SEC104 - Analyse de risques des données, réseaux et systèmes

Mis à jour le 15-01-2025

Code : SEC104

Unité d'enseignement de type cours

6 crédits

Volume horaire de référence (+/- 10%) : **50 heures**

Responsabilité nationale : EPN05 - Informatique / Véronique LEGRAND

Contact national :

EPN05-Informatique

2 rue Conté
33.1.10A
75003 Paris

Marlène DEFFON
marlene.deffon@lecnam.net

Présentation

Prérequis

Bac+2 Informatique

Objectifs pédagogiques

Lorsqu'une organisation vise l'amélioration continue de sa sécurité informatique, elle peut, en conformité avec le bouquet de norme ISO 27., mettre en place un système de management de la sécurité de l'information (SMSI) et un système de management de la continuité d'activité (SMCA) en s'appuyant sur une méthodologie d'analyse des risques.

Au cœur de l'analyse de risque, l'identification des actifs constitue une étape essentielle. Les données sont un cas d'actifs précieux dont les propriétés relèvent également d'une analyse spécifique vis à vis de la vie privée. Cette analyse peut suivre la méthode PIA proposée par la CNIL.

Une fois les actifs identifiés, l'analyse de risque permet d'appréhender les enjeux de l'organisation et d'identifier un ensemble d'exigences qui font appel à des connaissances organisationnelles et techniques en vue d'élaborer un Système de Management de la Sécurité de l'Information (SMSI). Pour ce faire, l'analyse de risque fait appel à une méthodologie qui en première intention contribue à une maitrise des risques connus et visera à appréhender ces risques avec une bonne connaissance de ses enjeux et menaces, en menant une démarche en alignement avec les autres directions de l'organisation et en mettant en place un plan de traitement des risques. Cette première intention ne prend pas toujours en compte les risques dans l'incertain, qui requièrent une amélioration continue de cette première mise en place.

Les enjeux d'un dispositif de continuité d'activité sont de de survivre à un sinistre et de préserver l'activité de l'organisation, la norme ISO 22301 en décrit les contours qui reposent sur un Système de Management de la Continuité d'Activité (SMCA).

L'objectif de ce cours est de fournir aux apprenants de SEC104 les outils et socles de connaissances pour parvenir à réaliser des missions (fiches métiers génériques).

Compétences

AR

- Savoir mener, argumenter et déployer une politique de sécurité informatique (PSSI) dans une entreprise en lien avec une analyse de risque (AR) des infrastructures et des données avec la compréhension des principales normes en matière de sécurité de l'information, données et IT,
- Mettre en place une hiérarchisation des risques entre eux afin de cibler les actions à mener, générer et gérer un plan d'action (PA),
- Rédiger les documents de gouvernance de la sécurité de l'information (Politique de Sécurité du SI, chartes informatiques, Gouvernance des données),
- Conduire une analyse de risque PIA à l'aide de la cartographie des données (DCP) et des traitements,
- Savoir mettre en place le reporting et les tableaux de bord pour assurer le suivi auprès de RSSI opérationnels,
- Identifier et analyser les risques opérationnels en utilisant les cartographies et audit d'un composant, en interprétant les indicateurs de compromission,
- Prendre en charge les analyses qualitatives et quantitatives menées au travers des audits et traiter les risques,
- Accompagner la mise en conformité aux référentiels de la sécurité du SI (ISO 2700x, RGPD, LPM, HDS, PCI DSSH, HADS, etc.).Savoir mener, argumenter et déployer un

tableau de bord à partir de la PSSI,
- Conduire des audits d'évaluation de conformité réglementaire et le suivi des veilles réglementaires d'un SI ou de l'un de ses composants,
- Répondre aux recommandations d'audit en acquérant une base solide sur les méthodes d'audit stratégiques et techniques au service de l'analyse de risques,

CA

- Faire l'ébauche de scénario à risque afin de mettre à jour les procédures opérationnelles,
- Savoir mener, argumenter et déployer une politique de résilience et de Préparation des TIC pour la Continuité d'Activité (PTCA),
- Concevoir et gérer un système de management de la sécurité (SOC) et de la continuité d'activité (SMCA) du système d'informations et de ses composants, mettre en place une cellule de réponse à incident au sein d'un SOC,
- Savoir mener, argumenter et gérer une réponse à incident en situation ou après sinistres (PRAS),
- Prévenir et anticiper les situations de crise, organiser la gestion des situations d'urgence
- Concevoir des exercices efficaces pour maîtriser la continuité de service et la résilience d'un système d'information.

Conduire une réponse à incident de sécurité en assurant la création de rapports et de feedback.

Programme

Contenu

- Introduction Présentation de la boucle d'analyse et AC de la sécurité informatique d'un SI ***(AR et CA)***
  - Travail personnel : recherche bibliographique sur les analyses de risque
- Temps 1 : Analyse de risques : enjeux, processus et bien informationnels ***(AR)***
  - Cours 1 : Analyse de risques (AR)
  - Cours 2 : Classification
  - TD 1 : Cartographies
  - Cours 3 : Classes de menaces
  - Cours 4 : Audit
  - TD 2 : Audit d'un composant du SI
- Temps 2 : Analyse de risques : SI ***(AR)***
  - Cours 5 : Méthode EBIOS
  - Cours 6 : Application spécifique
  - TD3 : Application spécifique et étude de cas EBIOS
- Temps 3 : Analyse de risques : données ***(AR)***
  - Cours 7 : Méthode PIA
  - TD4 : Application spécifique et cas d'étude PIA
- Temps 4 : AR et CA ***(CA)***
  - Cours 8 : continuité d'activité - incertain
  - Cours 9 : CA et services informatiques
  - Travail personnel : Recherche bibliographique sur une thématique de la continuité d'activité
- Temps 5 : AR et tests ***(CA)***
  - Cours 10 : Réaction aux incidents
  - Cours 11 : Suivi et revue du processus - Amélioration continue (AC)
  - Cours 12 : Essai et exercice
  - TD ou Cyberchallenge

Modalités de validation

- Contrôle continu
- Examen final

Description des modalités de validation

Dossier cahier des charges d'analyse de risque ou d'une analyse de sécurité ou de vulnérabilité et contrôle continu par la notation des travaux dirigés

Ou examen sur table

Ou les 2

Bibliographie

Titre	Auteur(s)
NF EN ISO/IEC 27001, ISSN 0335-3931, mai 2017, Cnam le 05/08/2021	ISO
ISO/IEC 27002:2013, Information technology — Security Techniques — Code of practice for information security controls	ISO
ISO/IEC 27004, Information technology — Security techniques — Information security management — Measurement	ISO
ISO/IEC 27005, Technologies de l'information — Techniques de sécurité — Gestion des risques liés à la sécurité de l'information,	ISO
ISO/IEC 27031, Information technology — Security techniques — Guidelines for information and communication technology readiness for business continuity,	ISO
« Comment organiser une cellule de crise en cas d'attaque cyber ? », INHESJ, Travaux des auditeurs, Cycle « Sécurité des usages numériques », Travaux de la 5e promotion (2014-2015).	BEDARD, Y.,BEGON, J.,MARTIN,B.,EL BOUHATI,N.,SEIMANDI,N.
ANSSI (2018), « La méthode EBIOS Risk Manager ».	ANSSI
ISO/DIS 22398 :2011, ISO/TC 223, (draft) - Societal security — Guidelines for exercises and testing, 2012-05-13	ISO
ISO 31000, Risk management — Principles and guidelines,https://www.iso.org/obp/ui/fr/" \l "iso:std:iso:31000:en	ISO
ISO 22301, Societal security — Business continuity management systems — Requirements,	ISO