Advisera

Livre blanc: Liste de contrôle de la documentation obligatoire pour ISO/IEC 27001 (Révision 2013)

27001 Academy
ISO 27001 and ISO 22301 Online Consultation Center

LIVRE BLANC

septembre 04, 2015

1. Quels documents et enregistrements sont nécessaires?

La liste ci-dessous montre l'ensemble minimal de documents et d'enregistrements requis par ISO/IEC 27001 révision 2013:

Documents*	Numéro de clause d'ISO 27001:2013
Domaine d'application du SMSI	4.3
Politique de sécurité de l'information et objectifs	5.2, 6.2
Méthodologie d'évaluation et de traitement des risques	6.1.2
Déclaration d'applicabilité	6.1.3 d)
Plan de traitement des risques	6.1.3 e), 6.2
Rapport d'évaluation et de traitement des risques	8.2, 8.3
Définition des rôles et responsabilités au sein de la sécurité	A.7.1.2, A.13.2.4
Inventaire des actifs	A.8.1.1
Utilisation correcte des actifs	A.8.1.3
Politique de contrôle d'accès	A.9.1.1
Procédures opérationnelles pour les technologies de l'information et de la communication	A.12.1.1
Principes d'ingénierie des systèmes sécurisés	A.14.2.5
Politique de sécurité des fournisseurs	A.15.1.1
Procédure de gestion des incidents	A.16.1.5
Procédures de continuité des activités	A.17.1.2
Exigences légales, réglementaires et contractuelles	A.18.1.1

Enregistrements*	Numéro de clause d'ISO 27001:2013
Enregistrements des formations, compétences, expériences et qualifications	7.2
Résultats de surveillance et de mesure	9.1
Programme d'audit interne	9.2
Résultats d'audits internes	9.2
Résultats de la revue de Direction	9.3
Résultats des actions correctives	10.1
Journaux de l'activité des utilisateurs, des exceptions et des évènements de sécurité	A.12.4.1, A.12.4.3

*Les mesures de l'Annexe A peuvent être exclues si une organisation conclut qu'il n'y a pas de risque ou si d'autres exigences demandent la mise en œuvre d'une mesure.

Ceci n'est en aucun cas une liste définitive de documents et d'enregistrements qui peuvent être utilisés lors de la mise en œuvre d'ISO 27001 – la norme permet d'autres documents pouvant être ajoutés pour améliorer le niveau de sécurité de l'information.

2. Documents non-obligatoires communément utilisés

D'autres documents qui sont très souvent utilisés sont les suivants:

Documents	Numéro de clause d'ISO 27001:2013
Procédure pour le contrôle des documents	7.5
Mesures pour la gestion des enregistrements	7.5
Procédure d'audit interne	9.2
Procédure pour les actions correctives	10.1
Politique de bring your own device (BYOD)	A.6.2.1
Politique en matière d'appareils mobiles et de télétravail	A.6.2.1
Politique de classification de l'information	A.8.2.1, A.8.2.2, A.8.2.3

Documents	Numéro de clause d'ISO 27001:2013
Politique des mots de passe	A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, A.9.4.3
Politique d'élimination et de destruction	A.8.3.2, A.11.2.7
Procédure pour travailler dans des zones sécurisées	A.11.1.5
Politique du bureau propre et de l'écran verrouillé	A.11.2.9
Politique de gestion du changement	A.12.1.2, A.14.2.4
Politique de sauvegarde	A.12.3.1
Politique de transfert de l'information	A.13.2.1, A.13.2.2, A.13.2.3
Bilan d'impact sur les activités	A.17.1.1
Plan d'exercices et de tests	A.17.1.3
Plan de revue et de maintenance	A.17.1.3
Stratégie de continuité des activités	A.17.2.1

3. Comment structurer les documents et les enregistrements les plus courants

Domaine d'application du SMSI

Ce document est généralement assez court, et écrit au début de la mise en œuvre de la norme ISO 27001. Normalement, c'est un document autonome, mais il peut être fusionné avec la Politique de sécurité de l'information.

Lire plus ici: Problèmes avec la définition du domaine d'application de la norme ISO 27001.

Politique et objectifs de la sécurité de l'information

La Politique de sécurité de l'information est généralement un document court et de haut-niveau, décrivant les principaux buts du SMSI. Les objectifs du SMSI sont généralement un document autonome, mais il peut aussi être fusionné avec la Politique de sécurité de l'information. Contrairement à la révision de la norme ISO 27001 2005, il n'y a plus besoin à la fois de la Politique du SMSI et de la Politique de sécurité de l'information – seule la Politique de sécurité de l'information est nécessaire.

Lire plus ici: Politique de sécurité de l'information – comment doit-elle être détaillée?

Méthodologie et rapport d'évaluation et de traitement des risques

La Méthodologie d'évaluation et de traitement des risques est habituellement un document de 4 ou 5 pages, et il doit être écrit avant que l'évaluation et le traitement des risques ne soient réalisés. Le Rapport d'évaluation et de traitement des risques doit être écrit après que l'évaluation et le traitement des risques ne soient réalisés, et il résume tous les résultats.

Lire plus ici: Evaluation et traitement des risques de la norme ISO 27001 – 6 étapes de base

Déclaration d'applicabilité

La Déclaration d'applicabilité (ou DdA) est écrite sur la base des résultats de traitement des risques – c'est un document central au sein du SMSI, car il décrit non seulement quelles mesures de l'Annexe A sont applicables, mais aussi comment elles seront mises en œuvre, et leur statut actuel. Vous pourriez également envisager la Déclaration d'applicabilité comme un document qui décrit le profil de sécurité de votre entreprise.

Lire plus ici: L'importance de la Déclaration d'applicabilité pour la norme ISO 27001.

Plan de traitement des risques

Ceci est essentiellement un plan d'action sur la façon de mettre en œuvre différentes mesures définies dans la DdA – il est développé sur la base de la Déclaration d'applicabilité, et est activement utilisé et mis à jour tout au long de la mise en œuvre du SMSI. Parfois, il peut être fusionné avec le plan de projets.

Lire plus ici: Plan de traitement des risques et processus de traitement des risques – Quelle est la différence?

Rôles et responsabilités au sein de la sécurité

La meilleure méthode, est de les décrire dans toutes les politiques et procédures, aussi précisément que possible. Evitez les expressions comme "devrait être fait," et utilisez à la place quelque chose comme "le RSI effectuera xyz chaque lundi à zxy heure." Certaines entreprises préfèrent pour décrire les rôles et responsabilités au sein de la sécurité, utiliser les descriptions de poste; cependant, cela peut conduire à beaucoup de paperasse.

Les rôles et responsabilités au sein de la sécurité pour les parties tierces sont définis dans les contrats.

Lire plus ici: Quel est le métier du Responsable de la sécurité de l'information (RSI) dans la norme ISO 27001?

Inventaire des actifs

Si vous ne disposez pas d'un tel inventaire avant le projet ISO 27001, la meilleure façon de créer un tel document est directement à partir des résultats de l'évaluation des risques – lors de l'évaluation des risques, tous les actifs et leurs propriétaires doivent être de toutes façons identifiés, il vous suffit de copier les résultats à partir de là.

Lire plus ici: Comment gérer le Registre des actifs (Inventaire des actifs) selon la norme ISO 27001.

Utilisation correcte des actifs

Ceci est habituellement écrit sous la forme d'une politique, et un tel document peut couvrir un très large éventail de sujets, car la norme ne définit pas très bien ces mesures. Probablement, la meilleure façon de l'aborder est la suivante: (1) la laisser pour la fin de la mise en ouvre de votre SMSI, et (2) toutes les domaines

& toutes les mesures que vous n'avez pas couvert avec d'autres documents et qui concernent tous les employés, les couvrir avec cette politique.

Politique de contrôle des accès

Dans ce document, vous pouvez seulement couvrir l'aspect métier de l'accès autorisé à certaines informations et certains systèmes, ou encore le côté technique du contrôle des accès; en outre, vous pouvez choisir de définir les règles seulement pour l'accès logique, ou encore pour l'accès physique. Vous ne devriez écrire ce document seulement après avoir terminé votre processus d'évaluation et de traitement des risques.

Procédures opérationnelles pour la gestion informatique

Vous pouvez l'écrire en un seul document, ou en une série de politiques et de procédures – si vous êtes une plus petite entreprise, vous aurez tendance à avoir un nombre moins important de documents. Normalement, vous pouvez couvrir toutes les parties des sections A.12 et A.13 – la gestion du changement, les services de parties tierces, la sauvegarde, la sécurité du réseau, les codes malveillants, l'élimination et la destruction, le transfert d'information, la surveillance du système, etc. Vous ne devriez écrire ce document qu'après avoir terminé votre processus d'évaluation et de traitement des risques.

Lire plus au sujet de la gestion informatique ici: Blog ITIL & ISO 20000.

Principes d'ingénierie des systèmes sécurisés

Ceci est une nouvelle mesure dans la norme ISO 27001:2013, et exige que les principes d'ingénierie sécurisée soient documentés sous une forme de procédure ou de norme, et devraient définir la façon d'intégrer des techniques de sécurité dans toutes les couches de l'architecture – métier, données, applications et technologies. Ils peuvent inclure la validation des données, le débogage, les techniques pour l'authentification, les mesures de session sécurisée, etc.

Politique de sécurité des fournisseurs

Ceci est également une nouvelle mesure dans la norme ISO 27001:2013, et une telle politique peut couvrir un large éventail de mesures – comment sont scrutés les potentiels contractants, comment l'évaluation des risques d'un fournisseur est réalisée, quelles clauses de sécurité sont inscrites dans un contrat, comment superviser le respect des clauses contractuelles de sécurité, comment modifier le contrat, comment fermer les accès une fois que le contrat est résilié, etc.

Lire plus ici: Processus en 6 étapes pour gérer la sécurité des fournisseurs selon ISO 27001.

Procédure de gestion des incidents

Ceci est une procédure importante, qui définit la façon dont les failles de sécurité, les évènements et les incidents sont rapportés, classifiés et traités. Cette procédure définit également comment apprendre des incidents de sécurité de l'information, de sorte qu'ils puissent être évités la prochaine fois. Une telle procédure peut aussi invoquer le Plan de continuité des activités, si un incident a provoqué une longue interruption.

Procédures de continuité des activités

Ce sont généralement des plans de continuité des activités, des plans de réponse aux incidents, des plans de reprise des activités pour l'organisation, et des plans de reprise en cas de désastre (des plans de reprise pour les infrastructures informatiques). Ces derniers sont mieux décrits dans la norme ISO 22301, la norme de premier plan pour la continuité des activités.

Pour apprendre plus, cliquer ici: Plan de continuité des activités: Comment le structurer selon la norme ISO 22301.

Exigences légales, réglementaires et contractuelles

Cette liste devrait être faite aussitôt que possible dans le projet, car de nombreux documents devront être mis au point en fonction de ces données. Cette liste ne devrait pas seulement comprendre les responsabilités pour se conformer à certaines exigences, mais aussi les délais.

Enregistrements de la formation, des compétences, de l'expérience et des qualifications

Ces enregistrements sont normalement maintenus par le département des ressources humaines – si vous ne disposez pas d'un tel département, toute personne qui maintient normalement les enregistrements des employés devrait faire ce travail. Fondamentalement, un dossier avec tous les documents insérés, sera efficace.

Lire plus ici: Comment réaliser la formation et la sensibilisation pour les normes ISO 27001 et ISO 22301.

Résultats de la surveillance et de la mesure

La meilleure façon de décrire la manière dont les mesures sont évaluées, est de le faire au travers des politiques et des procédures qui définissent chaque mesure – normalement, cette description peut être écrite à la fin de chaque document, et une telle description définit le type de KPIs (indicateurs clé de performance) qui doit être mesuré pour chaque mesure ou groupe de mesures.

Une fois que cette méthode de mesure est en place, vous devez effectuer la mesure en conséquence. Il est important de signaler ces résultats régulièrement aux personnes en charge de les évaluer.

Lire plus ici: Objectifs des mesures de la norme ISO 27001 – Pourquoi sont-ils si importants?

Programme d'audit interne

Le Programme d'audit interne n'est rien d'autre qu'un plan annuel pour réaliser des audits – pour une petite entreprise, cela pourrait être qu'un seul audit, alors que pour une entreprise plus grande, cela pourrait être une série d'audits, par exemple, 20 audits internes. Ce programme devrait définir qui effectuera les audits, les méthodes, les critères d'audit, etc.

Lire plus ici: Comment faire une Liste de contrôle d'audit interne pour les normes ISO 27001 / ISO 22301.

Résultats des audits internes

Un auditeur interne doit produire le Rapport d'audit, qui comprend les résultats de l'audit (observations et actions correctives). Ce rapport doit être produit dans un intervalle de deux jours après qu'un audit interne ait été réalisé. Dans certains cas, l'auditeur interne devra vérifier si toutes les actions correctives ont été effectuées comme prévu.

Résultats de la revue de Direction

Ces enregistrements sont normalement sous la forme de comptes-rendus de réunion – ils doivent inclure tous les matériaux qui ont été utilisés lors de la réunion de Direction, ainsi que toutes les décisions qui ont été prises. Les comptes-rendus peuvent être sous forme papier ou électronique.

Lire plus ici: Pourquoi la revue de Direction est importante pour les normes ISO 27001 et ISO 22301?

Résultats des actions correctives

Ceux-ci sont traditionnellement inclus dans les Formulaires d'actions correctives (FACs). Cependant, il est beaucoup mieux d'inclure de tels enregistrements dans une application qui est déjà utilisée par le Help Desk de l'organisation – parce que les actions correctives ne sont rien d'autre que des listes de choses à faire avec des responsabilités, des tâches et des délais clairement définis.

Lire plus ici: Utilisation pratique des actions correctives des normes ISO 27001 et ISO 22301.

Journaux de l'activité des utilisateurs, des exceptions et des évènements de sécurité

Ceux-ci sont normalement maintenus sous deux formes: (1) sous forme numérique, automatiquement ou semi-automatiquement produits comme journaux de divers systèmes informatiques ou autres, et (2) sous forme papier, où chaque enregistrement est inscrit manuellement.

Procédure pour le contrôle des documents

Ceci est normalement une procédure autonome, de 2 ou 3 pages. Si vous avez déjà mis en œuvre une autre norme comme ISO 9001, ISO 14001, ISO 22301 ou similaire, vous pouvez utiliser la même procédure pour tous ces systèmes de management. Parfois, il est préférable d'écrire cette procédure en tant que premier document dans le projet.

Lire plus ici: Gestion documentaire dans les normes ISO 27001 & BS 25999-2.

Mesures pour la gestion des enregistrements

La meilleure façon est de décrire les enregistrements des mesures dans chaque politique ou procédure (ou autre document) qui nécessitent la création d'un enregistrement. Ces mesures sont normalement écrites à la fin de chaque document, et sont généralement sous le forme d'un tableau décrivant où les enregistrements sont conservés, qui a accès, comment sont-ils protégés, pour combien de temps sont-ils archivés, etc.

Procédure d'audit interne

Ceci est normalement une procédure autonome de 2 ou 3 pages, et qui doit être écrite avant le début de l'audit interne. Comme avec la Procédure pour le contrôle des documents, une Procédure d'audit interne peut être utilisée pour tout système de management.

Lire plus ici: Dilemmes avec les auditeurs internes des normes ISO 27001 & BS 25999-2.

Procédures pour les actions correctives

Cette procédure ne devrait être plus longue que 2 ou 3 pages, et peut être écrite à la fin du projet de mise en œuvre, mais il est préférable de l'écrire plus tôt afin que les employés puissent s'y habituer.

4. Modèles de documentation échantillon

Ici, vous pouvez télécharger un Aperçu gratuit de la boîte à outils documentaire de ISO 27001 & ISO 22301 – dans cet aperçu gratuit, vous serez en mesure de voir la Table des matières de chaque plan, politique et procédure mentionnés, ainsi que quelques sections de chaque document.

Advisera

27001 Academy
ISO 27001 and ISO 22301 Online Consultation Center

EPPS Services Ltd.
pour le conseil aux entreprises
UI. Vladimira Nazora 59, 10000 Zagreb
Croatie, Union Européenne

Email: support@advisera.com
Téléphone: +1 (646) 759 9933
Toll-free (U.S.A./Canada) : 1-888-553-2256
Toll-free (United Kingdom) : 0800 808 5485
Fax: +385 1 556 0711

EXPLORER LES ACADÉMIES

9001 Academy
ISO 9001 Online Consultation Center

14001 Academy
ISO 14001 Online Consultation Center

20000 Academy
ITIL and ISO 20000 Online Consultation Center

18001 Academy
OHSAS 18001 Online Consultation Center