Formation
« ISO27004 / Indicateurs et tableaux de bord cybersécurité »

Réf : ISO27004

Que ce soit un avion ou un organisme, il est toujours possible de conduire celui-ci avec peu d'informations, mais cela sera moins efficace, voire dangereux. Dans le cas de la gestion de la sécurité de l'information, le pilotage d'une telle activité consiste à prendre des décisions et ce à plusieurs niveaux. Ce peut être la décision de modifier une fréquence de scan antivirus ou encore, à un niveau plus stratégique, l'arbitrage en faveur d'une redistribution des budgets.

Si elles ne relèvent pas du même niveau d'arbitrage, ces décisions ont ceci en commun qu'elles se font de façon plus éclairée si elles sont prises en fonction d'informations fiables et pertinentes. La prise de décision est d'autant meilleure qu'elle peut s'appuyer sur des indicateurs concrets et pertinents.

Les indicateurs stratégiques, regroupés en tableaux de bord, permettent de répondre à ce besoin d'information. Pour ce faire ils doivent être adaptés au profil du lecteur et aux décisions qui sont attendues de lui. En ce sens, les tableaux de bord sont à rapprocher des principes de communication dont la finalité est d'obtenir une action de la cible de cette communication.

Un tableau de bord pertinent se doit également d'être réaliste, ce qui implique que son coût soit maitrisé et en rapport avec les enjeux qu'il permet d'arbitrer. L'objectif étant, non pas de construire des indicateurs trop complexes et coûteux à produire, ce qui contribuerait à consommer de la valeur plutôt qu'à sécuriser celle-ci…

Objectifs

- Comprendre ce qu'est un indicateur, ce en quoi il est nécessaire à une gestion efficace de la sécurité de l'information, comment en faire un outil de communication vis-à-vis de toutes les parties prenantes, comment mettre en place des tableaux de bord adaptés à un contexte
- Savoir concevoir des indicateurs pertinents et réalistes dans le contexte de son organisme
- Savoir concevoir des indicateurs conformes aux exigences de la norme ou du référentiel suivi
- Savoir tirer des informations utiles des indicateurs en produisant des tableaux de bord pour surveiller et améliorer un SMSI, pour prouver sa conformité et améliorer la SSI, et pour communiquer

Durée & horaires

- 1 jour soit 7 heures
- Horaires : de 9h30 à 12h00 et de 13h30 à 17h30/18h00.

Nombre de participant

- Minimum 6 participants – Maximum 24 participants

Public visé

- Personnes chargées de concevoir des indicateurs sécurité, de les produire, ou de présenter des tableaux de bord.
- Personnes chargées de déployer des indicateurs sécurité
  - RSSI et équipes du RSSI
  - Consultants en sécurité
  - Ingénieurs sécurité.
- Personnes chargées de produire des indicateurs de sécurité
  - Ingénieur de production informatique
  - Chef de projet métier

Pré-requis

- **Avoir suivi la formation "Essentiels ISO27001/ISO27002" ou la formation "RSSI"**
- **ou avoir suivi une formation plus complète à l'ISO27001 comme "ISO27001 Lead Implementer"**
- **ou avoir une connaissance de la SSI et une maîtrise de l'ISO27001 ou des systèmes de management en général**
- **ou être déjà RSSI ou consultant sécurité avec une expérience**

Méthode pédagogique

- **Cours magistral avec des exemples pratiques issus de l'expérience des formateurs.**
- **Exercices pratiques individuels de mise en œuvre d'indicateurs.**

Supports

- **Support de cours au format papier en français**
- **Cahier d'exercices et corrections des exercices**
- **Tous les documents nécessaires à la formation en français ou anglais**
- **Certificat attestant de la participation à la formation**

Modalité d'évaluation de la formation

- **Fiche d'évaluation remise aux stagiaires à l'issue de la formation afin de recueillir leurs impressions et identifier d'éventuels axes d'amélioration**

Certification

- **Cette formation n'est pas certifiante.**

Programme

- Introduction
  - Qu'est-ce qu'un indicateur ?
  - Vocabulaire
- Indicateurs : pourquoi mesurer une activité ?
  - Peut-on piloter sans instruments ?
  - Quelle valeur ajoutée
- Points à mesurer dans le domaine de la SSI
  - Efficience de la sécurité
  - Coût de la sécurité, ou de l'absence de sécurité
  - Conformité aux normes, référentiels, exigences, réglementations
- Approches pour gérer les indicateurs :
  - Travaux issus du monde de la sécurité : ANSSI, ISO, CLUSIF, CIGREF
  - Techniques de communication au service des indicateurs
  - Coût des indicateurs
- Démarche de mise en œuvre
  - Vue d'ensemble
  - Concevoir ses indicateurs
    - Définir ses besoins et ses finalités
    - Définir les moyens de production
  - Produire ses indicateurs
  - Communiquer ses indicateurs
  - Auditer ses indicateurs
- Conseils pratiques
  - Principaux indicateurs à mettre en place
    - Pour un Système d'Information
    - Pour un SMSI
  - Exemples
  - Erreurs à éviter
  - Identifier les solutions simples et efficaces (« quick wins »)
- Présentation de la norme ISO 27004
  - Raison d'être de la norme
  - Processus de mise en œuvre
  - Quels indicateurs pour quel usage
- Exercices