TOPCERTIFIER
www.topcertifier.com

MÉTHODOLOGIE DE SERVICE ISO 27001:2013

INFORMATION GESTION DE LA SÉCURITÉ SYSTÈME (SMSI)

TOPCERTIFIER
www.topcertifier.com

INTRODUCTION À LA NORME ISO 27001:2013

La norme ISO 27001:2013 permet à une organisation d'identifier les risques liés à la sécurité de l'information. Prendre en compte les menaces, les vulnérabilités, les impacts et protéger l'organisation sans compromettre sa CIA (Confidentiality Integrity Availability) d'informations en adoptant Système de gestion de la sécurité des informations approprié L'objectif global de la norme ISO 27001:2013 est de couvrir les aspects ci-dessous.

- Fournir un modèle pour établir, mettre en œuvre, exploiter, surveiller, examiner, maintenir et l'amélioration d'un système de gestion de la sécurité de l'information avec des contrôles physiques et techniques.

- Veiller à ce que le SMSI soit intégré aux processus métier de l'organisation.

- Créer une culture organisationnelle qui encourage la participation active des employés dans le Système de gestion de la sécurité de l'information.

DÉMARRER

La réunion de lancement est un outil essentiel pour communiquer et planifier l'exécution du projet avec un minimum d'obstruction et pour terminer le projet dans les délais et les coûts prévus. L'ordre du jour de la réunion de lancement est le suivant :

- Discussion sur le plan de projet : cela inclut une discussion sur la responsabilité et la responsabilité des parties prenantes. titulaires. jalons et livrables du projet

- Portée des services et portée de la certification

- Exigences légales et réglementaires

CRÉATION DE L'ÉQUIPE DE BASE

- Nomination du RSSI
- Nomination du comité de gestion de la sécurité de l'information
- Nomination des auditeurs internes
- Responsable PCA
- Nomination du leader ISO

TOPCERTIFIER
www.topcertifier.com

ANALYSE DES ÉCARTS

Au cours de cette phase, nous effectuons une analyse des écarts pour vérifier dans quelle mesure vos pratiques actuelles sont en conforme aux exigences standards. les pratiques sont vérifiées par rapport à ces quatre critères de référence

- Exigences de la norme ISO 27001 : 2013
- SOA
- Exigences légales, statutaires et réglementaires
- Exigences des clients
- Politiques et procédures internes

Les résultats de cette analyse sont présentés sous la forme d'un rapport d'analyse des écarts. Ce rapport agit ainsi que la liste des actions à entreprendre pour le rappel du projet.

FORMATION DE SENSIBILISATION SMSI de l'UA

Une formation de sensibilisation au SMSI sera dispensée aux employés de votre organisation. La formation La session vise à aider les employés à acquérir des connaissances, à comprendre les concepts de la norme ISO 27001:2013, et aligner les processus et les pratiques pour parvenir à un environnement de travail sécurisé et sans menace. Lorsque le personnel a été formé, il peut penser, agir et contribuer à la réalisation des objectifs. objectifs.

REGISTRE DES RISQUES & SOA

Une procédure de gestion des risques doit être documentée et utilisée comme référence pour gérer les risques identifiés en consultation avec tous les propriétaires de processus et les responsables fonctionnels. Nous utilisons la norme ISO 31000 & Techniques standards de gestion des risques ISO 27005 pour identifier, analyser, évaluer, documenter, prioriser, traiter et quantifier les risques identifiés. Cette étape crée un registre des risques. Risque approprié les plans de traitement sont identifiés en fonction du niveau d'appétit pour le risque et du facteur CIA de l'entreprise. Les résultats de ces actions sont calculés, enregistrés, évalués et documentés. Le La déclaration d'applicabilité (SOA) définit et identifie les contrôles physiques et techniques applicable à votre organisation en fonction de vos processus métier et de vos exigences.

TOPCERTIFIER
www.topcertifier.com

GESTION D'ACTIFS

Nous aidons à l'élaboration de politiques et de procédures de gestion d'actifs en nous coordonnant avec le chefs fonctionnels et compréhension du processus. L'objectif principal de l'actif la gestion est :

- Identifier les actifs de l'organisation et définir les responsabilités de protection appropriées.

- Pour empêcher la divulgation, la modification, la suppression ou la destruction non autorisée des informations stockées sur les médias

- Garantir que les informations bénéficient d'un niveau de protection approprié conformément à leurs importance pour l'organisation

SÉCURITÉ RÉSEAU / COMMUNICATION :

Nous aidons à développer des politiques et des procédures de gestion de la sécurité du réseau en coordonnant avec les responsables fonctionnels et compréhension du processus. L'objectif principal de la sécurité des réseaux est :

- Assurer la protection des informations dans les réseaux et le traitement des informations qui les supportent. installations

- Pour maintenir la sécurité des informations transférées au sein d'une organisation et avec toute entité externe

GESTION DES INCIDENTS

Nous aidons à élaborer des politiques et des procédures de gestion des incidents en nous coordonnant avec le chefs fonctionnels et compréhension du processus. L'objectif principal de l'incident la gestion est :

- To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses

TOPCERTIFIER
www.topcertifier.com

GESTION DE LA CONTINUITÉ DES ACTIVITÉS

Nous aidons à développer des politiques et des procédures de gestion de la continuité des activités en coordination avec les responsables fonctionnels et compréhension du processus. L'objectif principal de gestion de la continuité des activités est la suivante :

- Pour garantir que la continuité de la sécurité de l'information doit être intégrée aux activités de l'organisation. systèmes de gestion de la continuité

- Assurer la disponibilité des installations de traitement de l'information

SÉCURITÉ PHYSIQUE :

Nous aidons à élaborer des politiques et des procédures de sécurité physique en nous coordonnant avec le chefs fonctionnels et compréhension du processus. L'objectif principal du Physique la sécurité c'est :

- Pour empêcher l'accès physique non autorisé, les dommages et les interférences avec les activités de l'organisation. installations d'information et de traitement de l'information

- Pour prévenir la perte, les dommages, le vol ou la compromission des actifs et l'interruption des activités de l'organisation. opérations

SÉCURITÉ DES RESSOURCES HUMAINES :

Nous aidons à l'élaboration de politiques et de procédures RH en nous coordonnant avec les responsables fonctionnels. et la compréhension du processus. L'objectif principal de la sécurité RH est :

- S'assurer que les employés et les sous-traitants comprennent leurs responsabilités et sont aptes à les rôles pour lesquels ils sont considérés

- Pour protéger les intérêts de l'organisation dans le cadre du processus de changement ou de cessation emploi

- S'assurer qu'une formation adéquate a été donnée à tous les employés et fournisseurs avec en ce qui concerne la sécurité de l'information

TOPCERTIFIER
www.topcertifier.com

DOCUMENTATION

Nos experts répertorieront les politiques, les processus, les SOP, les SOA applicables et les enregistrements qui doivent être défini et documenté conformément aux exigences de la norme ISO 27001:2013 en discutant avec chacun chefs de département et de fonction, nous vous assistons pour la création de la documentation nécessaire.

ÉTABLIR DES CONTRÔLES ISMS

Une fois que les politiques, processus, déclaration d'applicabilité (SOA), ses contrôles et SOP ont été été documenté et la liste des dossiers à collecter a été répertoriée et le personnel a été identifiés et formés à de telles activités, il est alors nécessaire d'exploiter, de surveiller et d'examiner les l'efficacité de tels processus.

FORMATION D'AUDIT INTERNE

Une formation d'auditeur interne (IA) ISO 27001 : 2013 sera dispensée au personnel identifié. Cette formation permettra à ce personnel d'analyser le besoin d'IA, de planifier et de planifier l'IA, de préparer listes de contrôle d'audit, mener une IA et documenter et rapporter leurs observations au sommet gestion.

AUDIT INTERNE

Nos experts superviseront la conduite de l'audit interne par votre équipe d'audit interne. Cet audit interne identifiera les lacunes encore existantes dans le système et démontrera le niveau de préparation à faire face à l'audit de certification. Cet audit donne à l'organisation une chance de identifier et rectifier toutes les non-conformités avant de procéder à l'audit de certification. Le sommet la direction est informée des conclusions de l'audit interne.

TOPCERTIFIER
www.topcertifier.com

ANALYSE DES CAUSES PROFONDES (RCA) ETACTIONS CORRECTIVES

Toutes les non-conformités identifiées lors de l'audit interne, des audits clients ou tiers, ou du Méthodologie d'évaluation et de traitement des risques, registre des risques Registre des incidents, vulnérabilité Rapport d'évaluation et de test d'intrusion (VAPT), attaques de logiciels malveillants, registre des temps d'arrêt, réseau problèmes, contrôles d'accès, registre des actifs, rapports d'évaluation des risques de tiers, informations CIA la classification, les attaques internes et externes et toute autre source doivent être répertoriées. RCA sera réalisé à l'aide de techniques telles que les méthodes Brainstorming et Fish-Bone. Le correctif optimal des actions sont mises en œuvre. L'efficacité de ces actions est documentée et examinée via un Rapport d'action corrective (CAR).

RÉUNION DE REVUE DE GESTION (MRM)

Le MRM est l'occasion pour toutes les parties prenantes du SMSI de se réunir à intervalles réguliers pour examiner, discuter et planifier des actions sur les points ci-dessous de l'ordre du jour.

- Efficacité du système de gestion actuel en ce qui concerne le SMSI
- Plans et dossiers d'évaluation et de traitement des risques
- Résultats sur la CIA (Confidentiality Integrity & Availability) de l'information
- Constatations d'audit et non-conformités de toutes sources
- Plan d'actions correctives pour résoudre tous les éléments non soldés
- Améliorations continues apportées au système
- Ressources et formations requises
- Aspects statutaires et conformité

AUDIT DE CERTIFICATION : ÉTAPE 1

Lorsque le niveau de préparation a atteint des niveaux adéquats, le processus de certification commence. Un auditeur désigné par l'organisme de certification (OC) vérifie la norme exigences via un audit de niveau 1. Cela implique que l'auditeur examine les politiques, les processus, SOP, SOA, enregistrements opérationnels critiques, enregistrements IA et MRM. Tout écart majeur par rapport aux CB les attentes seront notifiées à ce stade pour apporter les corrections nécessaires. Cela réduit les risques de non-conformités majeures lors de l'audit de certification. Le certificateur TOP assurera la liaison avec toutes les parties prenantes et superviser le bon déroulement de l'audit.

TOPCERTIFIER
www.topcertifier.com

AUDIT DE CERTIFICATION : ÉTAPE 2

Une fois l'audit de l'étape 1 réussi, l'auditeur se concentre sur un audit détaillé du rapport et documentation du système de gestion de la sécurité de l'information de l'organisation. TOPCertifier aurait formé votre personnel aux exigences d'audit et en toute confiance face à l'audit. Nos experts seront présents pour vous assister dans tous les moyens nécessaires au bon déroulement fonctionnement du contrôle. TOPCertifier aidera votre équipe à clôturer toute non-conformité identifiés lors de l'audit. Après avoir réussi l'audit de certification, TOPCertifier assurera la liaison avec toutes les parties prenantes pour rédiger, approuver et publier le certificat final.

POURSUITE DE LA CONFORMITÉ

TOPCertifier fera partie du parcours de conformité de votre organisation et vous assistera régulièrement intervalles avec les formations nécessaires, le support et les mises à jour du système, les audits internes et externes et le renouvellement régulier de votre certification.