DMO Mickaël Ouvrard
Le RGPD simple et efficace

5 rue du Stade,
78300 Poissy
FRANCE

Tél : +336 79 71 28 28
mickaelouvrard@dmouvrard.com
https://dmouvrard.com



Formation « Gouverner le risque cyber : les responsabilités des dirigeants de PME et ETI », en 0,5 jour

Version octobre 2026

ACTIVATEUR [N] FRANCE NUM

Mickaël OUVRARD EI – DMOuvrard
5 rue du Stade, 78300 Poissy – FRANCE
mickaelouvrard@dmouvrard.com - +336 79 71 28 28
Entrepreneur Individuel - SIRET : 918 689 720 00012
N° TVA Intracommunautaire : FR24918689720

Sommaire

Édito 2

La formation 2

Durée : 2

Lieu 2

Profil des stagiaires 2

Objectifs pédagogiques 2

Méthodes pédagogiques 3

Méthodes pédagogiques générales 3

Documents fournis : 3

Programme de la formation 3

Module 1 – Enjeux et panorama des risques cyber 3

Module 2 – Le dirigeant face au risque cyber : responsabilités et obligations 3

Module 3 – Les exigences réglementaires et normatives essentielles 4

Module 4 – Construire une gouvernance cybersécurité adaptée à une PME ou une ETI 4

Module 5 – Préparer sa feuille de route cybersécurité 4

Édito

La cybersécurité n'est plus uniquement un sujet informatique. Elle constitue désormais un enjeu de gouvernance, de continuité d'activité, de conformité et de maîtrise des risques.

Face à l'augmentation des cyberattaques, aux exigences réglementaires croissantes et à la dépendance des organisations à leurs systèmes d'information, les dirigeants et décideurs doivent disposer des clés nécessaires pour piloter efficacement le risque cyber.

Cette formation permet de comprendre les responsabilités de la direction, d'identifier les principaux risques, de connaître les exigences réglementaires et de structurer une gouvernance adaptée aux réalités des PME et ETI.

La formation

Durée :

0,5 jour de 3h30.

Lieu

En présentiel (dans vos locaux pour les formations Intra-entreprises) **ou en distanciel** en mode synchrone (stagiaires en visio). Le mode présentiel est privilégié pour plus d'interactivité et d'efficacité.

Pas de frais de déplacement en Eure et en Ile-de-France.

Profil des stagiaires

Directions générales, présidents et dirigeants, DSI, responsables informatiques, directions qualité, directions des risques, responsables conformité, membres de CODIR.

Aucun prérequis technique.

Objectifs pédagogiques

- **Comprendre les enjeux stratégiques** de la cybersécurité.
- **Identifier les principaux risques cyber** auxquels leur organisation est exposée.
- **Comprendre les responsabilités** des dirigeants et des décideurs.
- **Identifier les principales exigences** réglementaires applicables.
- **Définir les composantes essentielles** d'une gouvernance cybersécurité.
- **Structurer une démarche de pilotage** du risque cyber.
- **Définir une feuille de route** de premier niveau.

Méthodes pédagogiques

Méthodes pédagogiques générales

- **Alternance théorie/pratique** dans chaque module.
- **Parties théoriques claires et compréhensibles**.
- Exemples, retours d'expérience, études de cas réels, auto-évaluation de maturité et ateliers pratiques conçus **pour une mise en œuvre simple, rapide et efficace**.
- **Échanges** entre participants, quiz interactifs.
- **Outils applicables dès le lendemain**.

Documents fournis :

- **Support pédagogique complet**.
- **Outils et modèles** : modèle de gouvernance cybersécurité PME/ETI, exemple de comité cyber, cartographie simplifiée des risques cyber, tableau de bord cybersécurité dirigeant, grille d'auto-évaluation de maturité, modèle de feuille de route cyber.
- **Guides pratiques** : guide des responsabilités du dirigeant, synthèse RGPD et cybersécurité, synthèse NIS2 pour les PME et ETI, guide de préparation à une crise cyber.

Programme de la formation

Module 1 – Enjeux et panorama des risques cyber

- **Objectifs :** comprendre pourquoi la cybersécurité est devenue un sujet de direction ; identifier les menaces majeures pesant sur les PME et ETI.
- **Contenu** : L'évolution de la menace (professionnalisation de la cybercriminalité, industrialisation des attaques, impact de la transformation numérique, nouveaux risques liés au télétravail et au cloud) ; les principales menaces (rançongiciels, hameçonnage, fraude au président, compromission de comptes, fuite de données, cyberattaques de la chaîne fournisseurs) ; les conséquences pour l'entreprise (arrêt d'activité, perte financière, perte ou divulgation de données, atteinte à l'image, responsabilité de la direction).
- **Atelier** : analyse rapide d'un scénario réel de cyberattaque en PME.

Module 2 – Le dirigeant face au risque cyber : responsabilités et obligations

- **Objectifs :** comprendre le rôle de la direction dans la maîtrise du risque cyber ; identifier les responsabilités partagées entre Direction, DSI et métiers.
- **Contenu** : pourquoi le risque cyber est un risque d'entreprise (comparaison avec les autres risques stratégiques, place du cyber dans la gestion des risques) ; les responsabilités de la Direction Générale (pilotage, arbitrage, allocation des ressources, contrôle) ; les responsabilités des autres acteurs (DSI, RSSI, managers,

collaborateurs) ; les erreurs fréquentes (déléguer entièrement le sujet à l'informatique, absence de pilotage, manque de sensibilisation).

- **Atelier** : auto-évaluation de la gouvernance actuelle.

Module 3 – Les exigences réglementaires et normatives essentielles

- **Objectifs :** comprendre les principales obligations applicables ; identifier les impacts pour l'organisation.
- **Contenu** : RGPD et cybersécurité (sécurité des données personnelles, violations de données, notification des incidents) ; Directive NIS2 (principes généraux, entreprises concernées, exigences attendues en matière de gouvernance) ; référentiels de référence (ISO 27001, ISO 27002, NIST Cybersecurity Framework, guides de l'ANSSI) ; les attentes des assureurs (authentification multifacteur, sauvegardes, sensibilisation, gestion des incidents).
- **Atelier** : Diagnostic rapide de conformité.

Module 4 – Construire une gouvernance cybersécurité adaptée à une PME ou une ETI

- **Objectifs :** identifier les éléments constitutifs d'une gouvernance efficace ; construire un dispositif proportionné à la taille de l'entreprise.
- **Contenu** : Les piliers d'une gouvernance cyber : gouvernance (sponsoring de direction, Comité Cyber, reporting), gestion des risques (identification des actifs critiques, cartographie des risques, priorisation), politique de sécurité (règles de sécurité, gestion des accès, gestion des prestataires), sensibilisation (formation des collaborateurs, exercices de simulation, communication régulière), indicateurs à suivre (nombre d'incidents, niveau de sensibilisation, taux de conformité, niveau de couverture des risques).
- **Atelier** : Construction d'un schéma de gouvernance cible.

Module 5 – Préparer sa feuille de route cybersécurité

- **Objectifs :** prioriser les actions ; définir une trajectoire réaliste.
- **Contenu** : Les 10 actions prioritaires pour une PME ou une ETI : en gouvernance, en gestion des risques, en protection et en résilience.
- **Livrable** : première feuille de route cyber à 12 mois.