1

Support de présentation

Durée : 1 heure
Date : 10/04/2020
Auteur : Jérôme Thémée
Animateurs : Alexandre Jawor, Ibrahima Bass

Formations, certifications, mastère en cybersécurité made in FR/EU
En savoir plus : https://esdacademy.eu/

ESD Cybersecurity Academy
10 rue de Penthièvre 75008 PARIS
08 05 62 60 00
contact[a]esdacademy.eu

Sommaire

Le webinar

Le webinaire :

- ***titre*** : Tour d'horizon de la norme ISO 27001;
- ***objectif*** : Comprendre les principes fondamentaux associés à la norme ISO 27001;
- ***cible*** : DSI, RSSI, Risk Manager, Ingénieur SI & SSI.
- ***temps*** : 1h ;
- ***reprend la formation ECA*** : ;

L'ESD academy

Formations, certifications, diplôme en cybersécurité.

- l'ESD academy est une organisation créée en 2015 dont l'objectif est d'apporter des **formations**, des **certifications** et un **mastère** en cybersécurité #MadeInFrance, #EU;
- formation pro disponible chez M2I et en ligne; (https://www.m2iformation.fr/)
- le mastère est accessible à Paris, Rennes, Nantes, Lille, La Réunion et en ligne en septembre (écoles Aston, ENI, Expernet, IT-akademy).

Fondée en 2015, l'ESD academy a pour mission d'apporter des formations, des certifications et un mastère en cybersécurité pour les organisations francophones et européenne.

Notre objectif est clairement identifié, concurrencer les acteurs étrangers dans la formation et la reconnaissance en sécurité des systèmes d'information. Pour y arriver nous regroupons autour d'un label, des experts du domaine (étatiques et privés) pour de la création de contenu et l'enseignement.

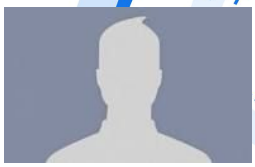
Partie d'un modèle startup, nous dépassons les 500 personnes formés en 2018 dans les domaines de l'offensif, défensif et de la gouvernance pour des clients stratégiques dans le secteur de la cybersécurité française.

La liste des formateurs agréés ESD academy se trouve ici :

https://esdacademy.eu/listeformateurs

Animateurs

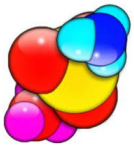
Animateurs



- Alexandre JAWOR
  - Fondateur @ ESD academy
  - Consultant en sécurité de l'information

- Ibrahima Bass
  - CSO @ Capgemini Financial Services France
  - Formateur @ ESD academy

Le webinar



Folding@home

- Aidons la recherche à combattre le #COVID19;
- covid-19 ESD academy : La team ESD arrive dans le top 10.000 en 2802e place sur plus de 246.000 équipes 👍. Avec 29 membres actuellement;
- **tutoriel vidéo** : https://lnkd.in/gR47NsV #cybersecurité #aidons
- **tutoriel .pdf** : https://lnkd.in/gzKyn4y

Équipe ESD academy : 250484
Lien : https://foldingathome.org/

Sommaire

1. Introduction, définitions et cadre d'utilisation de la norme ISO 27001

Introduction - ISO

- L'ISO (Organisation internationale de normalisation) est une organisation internationale non gouvernementale, indépendante, dont les 164 membres sont les organismes nationaux de normalisation.

- Par ses membres, l'Organisation réunit des experts qui mettent en commun leurs connaissances pour élaborer des Normes internationales d'application volontaire, fondées sur le consensus, pertinentes pour le marché, soutenant l'innovation et apportant des solutions aux enjeux mondiaux.

1. Introduction, définitions et cadre d'utilisation de la norme ISO 27001

Norme vs Réglementation

- Un amalgame peut être fait entre la notion de norme et de réglementation.
- La norme est un document de référence approuvé par un institut de normalisation. Dans la plupart des cas, se conformer aux normes n'est pas obligatoire.
- La réglementation est créée par des autorités administratives (Etat, Sénat, collectivités, etc.). Son application est imposée.

1. Introduction, définitions et cadre d'utilisation de la norme ISO 27001

Système de management

- Un ***système de management***, est un ensemble d'éléments corrélés au sein d'un organisme. Ils sont utilisés pour établir des processus afin d'atteindre des objectifs.

- Ces objectifs sont préalablement définis par la direction en déclinaison de la politique de l'organisme.

1. Introduction, définitions et cadre d'utilisation de la norme ISO 27001

Zoom sur la norme ISO 27001

- La norme ISO/CEI 27001 porte sur le management de la sécurité et de l'information.
- Elle tire ses origines de la norme britannique BS 7799-2:2002 « Technologie de l'information – Guide pratique pour le management de la sécurité de l'information », dont la première version a été publiée en 1999.
- En 2005, l'ISO adopte et améliore cette norme pour donner naissance à la norme ISO/CEI 27001. En 2013, celle-ci a été révisée, se rapprochant d'une structure similaire aux autres normes de systèmes de management (ISO 9001, ISO 14001...).

1. Introduction, définitions et cadre d'utilisation de la norme ISO 27001

Zoom sur la norme ISO 27001

- Comme cela se produit de temps à autre, la norme internationale existante, ISO/IEC 27001:2013, a été adoptée comme EuroNorm Standard et devient EN ISO/IEC 27001:2017.
- La version EN ISO/IEC27001:2017 est donc une nouvelle version européenne de la norme qui inclut l'approbation par le CEN/Cenelec.
- La nouvelle version de la norme n'introduit cependant pas de nouvelles exigences.

CEN : Comité européen de normalisation / électronique (composé de 30 pays européen)

1. Introduction, définitions et cadre d'utilisation de la norme ISO 27001

Zoom sur la norme ISO 27001

- La norme ISO/CEI 27001:2013 spécifie les exigences relatives à la mise en œuvre, le maintien en condition opérationnel, la mise à jour et l'amélioration continue d'un SMSI (Système de management de la sécurité de l'information).

- Elle définit également une gestion globale et le cadre de contrôle afin de traiter les risques liés à la sécurité de l'information.

- Les exigences présentes au sein de l'ISO/CEI 27001:2013 couvre tous les types d'organisations, quel que soit son type, sa taille et sa nature.

1. Introduction, définitions et cadre d'utilisation de la norme ISO 27001

Zoom sur la norme ISO 27001

- La norme ISO27001:2013 est orientée processus et applique donc par logique une démarche d'amélioration continue de type PDCA.
- La mise en oeuvre d'un Système de Management de la Sécurité de l'Information ne se déroulant en une seule et unique phase, l'implémentation de cette même démarche est donc nécessaire à son bon fonctionnement.

1. Introduction, définitions et cadre d'utilisation de la norme ISO 27001

Zoom sur la norme ISO 27001

- Quelle que soit la structure qui la met en place, la certification ISO 27001 apporte tout un tas d'avantages.
- La protection des informations des entreprises étant un enjeu fondamental, un prestataire pouvant attester de garanties en la matière sera préféré à un autre.
- Bénéficier de la norme ISO 27001 est une excellente façon de certifier une sécurisation globale de la sécurité de l'information sur un périmètre défini. C'est un facteur de confiance, elle représente un message fort et convaincant auprès de ses utilisateurs actuels et futurs.

1. Introduction, définitions et cadre d'utilisation de la norme ISO 27001

Zoom sur la norme ISO 27001

- Voici quelques objectifs de mise en oeuvre de la norme ISO 27001 :
    - Remporter de nouvelles affaires et fidéliser une clientèle existante
    - Éviter les pertes et pénalités financières associées aux violations des données
    - Protéger et améliorer sa réputation
    - Se conformer aux exigences légales, réglementaires et contractuelles
    - Obtenir une opinion indépendante sur son niveau de sécurité
    - Garantir la sécurité de l'information et des données sensibles,
    - Identifier les risques et mettre des contrôles en place pour les gérer ou les éliminer
    - Etc...

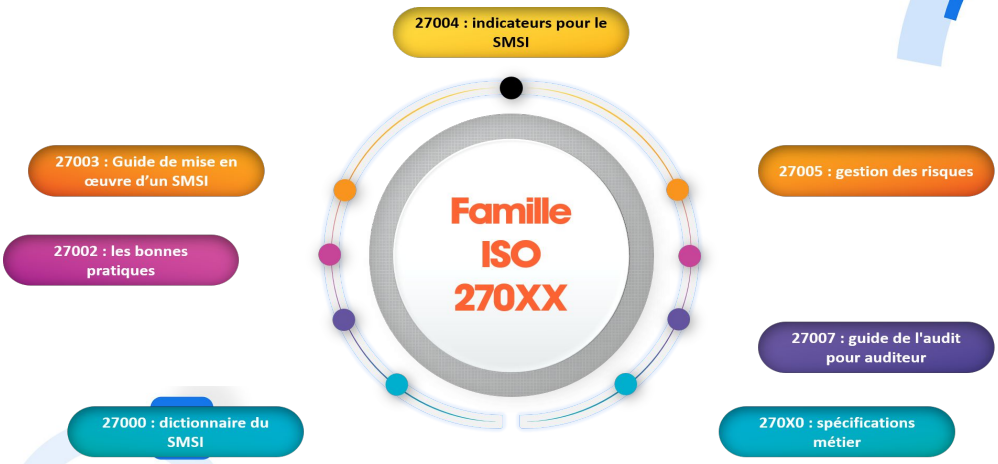
ISO 27001 et SMSI

- Une organisation peut faire le choix d'implémenter un SMSI sans forcément avoir comme finalité l'obtention de la norme ISO 27001.
- Cela reste une très bonne pratique montrant l'intérêt de la direction vis-à-vis des sujets de la sécurité de l'information et permettant un alignement dans sa construction avec les exigences de la présente norme.

Sommaire

2. La famille ISO 2700X

Tour d'horizon de la famille ISO 2700X



2. La famille ISO 2700X

ISO 27000

- La norme ISO 27000 fournit un aperçu de la famille des normes du SMSI.
- Elle définit les termes et expressions utilisés dans ces normes.
- Elle fournit une introduction aux systèmes de management de la sécurité de l'information.
- Elle propose une brève description du processus Plan-Do-Check-Act.

2. La famille ISO 2700X

ISO 27002

- L'ISO/CEI 27002:2013 donne les lignes directrices en matière de normes organisationnelles relatives à la sécurité de l'information et des bonnes pratiques de management de la sécurité de l'information.

- Ce document permet aux organisations de sélectionner les mesures nécessaires et d'avoir une vue plus clair sur celles-ci dans le cadre de processus de mise en œuvre d'un SMSI selon l'ISO/CEI 27001.

2. La famille ISO 2700X

ISO 27003

- La Norme ISO 27003 se concentre sur les aspects critiques nécessaires à une mise en œuvre réussie d'un SMSI.
- La norme ISO 27003 reprend la structure de la norme ISO 27001 en y précisant :
  - Activité requise (rappel de l'exigence de la norme)
  - Explication (précision de l'attente vis-à-vis de l'exigence)
  - Recommandations de mise en place
  - Autres informations

La norme donne des recommandations sur la façon de convaincre la direction, ainsi que les différents concepts pour la conception et la planification d'un projet SMSI dont la réalisation sera un succès garanti.
Cette Norme internationale fournit des lignes directrices pratiques de mise en œuvre et apporte des informations complémentaires pour :
l'établissement, la mise en oeuvre, l'exploitation, la surveillance, le réexamen, la mise à jour et l'amélioration d'un SMSI selon l'ISO/CEI 27001.

2. La famille ISO 2700X

ISO 27004

- La Norme ISO 27004 fournit des éléments sur l'élaboration et l'utilisation de mesures afin d'évaluer l'efficacité d'un SMSI.
- Son application reste facultative au même titre que l'ISO 27002, l'implémenteur pourra y sélectionner ce qui lui paraît le plus approprié vis-à-vis du contexte.

La norme est divisé en 2 parties :

1) Les principes de base pour mettre en place les indicateurs
2) Des annexes plus concrètes proposant une liste d'indicateurs couvrant les articles de l'ISO 27001 ainsi que plusieurs mesures de sécurité de l'Annexe A

Les objectifs de mise en place des tableaux de bord :

- Démontrer le niveau de conformité d'une organisation vis à vis du référentiel de ses obligations (légales, réglementaires, etc.)
- Permettre l'identification de problèmes de sécurité insoupçonnés ou non détectés à ce

- jour
- Améliorer la faculté à répondre aux besoins en reporting de la Direction
- Fournir des éléments pour le processus de gestion des risques de la sécurité de l'information, audits du SMSI et revues de Direction

2. La famille ISO 2700X

ISO 27005

- La Norme 27005 contient les lignes directrices relatives à la gestion des risques en sécurité de l'information.
- Elle vient en appui des concepts généraux énoncés dans l'ISO/CEI 27001 et est conçue pour aider à la mise en place de la sécurité de l'information basée sur une approche de gestion des risques.

2. La famille ISO 2700X

ISO 27007

- La Norme ISO 27007 fournit des lignes directrices permettant d'aider les auditeurs qu'ils soient internes ou externes à remonter des non-conformités ainsi qu'à contrôler que le SMSI est correctement développé.
- La norme ISO 27007 a comme base la norme ISO 19011 (permettant d'auditer les systèmes de management) et vient y ajouter des spécificités propre aux SMSI.
- Une annexe est disponible reprenant clause par clause la 27001 en précisant les différentes preuves à recueillir pour en vérifier la conformité.

- Une partie des articles de la norme ISO 27007 renvoi vers la norme ISO 19011
- Cette norme peut être intéressante pour les implémenteurs qui y trouveront toutes les informations nécessaires pour réaliser les audits internes
- La norme ISO 27007 ne traite que les aspects propre au système de management. Les contrôles des mesures de sécurité sont évoqués dans la norme ISO 27008.

2. La famille ISO 2700X

ISO 27008

- La Norme ISO 27008 décrit le processus destiné à contrôler l'efficacité des mesures de sécurité. Les systèmes d'information étant en perpétuelle évolution, certaines mesures de sécurité mise en oeuvre peuvent perdre de leurs efficacités dans le temps.

- Les revues passent par 3 grandes approches :
  - Les examens (politiques, procédures, etc..)
  - Les entrevues (rencontre avec les différents intervenants à auditer)
  - Les tests (vérification de l'efficacité de la mesure)

Elle diffère de la norme ISO 27007 qui est davantage axée sur le fonctionnement du Système de Management que sur l'implémentation des mesures de sécurité.
La norme ISO 27007 dit qu'il faut élaborer un "Plan de revue" (périmètre exact de la revue, les détails des mesures de sécurité qui seront contrôlées et la façon de les contrôler)
De nombreux apports sont liés à la revue des mesures de sécurité :

- Comprendre les impacts potentiels des vulnérabilités et des menaces
- Identifier les problèmes potentiels de sécurité
- Priorité les actions de sécurisation

- Vérifier les actions déjà décidés pour sécuriser le système
- Aider les arbitrages budgétaires

2. La famille ISO 2700X

Tour d'horizon de la famille ISO 270XX

- La famille des normes ISO 2700X peut donc permettre d'accompagner une organisation souhaitant obtenir des informations complémentaires sur l'implémentation et le maintien en condition opérationnel de son SMSI.

- De plus, d'autres normes de la famille ISO 270XX peuvent venir en complément de celles-ci (exemple : ISO 27017, 27035, 27037)

2. La famille ISO 270XX

ISO 27017

- La Norme 27017 affine certaines mesures de sécurité de l'ISO 27002 pour lui faire tenir compte de la notion de "Cloud" et y ajoute de nouvelles mesures spécifiques à ce domaine.
- Au sein de la première partie cette norme l'enrichissement des mesures de sécurité reprend les mesures de sécurité de l'ISO 27002 en présentant 2 cas de figure :
    - La mesure de sécurité de l'ISO 27002 spécifiée est applicable en l'état aux fournisseurs "Cloud" alors que la 27017 se contente de la valider.
    - Soit la mesure de sécurité mériterait quelques précisions spécifiques aux fournisseurs "Cloud", dans ce cas, la norme apporte ces spécificités.
- La seconde partie de la norme ajoute des mesures de sécurité complémentaires non-présentes au sein de l'ISO 27002 et propre au contexte "Cloud".

Exemple de la seconde partie de la norme ISO 27017 :

- Suppression des actifs
- Cloisonnement des réseaux virtuels
- Durcissement des machines virtuelles
- Supervision des services Cloud
- etc..

2. La famille ISO 270XX

ISO 27035

- La Norme 27035 fournit une approche structurée et planifiée pour :
    - Déctecter, signaler et évaluer les incidents de sécurité de l'information.
    - Détecter, signaler et évaluer les vulnérabilités de sécurité de l'information.
    - Améliorer en permanence la sécurité de l'information au travers de la gestion des incidents et des vulnérabilités.

- Elle fournit les lignes directrices pour la gestion des incidents de sécurité de l'information ainsi que des conseils aux organisations externes fournissant des services de gestions des incidents de sécurité de l'information.

Cette norme présente plusieurs avantages :

- Améliorer la sécurité de l'information
- Réduire les conséquences sur l'activité
- Renforcer la prévention d'incident
- Assurer la recevabilité des preuves
- Mettre à jour l'appréciation des risques
- Fournir un axe de prévention et de sensibilisation

2. La famille ISO 270XX

ISO 27037

- La Norme 27037 s'intitule : Lignes directrices pour l'identification, la collecte, l'acquisition et la préservation de preuves numériques.

- L'ISO 27037 aborde 3 sujets principaux :

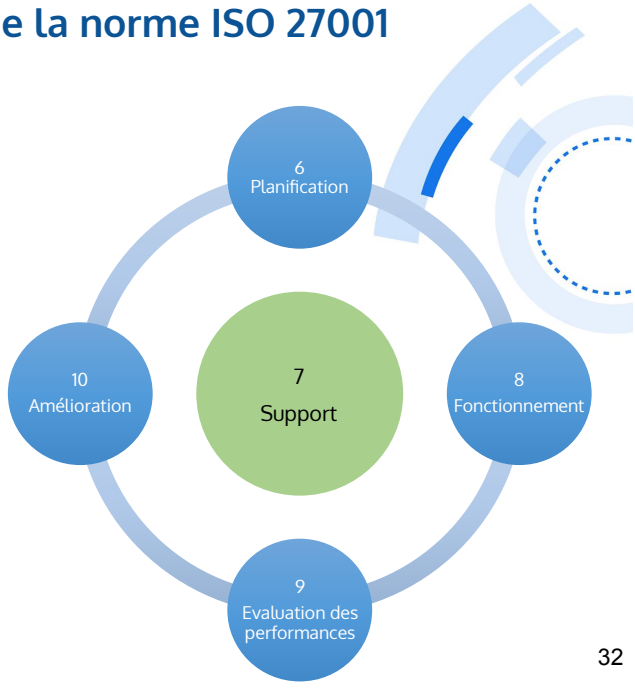
    - Les généralités, qui sont composés des principes de base de la gestion des preuves.
    - Des exemples permettant d'apporter des cas pratiques à la collecte, au transport et au stockage des preuves numériques.
    - Des annexes apportant des précisions complémentaires.

Sommaire

3. Présentation de la norme ISO 27001

4 Contexte

5 Leadership



3. Présentation de la norme ISO 27001

Introduction

- Les exigences fixées dans la Norme ISO 27001 sont génériques et prévues pour s'appliquer à toute organisation, quel que soit son type, sa taille et sa nature.

- Il n'est pas admis qu'une organisation s'affranchisse de l'une des exigences spécifiées aux Articles 4 à 10 lorsqu'elle revendique la conformité à la présente norme.

3. Présentation de la norme ISO 27001

Introduction

- La norme rappel que les exigences présentées dans la norme ne reflète pas leur importance, ni l'ordre dans lequel elles doivent être mises en oeuvre.

3. Présentation de la norme ISO 27001

4 - Contexte

- Dans cet article l'objectif est l'analyse du contexte de l'organisme afin d'en définir le domaine d'application pour le SMSI.
- L'organisation devra donc prendre en considération ses enjeux externes et internes pertinents compte tenu de sa mission et qui influent sur sa capacité à obtenir les résultats attendus pour son SMSI.
- Elle devra en même temps penser aux exigences demandés/imposées par les différentes parties intéressées concernant la sécurité de l'information.

3. Présentation de la norme ISO 27001

5 - Leadership

- Au travers les différentes exigences de l'article "Leadership", la direction affirme son engagement en faveur du SMSI.

- Elle doit entre autre fournir les ressources nécessaires, soutenir les personnes pour qu'elles contribuent à l'efficacité du SMSI, s'assurer que les responsabilités des rôles concernés par la sécurité de l'information sont attribuées et communiqués et veiller à ce qu'une politique et des objectifs en matière de sécurité de l'information soient établi et compatibles avec l'orientation stratégique de l'organisation.

3. Présentation de la norme ISO 27001

6 - Planification

- L'organisation doit fixer ses objectifs, définir et appliquer un processus d'appréciation des risques de sécurité de l'information. Cela passe en autre par l'établissement et la mise à jour de ses critères d'acceptation des risques, les critères de réalisation des appréciations des risques.

- Elle devra aussi définir et planifier un processus de traitement des risques pour la sécurité de l'information.

- La partie planification comprend (dans la partie traitement des risques) la réalisation d'une déclaration d'applicabilité basée sur l'Annexe A de la norme ISO 27001.

3. Présentation de la norme ISO 27001

6 - Planification - Zoom sur la DDA

- Lors de sa déclaration d'applicabilité, l'organisation devra prendre en considération plusieurs éléments :
    - La politique de sécurité
    - Le périmètre du SMSI
    - L'appréciation des risques
    - La notion de transitivité avec les exigences de la norme ISO 27001.

3. Présentation de la norme ISO 27001

7 - Support

- Dans l'article "Support", 5 éléments sont essentiels :
  - *Les ressources* (identifier et fournir les ressources nécessaires)
  - *Les compétences* (déterminer les compétences nécessaires et s'assurer de celles-ci sur la base d'une formation ou d'une expérience appropriée)
  - *La sensibilisation* (Politique de sécurité de l'information)
  - *La communication* (déterminer les besoins en communication interne et externe pertinents pour le SMSI)
  - *Les informations documentées* (création et mise à jour, maîtrise des informations documentées)

Ressources : L'organisation doit identifier et fournir les ressources nécessaires à l'établissement, la mise en œuvre, la tenue à jour et l'amélioration continue du système de management de la sécurité de l'information.

Communication :a) sur quels sujets communiquer; b) à quels moments communiquer; c) avec qui communiquer; d) qui doit communiquer; et e) les processus par lesquels la communication doit s'effectuer

Maîtrise des informations documentées : Cycle de vie documentaire (cartouche avec identification et description) , disponibles et convient à l'utilisation ou et quand elles sont nécessaires, correctement

protégées (CID)

3. Présentation de la norme ISO 27001

8 - Fonctionnement

- L'organisation doit au sein de cet article planifier, mettre en oeuvre et contrôler les processus nécessaires à la satisfaction des exigences liés à la sécurité de l'information ainsi que les plans pour atteindre ses objectifs de sécurité.

- De plus la norme demande la réalisation d'une appréciation des risques de sécurité de l'information à des intervalles planifiés ou quand des changements significatifs apparaissent.

- Elle devra pour finir mettre en oeuvre le plan de traitement des risques de sécurité de l'information.

3. Présentation de la norme ISO 27001

9 - Evaluation des performances

- L'organisation doit dans cet article définir un ensemble d'indicateurs capable de lui fournir des informations sur les performances et l'efficacité de son SMSI.
- Des audits internes doivent être menés à des intervalles planifiés dans le but de recueillir des informations permettant de valider un certain nombre de points sur son SMSI (conformité, efficacité de sa mise en oeuvre et de sa tenue à jour).
- La notion de revue de direction y est introduite lui permettant de mieux gérer et d'adapter son SMSI (modifications des enjeux internes et externes, retour des performances, non-conformités et actions correctives, retours des parties intéressées, résultats d'appréciation et des risques et avancement du plan de traitement, opportunités d'amélioration continue).

KPI :

- ce qu'il est nécessaire de surveiller et de mesurer, y compris les processus et les mesures de sécurité de l'information;
- les méthodes de surveillance, de mesurage, d'analyse et d'évaluation, selon le cas, pour assurer la validité des résultats;
- quand la surveillance et les mesures doivent être effectuées;
- qui doit effectuer la surveillance et les mesures;
- quand les résultats de la surveillance et des mesures doivent être analysés et évalués; et
- qui doit analyser et évaluer ces résultats

3. Présentation de la norme ISO 27001

10 - Amélioration

- Dans l'article 10, la norme impose de réagir vis-à-vis d'une non-conformité, d'effectuer une action pour éliminer les causes de celle-ci puis de réviser l'efficacité de toute action corrective mise en oeuvre.

- L'amélioration continue étant l'un des points les plus importants au sein d'un système de management.

- Le SMSI doit donc être en amélioration constante, adapté aux besoins changeants, être pertinent, efficace, et être compatible et aligné aux objectifs de sécurité de l'information de l'organisation.

Sommaire

4. Problématique de l'approche séquentielle normative

- L'approche consiste à suivre scrupuleusement les exigences de la norme (de l'article 4 jusqu'à l'article 10), dans l'ordre des chapitres :

1. Description du contexte, conception du périmètre et de la politique de sécurité;
2. Appréciation des risques;
3. Sélection des mesures de sécurité dans la déclaration d'applicabilité;
4. Rédaction du plan de traitement des risques et implémentation des mesures de sécurité nécessaires;
5. Contrôle du bon fonctionnement des mesures de sécurité;
6. Mise en place d'un audit interne;
7. Revue du SMSI
8. Action d'amélioration

4. Problématique de l'approche séquentielle normative

- Si cette démarche répond bien aux exigences de la norme, elle n'est pas pour autant viable, d'un point de vue strictement pratique, car elle oublie de prendre en compte certains paramètres :
    - La réalité du terrain
    - Les mesures déjà existantes
    - La définition des priorités
    - La nécessité de paralléliser les tâches
    - Certaines tâches manquantes

Sommaire

5. L'approche SMSI en mode "Projet"

- Prendre toute la liberté nécessaire pour garantir le succès du projet, en respectant trois contraintes :
    - **Exigences de la norme** : Le SMSI doit satisfaire toutes les exigences de l'article 4 à 10 de la norme, sans exception.
    - **Le modèle PDCA :** Les fonctions du SMSI doivent respecter le modèle *Plan, Do, Check, Act,* tant au niveau global qu'au niveau des processus, ou à celui des mesures de sécurité.
    - **Cohérence générale :** Il doit y avoir une cohérence entre le périmètre du SMSI, la politique de sécurité, l'appréciation des risques et les mesures de sécurité effectivement mises en place.
- Peu importe dans quel ordre, seront montées les différentes briques du projet, pourvu qu'à l'arrivée, le SMSI satisfasse ces trois contraintes fondamentales.

5. L'approche SMSI en mode "Projet"

Mais comment procéder ? par ou commencer ? …. ?

- Phase 1 : analyse préalable
  - Etudes d'opportunité
  - Etat des lieux
  - Etudes des options (politiques et périmètre)

- Phase 2 : mise en place de la structure de base
  - Gouvernance de la sécurité
  - Documentation
  - Audit interne et suivi des actions
  - Formation et sensibilisation
  - Indicateurs

5. L'approche SMSI en mode "Projet"

Mais comment procéder ? par ou commencer ? …. ??

- Phase 3 : mise en place des processus du SMSI
  - Appréciation des risques
  - Adaptation des mesures de sécurité existantes
  - Implémentation des mesures de sécurité manquantes
  - Revue

- Phase 4 : Démarrage du SMSI
  - Revue du SMSI
  - Préparation à l'audit
  - Audit à blanc
  - Action corrective et préventive

5. L'approche SMSI en mode "Projet"

Principales erreurs à éviter (RETEX)

- Se lancer sans l'appui de la direction générale
- Travailler seul
- Ne pas mettre en place la structure de base
- Se tromper de périmètre
- Déclaration d'applicabilité
- Faire « de la procédure »

Sommaire

5. L'approche SMSI en mode "Projet"

Démonstration

La formation

Notre formation

- accessible dans les centres M2I formation pour les profesionnels (35 centres en France);
- plusieurs financements possibles, CPF, Plan de formation, etc.
- formation type “fondamentaux“ dans notre mastère présent à Paris sud, Lille, Rennes, Nantes, La Réunion;
- disponible en ligne;
- examen et supports réalisés par des professionnels reconnus

Certification

Nos badges pour *Intégration SMSI et l'ISO 27001*

- étude de cas et QCM;
- 120 minutes;
- évaluer les compétences dans la compréhension des différentes phases d'un test d'intrusion, ainsi que les aspects juridiques et contractuels;

- la liste de nos certifiés sont disponibles à cette adresse **https://badges.esdacademy.eu/**

La formation

Nos prochains webinaire (lien sur *https://esdacademy.eu*)

- 05/06 - État de l'art du PCA avec ISO 22031 -
- 12/06 - Juridique et Cybersécurité -
- 19/06 - Intégrer le DevSecOps dans un SI -

Liste des prochains webinaire :

17/04 - Techniques de hacking avancées - https://meeting.zoho.eu/meeting/register?sessionId=1295492647
24/04 - Langages et bibliothèques pour un test d'intrusion - https://meeting.zoho.eu/meeting/register/embed?sessionId=1245549196
30/04 - Présentation de la cyber défense - https://meeting.zoho.eu/meeting/register/embed?sessionId=1243632008
07/05 - État de l'art de l'investigation numérique (Digital Forensics) - https://meeting.zoho.eu/meeting/register/embed?sessionId=1290215890
15/05 - État de l'art de l'analyse de malware - https://meeting.zoho.eu/meeting/register/embed?sessionId=1269089823
29/05 - ISO 27001 et la conformité SSI - https://meeting.zoho.eu/meeting/register/embed?sessionId=1270875049
05/06 - État de l'art du PCA avec ISO 22031 - https://meeting.zoho.eu/meeting/register/embed?sessionId=12535730

04
12/06 - Juridique et Cybersécurité - https://meeting.zoho.eu/meeting/register/embed?sessionId=1221256661
19/06 - Intégrer le DevSecOps dans un SI - https://meeting.zoho.eu/meeting/register/embed?sessionId=1274668656

Facebook

Twitter

LinKedIn

Instagram

Équipe ESD academy : 250484

Crédit : Alexandre Jawor et Ibrahima Bass
Liens utiles : https://esdacademy.eu, https://badges.esdacademy.eu

Formations, certifications, mastère en cybersécurité made in FR/EU
En savoir plus : https://esdacademy.eu/

ESD Cybersecurity Academy
10 rue de Penthièvre 75008 PARIS
08 05 62 60 00
contact[a]esdacademy.eu