

Sessions garanties disponibles

Formation Analyse des risques cyber

Réf. SF34453

De la menace cyber aux décisions de sécurité, structurez une analyse de risques adaptée à votre contexte !

2 j Durée	1 700 € HT Inter / participant	4 300 € HT Intra (≤12 pers.)	12 Sessions à venir
--------------	-----------------------------------	---------------------------------	------------------------

Objectifs pédagogiques

- ✓ Comprendre les spécificités des risques cyber par rapport aux risques SI « classiques »
- ✓ Identifier et cartographier les actifs critiques (données, applications, services, chaînes métier)
- ✓ Décrire des scénarios de menaces cyber réalistes (ransomware, fraude, espionnage, sabotage, etc.)
- ✓ Évaluer la vraisemblance, l'impact et le niveau de risque cyber pour les métiers
- ✓ Prioriser les risques à l'aide de matrices, grilles et critères de décision partagés
- ✓ Situer et utiliser les principales méthodes d'analyse de risques (EBIOS RM, ISO 27005, NIST CSF)
- ✓ Construire un registre de risques cyber et un plan de traitement associé
- ✓ Suivre les risques résiduels, mettre à jour l'analyse et alimenter la gouvernance cyber (comité risques, COMEX, audits)

Public visé & prérequis

Public visé Auditeurs, Chefs de projet, DSI, Responsables de la sécurité des systèmes d'information (RSSI)

Prérequis Connaissances générales en sécurité des systèmes d'information. Une première exposition aux enjeux cyber (RSSI, IT, audit, conformité) est un plus, sans être indispensable.

Programme détaillé

Panorama & fondamentaux des risques cyber

Tendances des menaces cyber : acteurs, motivations, modes opératoires
Typologie des risques cyber : disponibilité, intégrité, confidentialité, traçabilité, image, conformité
Notions clés : scénario de menace, vulnérabilité, probabilité, impact, risque résiduel
Articulation avec la gestion globale des risques (ERM, risques opérationnels, BCP/DRP)

Activités pratiques :

Analyse d'incidents cyber réels et premières réflexions « risques »

Cartographier les actifs et le périmètre cyber

Identification des actifs critiques : données sensibles, applications, infrastructures, services cloud
Prise en compte des parties prenantes : métiers, IT, prestataires, fournisseurs SaaS, infogérants
Cartographie « métier – processus – SI » et identification des dépendances critiques
Classification des actifs et données (sensibilité, criticité métier, exigences réglementaires)

Activités pratiques :

Construction d'une mini-cartographie d'actifs cyber sur le cas fil rouge

Construire les scénarios de menaces et évaluer les risques

Identification des menaces cyber : attaque externe, menaces internes, partenaires, erreurs, pannes
Détection des vulnérabilités : organisationnelles, techniques, humaines, contractuelles
Méthodes de construction de scénarios de risques cyber (approche par scénarios, par actifs, par processus)
Grilles d'évaluation : vraisemblance, impacts métier (financier, image, juridique, opérationnel)

Matrices de criticité, seuils d'acceptabilité et hiérarchisation des risques

Activités pratiques :

Élaboration de 2–3 scénarios de risques cyber et notation collective

Méthodes, référentiels et conformité en analyse de risques cyber

Présentation d'EBIOS Risk Manager : principes, étapes, apports pour l'analyse cyber
ISO 27005 : cadre de gestion des risques liés à la sécurité de l'information
Lien avec ISO 27001 / 27002, NIST Cybersecurity Framework et exigences réglementaires (ex. RGPD, NIS2 selon contexte)
Critères de choix et de combinaison des méthodes dans un contexte d'entreprise
Intégration dans les projets (Build) et les opérations (Run) : analyses de risques récurrentes, revues périodiques

Activités pratiques :

Comparaison de démarches et choix d'une approche adaptée au cas fil rouge

Plan de traitement, pilotage et communication des risques cyber

Options de traitement : réduction, transfert (assurance cyber, externalisation), acceptation, évitement
Construction du plan de traitement : objectifs, mesures de sécurité, responsables, échéances, budget
Articulation avec les contrôles de sécurité (techniques & organisationnels) et les plans de continuité
Registre de risques cyber : structure, mise à jour, liens avec les plans d'action et indicateurs
Communication aux métiers et à la direction : tableaux de bord, cartographies des risques, synthèse COMEX

Activités pratiques :

Élaboration d'un plan de traitement cyber complet à partir du registre de risques

Prochaines sessions

DATE	LIEU	STATUT
18/03/2027	Lyon	Sur confirmation
18/03/2027	Lille	Sur confirmation
18/03/2027	Nantes	Sur confirmation
18/03/2027	à distance	Sur confirmation
22/06/2027	Grenoble	Sur confirmation
22/06/2027	Paris	Sur confirmation

Pourquoi choisir Sparks Formation ?

20 ans d'expertise IT, des formateurs experts et des sessions garanties contre l'annulation.

20 ans
d'expertise

1 068+
formations

11 178
apprenants formés/an

+67
Net Promoter Score

Avis des participants

4,9/5 — 7 avis

William B. — Prévoir l'envoi à chaque participant du livre de CISS au moins un mois avant la formation.

Mickael L. — il est top Romain GARCIA

Votre formateur

Adrien C. — Formateur Gouvernance & Risques

Adrien intervient sur des formations portant sur la gouvernance, les risques et la conformité (GRC). Parmi les formations qui lui sont confiées figurent notamment « Analyse des risques cyber »...

Ils nous font confiance

Cette année notre filière Gouvernance, Risques & Conformité (GRC) a accompagné plus de 30 entreprises dont :

AVEM MÉTROPOLE DE LYON ADISTA ALSTOM ASTEK FRANCE AXA ASSISTANCE FRANCE COMMUNAUTÉ DE COMMUNES DES HAUTS DE FLANDRE CONSORT FRANCE ECONOCOM SERVICES & SOLUTION EGIS +20 autres

Financement & certifications

Cette formation est éligible aux financements OPCO et FNE-Formation. Nos équipes vous accompagnent dans le montage de votre dossier.



Réservez votre place dès maintenant

20 ans d'expertise · 1 000+ formations · NPS +67 · réponse sous 24h ouvrées

0 805 950 800

demande@sparks-formation.com