Advisera

Livre blanc: Liste de contrôle de la documentation obligatoire pour ISO 22301

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 22301:2012 (la norme se réfère aux documents et enregistrements en tant qu'informations documentées):

Documents et enregistrements	Numéro de clause d'ISO 22301
Détermination du contexte de l'organisation	4.1
Procédure d'identification des exigences légales et réglementaires applicables	4.2.2
Liste des exigences légales, réglementaires et autres	4.2.2
Domaine d'application du SMCA (Système de management de la continuité des activités) et explication des exclusions	4.3
Politique de continuité des activités	5.3
Objectifs de continuité des activités	6.2
Compétences du personnel	7.2
Communication avec les parties intéressées	7.4
Processus pour le bilan d'impact sur les activités et l'évaluation des risques	8.2.1
Résultats du bilan d'impact sur les activités	8.2.2
Résultats de l'évaluation des risques	8.2.3
Procédures de continuité des activités	8.4.1
Procédures de réponse aux incidents	8.4.2
Décision si les risques et les impacts doivent être communiqués à l'extérieur	8.4.2

Documents et enregistrements	Numéro de clause d'ISO 22301
Communication avec les parties intéressées, y compris les autorités consultatives de gestion des risques au niveau national ou régional	8.4.3
Enregistrements des informations importantes sur les incidents, actions menées et décisions prises	8.4.3
Procédures pour répondre aux incidents perturbateurs	8.4.4
Procédures pour la restauration et la reprise des affaires après des mesures temporaires	8.4.5
Résultats des actions portant sur des tendances ou des résultats indésirables	9.1.1
Données et résultats de la surveillance et de la mesure	9.1.1
Résultats de la revue post-incident	9.1.2
Résultat d'audit interne	9.2
Résultat de la revue de Direction	9.3
Nature des non-conformités et des actions prises	10.1
Résultats des actions correctives	10.1

Ceci n'est en aucun cas une liste définitive des documents et des enregistrements qui peuvent être utilisés lors de la mise en œuvre d'ISO 22301 – la norme permet l'ajout d'autres documents pour améliorer le niveau de résilience.

2. Documents non-obligatoires communément utilisés

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

Documents	Numéro de clause d'ISO 22301
Plan de mise en œuvre pour atteindre les objectifs de continuité des activités	6.2
Plan de formation et de sensibilisation	7.2 e 7.3
Procédure pour le contrôle des informations documentées	7.5

Contrats et accords de niveau de service (SLAs) avec les fournisseurs et les partenaires d'externalisation	8.1
Stratégie de continuité des activités	8.3
Atténuation des risques	8.3.3
Scénarios d'incidents	8.5
Plans d'exercice et de tests	8.5
Rapports post-exercice	8.5
Plan de maintenance su SMCA	9.1.1
Méthodes de surveillance, de mesure, d'analyse et d'évaluation	9.1.1
Procédure d'audit interne	9.2
Programme d'audit interne	9.2
Procédure pour les actions correctives	10.1

3. Comment structurer les documents et les enregistrements

Détermination du contexte de l'organisation (4.1)

Le contexte est généralement déterminé par plusieurs documents, par exemple, la Procédure pour l'identification des exigences, la Politique de continuité des activités, la Méthodologie de bilan d'impact sur les activités, la Méthodologie d'évaluation des risques, etc.

En d'autres termes, vous ne voudrez pas produire un seul document pour déterminer un contexte; mais plutôt le décrire à travers plusieurs documents appropriés.

Procédure d'identification des exigences légales et réglementaires applicables & Liste des exigences légales, réglementaires et autres (4.2.2)

C'est généralement une procédure assez courte, qui définit qui est responsable de la conformité: qui doit identifier toutes les parties intéressées, qui doit suivre toutes les lois, règlements et autres exigences des parties intéressées, qui sera responsable de se conformer aux exigences, comment ces exigences seront communiquées, etc.

Cette procédure, et la Liste obtenue, doivent être définies dès le début du projet, car elles fourniront des contributions pour l'ensemble du SMCA.

Lire plus ici: Comment identifier les parties intéressées selon ISO 27001 et ISO 22301.

Domaine d'application du SCMA et explication des exclusions (4.3)

Ce document est également très court, et doit être rédigé au début du projet de continuité des activités. Il faut définir clairement à quelles parties de votre organisation le SMCA sera appliqué, en fonction des exigences identifiées et des aspirations de l'organisation. Il peut également expliquer pourquoi certaines parties de votre organisation ont été exclues du domaine d'application.

Très souvent, ce document est fusionné avec la Politique de continuité des activités.

Politique de continuité des activités et objectifs de continuité des activités (5.3, 6.2)

C'est le document central dans lequel la direction devrait indiquer ce qu'elle veut réaliser avec le SMCA, et comment elle va le contrôler. Très souvent, la direction approuvera seulement ce document de haut niveau, alors que les autres documents du SMCA seront approuvés par des managers de niveau inférieur.

Ce document est plutôt court et les organisations plus petites et de taille moyenne fusionnent généralement le domaine d'application au sein de ce document, ainsi que les objectifs du SMCA; les organisations plus grandes auront normalement un domaine d'application et des objectifs dans des documents distincts.

Les objectifs du SMCA ne doivent pas être mélangés avec les Objectifs de temps de reprise (OTRs) – les objectifs du SMCA sont fixés pour l'ensemble du SMCA, et non pas pour les activités.

Lire plus ici: Le but de la politique de continuité des activités selon ISO 22301.

Plan de formation et de sensibilisation; compétences du personnel (7.2, 7.3)

Ces plans sont généralement développés de façon annuelle, et sont normalement développés par la personne responsable de la continuité des activités ensemble avec le département des ressources humaines (si vous en avez un). Les enregistrements des compétences sont généralement 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 selon ISO 27001 et ISO 22301.

Communication avec les parties intéressées (7.4)

Cette communication se présente habituellement sous différentes formes: email, courrier régulier, par téléphone, etc.

Documenter cette communication est plutôt facile - vous avez seulement besoin de conserver des copies de ces emails, lettres, documents, etc. dans une sorte d'archive. Si la communication a été faite par téléphone, une note doit être faite et ensuite archivée selon les règles prédéfinies.

Procédure pour le contrôle des informations documentées (7.5)

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 comme premier document dans un projet.

Lire plus ici: La gestion documentaire pour ISO 27001 & BS 25999-2.

Contrats et accords de niveau de service (8.1)

Il est crucial que vos fournisseurs et partenaires d'externalisation réagissent d'une manière attendue lorsqu'un incident se produit - c'est pourquoi, il est préférable de produire un modèle avec les exigences de continuité des activités minimales que vous devez insérer dans chacun des contrats que vous signez avec eux.

Processus pour le bilan d'impacts sur les activités & résultats (8.2.1, 8.2.2)

Avant de commencer votre bilan d'impact sur les activités (BIA), vous devez définir les règles sur la façon dont il sera exécuté – cela se fait généralement avec la Méthodologie de bilan d'impact sur les activités. Cette méthodologie devrait être écrite sur 4 ou 5 pages - assez courte pour être facilement lisible, mais pas trop courte pour ne pas être vague.

La collecte de données pour une telle analyse est effectuée au moyen de questionnaires BIA, qui peuvent être dans un format Excel simple, ou vous pouvez utiliser certains outils du BCM.

Les résultats du processus BIA sont documentés dans le Rapport du bilan d'impact sur les activités (pour les grandes entreprises), ou vous pouvez résumer les résultats de la Stratégie de continuité des activités (ce qui est la version courte - plus applicable pour des organisations plus petites ou de taille moyenne).

Lire plus ici: Comment implémenter un bilan d'impacts sur les activités (BIA) selon ISO 22301.

Processus pour l'évaluation des risques & résultats (8.2.1, 8.2.3)

Comme le Bilan d'impact sur les activités, l'évaluation des risques doit également être définie dans une méthodologie, avant de l'exécuter. Comme ISO 22301 ne spécifie pas vraiment les exigences pour l'évaluation des risques, vous pouvez utiliser la méthodologie d'ISO 27001 et d'ISO 27005, étant donné que ces normes donnent probablement la meilleure méthodologie pour l''évaluation des risques de la continuité des activités. Les résultats de l'évaluation des risques doivent être documentés dans le Rapport d'évaluation des risques.

Apprendre plus ici: Est-ce que l'analyse des risques ISO 27001 peut être utilisée pour ISO 22301?

Stratégie de continuité des activités (8.3)

Ceci est un lien essentiel entre le bilan d'impact sur les activités, l'évaluation des risques et les plans - son but est de veiller à ce que toutes les ressources soient disponibles en cas de perturbation. Ceci est crucial, car sans toutes les ressources, le Plan de continuité des activités ne sera pas réalisable.

La Stratégie de continuité des activités est habituellement un document de haut niveau, comprenant des stratégies pour chaque activité sous forme d'annexes.

Lire plus ici: Est-ce que les stratégies de continuité des activités peuvent vous faire économiser de l'argent?

Atténuation des risques & Plan de mise en œuvre pour atteindre les objectifs de continuité des activités (6.2, 8.3.3)

L'atténuation des risques est normalement documentée au travers du Plan de traitement des risques; cependant, il est plus pratique de le fusionner dans un Plan de mise en œuvre plus complet, qui inclurait toutes les activités nécessaires pour la mise en œuvre de l'ensemble du SMCA.

Lire plus ici: Plan et processus de traitement des risques – quelle différence?

Procédures de continuité des activités (8.4.1)

De manière générale, les procédures de continuité des activités comprennent les plans de réponse aux incidents, les plans de reprise des activités, les plans de reprise en cas de désastre, les plans de communication, etc. Vous pouvez organiser tous ces documents dans un unique Plan de continuité des activités, qui aura des annexes pour chaque élément mentionné.

Voir des détails dans cet article: Plan de continuité des activités: Comment le structurer selon ISO 22301.

Procédures de réponse aux incidents & enregistrements sur un incident (8.4.2, 8.4.3)

Dans ces procédures, vous devez adresser tous les risques majeurs auxquels votre organisation est confrontée - et, quelles réponses initiales fournir si de tels incidents se produisent. Vous pouvez rédiger ces procédures dans un document unique, ou comme des procédures séparées – un document pour chaque incident potentiel. Très souvent, celles-ci sont écrites dans un document appelé Plan de réponse aux incidents; de tel(s) document(s) peut(vent) également inclure des procédures de communication, des plans de transport, etc. En d'autres termes, ces procédures peuvent être assez longues.

Un plan de réponse aux incidents devrait définir la méthode d'enregistrement des faits lors d'un incident – cela peut être quelque chose d'aussi simple que des notes manuscrites à côté de chaque étape dans le plan tel qu'il a été exécuté.

Apprendre plus ici: Procédures d'activation pour un plan de continuité des activités.

Procédures de communication (8.4.2, 8.4.3)

Ces procédures doivent couvrir la décision de comment les risques et les impacts doivent être communiqués à l'extérieur, et comment sont-ils communiqués aux parties intéressées, en particulier aux autorité de consultation de gestion des risques nationales ou régionales (par exemple, tsunamis). Pour des entreprises plus petites ou de taille moyenne, de telle procédures seront comprises dans le Plan de réponse aux incidents, alors que dans des entreprises plus grandes, elles seront des documents distincts.

Le point essentiel ici, est de définir clairement qui est responsable de la communication avec qui, en particulier, qui est autorisé à communiquer aux médias publics, et aux autorités. En outre, des modèles peuvent être développés pour communiquer avec les médias, qui vous aideront à publier des communiqués rapidement, si nécessaire.

Procédures pour répondre aux incidents perturbateurs (8.4.4)

Ce sont normalement des procédures de reprise après un désastre (en se concentrant sur la façon de récupérer les infrastructures des technologies de l'information et de communication), et des procédures de reprise des activités (en se concentrant sur la reprise des activités commerciales de l'organisation).

Ensemble avec le Plan de réponse aux incidents, ces procédures forment la plus grande partie des procédures de continuité des activités.

Lire plus ici: Reprise en cas de désastre et continuité des activités : quelles différences.

Procédures pour la restauration et la reprise des affaires de mesures temporaires (8.4.5)

Dans la plupart des cas, ces procédures ne seront pas très détaillées, car vous ne pouvez pas savoir à l'avance quels types de dégâts vos installations subiront. Par conséquent, vous pouvez définir brièvement qui aura la responsabilité d'évaluer les dommages et prendra les décisions appropriées – vous pouvez mettre ces procédures dans le Plan de continuité des activités de haut-niveau.

Scénarios d'incident (8.5)

Ce sont de courtes descriptions (ou scénarios) présentant la façon dont un certain incident peut se développer et de comment il peut impacter les activités de votre entreprise.

Elles devraient être élaborés sur la base des résultats de l'évaluation des risques (elles devraient refléter les risques majeurs), et peuvent être ajoutées soit au Plan d'exercice et de test, soit à la Stratégie de continuité des activités.

Plans d'exercice et de test & rapports de post-exercice (8.5)

Les exercices et les tests sont cruciaux pour l'amélioration des procédures de continuité des activités – normalement, vous devez effectuer des exercices et des tests au moins une fois par an, et ils devraient devenir de plus en plus difficiles les années suivantes.

Chaque plan devrait définir les objectifs qui doivent être remplis et les scénarios; le rapport doit indiquer jusqu'à quel point ces objectifs ont été atteints.

Résultats des actions portant sur des tendances ou des résultats indésirables (9.1.1)

Ces actions se reflètent sous deux formes: (1) Plan de traitement des risques (mentionné ci-dessus), et (2) actions préventives.

Les actions préventives ne sont pas obligatoires dans la norme ISO 22301, mais elles existent dans les normes ISO 27001, ISO 9001 et autres systèmes de management – donc si vous avez déjà une Procédure pour les actions préventives en raison d'autres systèmes, vous pouvez aussi l'utiliser pour votre SMCA.

Plan de maintenance du SMCA (9.1.1)

Comme la documentation du SMCA peut être très complète, et devenir obsolète très facilement, il convient de définir exactement quand chaque document sera révisé. Cela peut être un simple tableau définissant quand chaque document devrait être révisé, et par qui.

Méthodes de surveillance, de mesure, d'analyse et d'évaluation (9.1.1)

La meilleure façon de décrire comment le système doit être mesuré, est au travers chaque politique et procédure – normalement, cette description peut être écrite à la fin de chaque document, et ces descriptions définissent le type de KPIs (indicateurs clés de performance) qui a besoin d'être mesuré pour chaque document.

Données et résultats de la surveillance et de la mesure (9.1.1)

Ce sont tous les rapports, KPIs, résultats non-officiels envoyés par email, décisions, etc. – tout cela doit être conservé pendant une période de temps spécifiée.

Résultats de la revue post-incident (9.1.2)

La meilleure méthode, serait de créer un formulaire avec toutes les données nécessaires qui doivent être prises en compte après qu'un incident ait eu lieu. Quand un tel formulaire est rempli et que les conclusions appropriées sont prises (que les plans de continuité des activités sont bien ou mal réalisés), cela doit être conservé pour une période de temps spécifiée.

Procédure d'audit interne, programme d'audit interne et résultats d'audits internes (9.2)

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

Un programme d'audit interne pourrait être un simple document d'une page, décrivant quand chaque audit aura lieu, et qui le réalisera.

Les résultats de l'audit interne sont documentés au travers du Rapport d'audit interne – un tel rapport devrait couvrir toutes les non-conformités, ainsi que les observations.

Lire plus ici: Comment faire une liste de contrôle pour l'audit interne de ISO 27001 / ISO 22301.

Résultats de la revue de management (9.3)

Ces documents sont normalement sous la forme de compte-rendus de réunions - ils doivent comprendre tous les matériaux qui ont été inclus lors de la réunion de management, ainsi que toutes les décisions qui ont été prises. Le compte-rendu peut être sous forme papier ou numérique.

Lire plus ici: Pourquoi est-ce que la revue de Direction est importante pour ISO 27001 et ISO 22301?

Non-conformités et actions correctives (10.1)

Habituellement, cela est couvert par la Procédure pour les actions correctives– si vous avez déjà les normes ISO 27001, ISO 9001 ou autre système de management, alors vous pouvez utiliser les procédures existantes à cet effet.

Habituellement, une telle procédure ne dépasse pas 2 ou 3 pages. Cette procédure 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.

Les résultats des actions correctives sont traditionnellement inclus dans les Formulaires d'actions correctives (FACs). Cependant, il est beaucoup mieux d'inclure de tels enregistrements dans des applications qui sont déjà utilisées dans une organisation pour Help Desk – car 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 pour ISO 27001 et ISO 22301.

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