils été pris en compte ?
- Êtes-vous au courant des exigences des parties intéressées, notamment dans les domaines réglementaires et statutaires ?
- Êtes-vous au courant des exigences de vos clients vis-à-vis de votre SMSI ?
- Les risques et opportunités associés à ces enjeux et exigences ont-ils été pris en compte ?
- Un processus d'amélioration continue a-t-il été envisagé ?

Leadership

- La direction s'est-elle porté garante du maintien du SMSI, et du fait de s'assurer de son efficacité ?
- La direction et a-t-elle communiqué sur l'importance du SMSI, et de la bonne application des procédures et des processus ?
- La politique et les objectifs du SMSI, lesquels sont compatibles avec le contexte et l'orientation stratégique de l'organisation ; ont-ils été établis et communiqués ?
- Les rôles au sein du SMSI ont-ils été clairement définis, couchés et communiqués ?
- La répartition des rôles et des responsabilités définies au sein du SMSI, permettent-ils de veiller à la conformité du système et à un reporting efficace ?

Suite >>

Leadership – *suite*

Un programme visant à garantir que votre SMSI atteint bien ses objectifs et remplit les exigences attendues, a-t-il été élaboré et mis en œuvre ?

Planification

Les risques et opportunités devant être traités pour veiller à ce que votre SMSI puisse atteindre son/ses résultat(s) escompté(s) ont-ils été établis ?

Un processus d'évaluation des risques relatifs à la sécurité de l'information a-t-il été établi pour inclure des critères d'acceptation des risques ?

Le processus d'évaluation des risques relatifs à la sécurité de l'information a-t-il été pensé pour être reproduit facilement et rapidement ?

Le processus d'évaluation des risques produit-il des résultats cohérents, valables et compatibles avec vos hypothèses ?

L'organisation a-t-elle planifié des actions pour traiter ces risques et opportunités ?

Le traitement des risques et opportunités est t'il pleinement intégré dans l'organisation ?

Le processus d'évaluation des risques relatifs à la sécurité de l'information suffit-il à identifier les risques associés à la perte de confidentialité, d'intégrité et de disponibilité des informations au sein du champ d'application du SMSI ?

Les responsables associés à la gestion des risques identifiés ont-ils été désignés ?

Les risques ont-ils été analysés pour évaluer une probabilité réaliste qu'ils surviennent et pour évaluer les conséquences potentielles qui en découleraient ?

Les différents niveaux de risques par nature des incidents potentiels, ont-ils été déterminés ?

Les risques réels observés relatifs à la sécurité de l'information sont-ils comparés aux critères de risque établis et hiérarchisés ?

Les informations sur le processus d'évaluation des risques relatifs à la sécurité de l'information ont-elles été documentées et sont-elles disponibles ?

Le processus de traitement des risques relatifs à la sécurité de l'information propose-t-il des solutions et des actions réalistes et applicables (temps, ressources, moyens) ?

Des contrôles ont-ils été déterminés pour mettre en œuvre l'option appropriée de traitement des risques choisie ?

Les contrôles ont-ils été établis en rapport avec ISO/IEC 27001:2013 Annexe A pour vérifier qu'aucun contrôle nécessaire n'a été omis ?

Avez-vous produit une Déclaration d'applicabilité pour justifier les exclusions et inclusions à l'Annexe A, ainsi que le statut de mise en œuvre du contrôle ?

Planification – *suite*

Un plan de traitement des risques relatifs à la sécurité de l'information a-t-il été créé ?

- Les propriétaires des risques ont-ils revu et approuvé le plan ?
- Les risques résiduels relatifs à la sécurité de l'information ont-ils été autorisés par les propriétaires des risques ?
- Cela a-t-il été documenté ?

Un plan est-il prévu pour déterminer le besoin de modifications à apporter au SMSI et gérer leur mise en œuvre ?

Des objectifs SMSI mesurables ont-ils été établis, documentés et communiqués à travers l'ensemble de l'organisation ?

Lors de l'établissement de ses objectifs SMSI, l'organisation a-t-elle déterminé quels besoins doivent être comblés et sur quelle échelle de temps ?

Support

L'organisation a-t-elle déterminé et fourni les ressources requises pour l'établissement, la mise en œuvre, la tenue et l'amélioration continue du SMSI (en tenant compte des individus, de l'infrastructure et de l'environnement pour le fonctionnement des processus) ?

Avez-vous mis en place un processus défini et documenté pour déterminer la compétence des rôles SMSI ?

- Ce processus et les compétences de ceux qui assument ces rôles ont-ils été documentés ?

L'organisation a-t-elle déterminé les connaissances nécessaires pour les personnes assumant ces rôles SMSI ?

L'organisation s'est-elle assurée que les personnes pouvant affecter les performances et l'efficacité du SMSI sont compétentes en termes d'expérience, de qualification et de formation ?

Dans le cas où cela est nécessaire, l'organisation a-t-elle pris des mesures pour veiller à ce que ces personnes puissent acquérir les compétences nécessaires ?

Des formations relatives aux exigences de l'ISO 27001:2013 ont t'elles été réalisées ou planifiées :

- Pour les responsables du SMSI
- Pour l'équipe d'audit interne
- Pour la direction dans le cadre des responsabilités qui sont les siennes vis-à-vis du SMSI

Les informations documentées requises par la norme et nécessaires pour la mise en œuvre et le fonctionnement efficaces du SMSI ont-elles été établies ?

Les informations documentées requises par l'organisation dans le cadre du SMSI sont-elles contrôlées de sorte à être disponibles, protégées, distribuées, stockées, conservées et soumises au contrôle des changements (y compris les documents d'origine externe) ?

Suite >>

Fonctionnement

Des preuves documentées ont-elles été réunies pour démontrer que les processus ont été mis en place et fonctionnent tel que prévu ?

Un plan est-il prévu pour déterminer le besoin de modifications à apporter au SMSI et gérer leur mise en place ?

Lorsque des modifications sont prévues, sont-elles effectuées de manière contrôlée et des mesures sont-elles prises pour limiter toute incidence négative ?

Si vous sous-traitez certains processus, sont-ils adéquatement contrôlés ?

Les évaluations des risques relatifs à la sécurité de l'information sont-elles conduites à des intervalles planifiés ou à la suite de modifications notables et des informations documentées sont-elles conservées ?

L'organisation a-t-elle planifié des actions pour traiter ces risques et opportunités et les intégrer dans les processus du SMSI ou dans de nouveaux processus ?

Ces mesures d'évaluations des risques ont-elles été documentées ?

Évaluation des performances

Avez-vous des critères pour l'évaluation, la sélection, le contrôle des performances et la ré-évaluation de vos prestataires externes ?

Avez-vous déterminé ce qui doit être contrôlé et mesuré, quand, par qui, les méthodes à utiliser et quand les résultats seront évalués ?

Les résultats du contrôle et de la mesure de la performance du SMSI sont-ils documentés ?

Des audits internes sont-ils conduits régulièrement pour vérifier le SMSI est efficace et conforme à ISO/IEC 27001:2013 ainsi qu'aux exigences et objectifs de l'organisation ?

L'organisation a-t-elle établi un programme pour les audits internes du SMSI ?

Dans le cas où ces audits seront réalisés par des salariés de l'entreprise, ce programme intègre-t-il un processus de formation spécifique de ces salariés à la technique d'audit et aux exigences d'audit interne selon l'ISO 2700:2013 ?

Dans le cas où ces audits seront réalisés par des prestataires externes, une procédure de contrôle de leur qualification a-t-elle été mise en place ?

Un contrôle de la bonne réalisation de ce processus d'audit interne est-il prévu et documenté ?

Les résultats de ces audits internes sont-ils rapportés à la direction, documentés et conservés ?

Évaluation des performances – *suite*

Lorsque des non-conformités sont identifiées, l'organisation a-t-elle établi des processus appropriés pour gérer ces non-conformités et mettre en place les actions correctives associées ?

La direction entreprend-elle des revues régulières et périodiques du fonctionnement du SMSI ?

Les conclusions de la revue de direction du SMSI identifie-t-elles des modifications et améliorations à apporter ?

Les résultats de la revue de direction sont-ils documentés, traités et communiqués aux parties intéressées le cas échéant ?

Amélioration continue

Les actions à mettre en œuvre pour contrôler, corriger et traiter les conséquences des non-conformités ont-elles été identifiées et organisées ?

Le besoin d'action a-t-il été évalué dans le but éliminer la cause racine des non-conformités identifiées en vue d'éviter qu'elles ne se reproduisent ?

Un processus de revue de l'efficacité des actions de traitement des non conformités envisagées, est-il prévu en termes d'efficacité et d'améliorations du SMSI ?

Des informations documentées sont-elles conservées pour attester de la nature des non-conformités ?

Des informations documentées sont-elles prévues pour suivre efficacement le processus d'amélioration continue sa mise en œuvre et sa bonne application dans le temps ?

Chez BSI, nous favorisons l'excellence en développant des normes pour aider les entreprises dans leur développement et volonté de performance. Nous aidons les organisations à faire preuve de résilience, à se développer de façon durable, à être capable de s'adapter au changement, à prévenir le risque et à **faire de l'excellence une habitude.**

Pour en savoir plus, appelez :
T: +33 (0)1 55 34 11 40
Consultez notre page Web :
www.bsigroup.fr
Ou venez à nos évènements ISO 27001

Les marques déposées sur le matériel (par exemple le logo BSI ou le mot "KITEMARK") sont des marques déposées enregistrées et non enregistrées détenues par The British Standards Institution au Royaume-Uni et dans certaines autres pays dans le monde.

© BSI Group BSI/UK/820/SC/0316/EN/BLD

En 1996 BSI a développé la norme BS 7799, point de départ de l'actuelle norme ISO 27001 management de la sécurité de l'information.

BSI est l'organisme de normalisation qui aide les organisations à faire de l'excellence une habitude, dans le monde entier. C'est notre créneau, permettre aux autres d'obtenir de meilleures performances. Avec plus de 80 000 clients dans plus de 170 pays, nos clients nous font confiance pour les aider à obtenir de meilleures performances, à réduire les risques et à se développer de façon durable.

L'ISO/IEC 27001 aidera votre entreprise à être conforme à la réglementation gouvernementale en constante augmentation et aux exigences spécifiques de l'industrie. En travaillant avec BSI à la mise en place des mesures de sécurité rigoureuses, vous pourrez renforcer la réputation de votre entreprise et sécuriser de nouvelles affaires.

bsi.

bsigroup.fr

bsi. ISO/IEC 27001:2013 Information Security Management

Les marques déposées sur le matériel (par exemple le logo BSI ou le mot "KITEMARK") sont des marques déposées enregistrées et non enregistrées détenues par The British Standards Institution au Royaume-Uni et dans certaines autres pays dans le monde.