Module de formation
Diriger son entreprise en intégrant les enjeux de cybersécurité dans ses processus et ses projets

Version du 01/12/2024

Formation distancielle adaptée aux besoins, intérêts et disponibilités de l'apprenant

Durée de validité de la version : 1 an renouvelable

A QUI S'ADRESSE CETTE FORMATION ?

Profils du stagiaire

- ★ Dirigeant d'entreprise ou cadre dirigeant

Prérequis

- ★ Aucun prérequis technique
- ★ Remplir le questionnaire de positionnement et d'attentes en complément de l'analyse du besoin préalable à l'inscription

Information : Ce module permet également de se préparer au module suivant : "Développer son entreprise en intégrant la cybersécurité comme levier stratégique d'opportunités"

OBJECTIFS PÉDAGOGIQUES ET COMPÉTENCES VISÉES

Au terme de la formation, le stagiaire sera capable de :

- ★ S'approprier les enjeux et le contexte de la Cybersécurité
- ★ Etre en mesure d'accompagner et d'orienter la gouvernance de la Cybersécurité de son entreprise
- ★ Définir une stratégie de cybersécurité adaptée à son entreprise ou organisation
- ★ Assurer les exigences ou les obligations légales liées à la Cybersécurité et au contexte de son entreprise
- ★ Initier une culture Cyber au sein de l'organisation

Compétence(s) visé(es) :

- ★ Piloter la stratégie globale de cybersécurité de l'entreprise avec une compréhension des menaces actuelles, des enjeux réglementaires (NIS2 RGPD, lois sectorielles) et des implications économiques, en évaluant les risques inhérents et résiduels en alignant les priorités de sécurité sur les objectifs de l'entreprise afin d'assurer la protection des actifs critiques, la résilience organisationnelle et la continuité opérationnelle.
- ★ Superviser et coordonner la mise en place des solutions de cybersécurité en appréhendant les solutions technologiques clés (systèmes de détection d'intrusion, gestion des accès, chiffrement) et en assurant une gestion efficace des projets liés à de la cybersécurité en collaboration avec les responsables IT et métiers pour minimiser les vulnérabilités et garantir la résilience organisationnelle face aux menaces.
- ★ Garantir un niveau de conformité réglementaires et normatives en matière de cybersécurité (NIS 2,RGPD, ISO 27001, PCI DSS, domaine bancaire etc.), en mettant en place des processus internes de suivi et de mise à jour des exigences légales afin d'éviter les sanctions, de préserver la réputation de l'entreprise et de renforcer la confiance des parties prenantes.

CONTENU & PROGRESSION PÉDAGOGIQUE

Jour	Titre de la séquence	Contenu	Méthode pédagogique utilisées
J1 : Date de début	**S1 - Fondamentaux de la cybersécurité**	• Introduction aux enjeux de la cybersécurité • Panorama des cyberattaques : de quoi parle-t-on ? • Le contexte et les enjeux stratégiques de la cybersécurité • Les actifs critiques et leur importance en cybersécurité • Évaluation des besoins de protection de son SI • Collaboration et partage d'information en cybersécurité • Les bonnes pratiques pour une approche méthodique de la Cybersécurité et sa veille inhérente	**Apport théorique (0h30)** Assimiler les fondamentaux en cybersécurité, Capsules vidéos courtes et quiz **Atelier pratique (2h30)** Identifier ses actifs critiques et les prioriser avec méthode dans son contexte d'entreprise **Live Mentor (1h)** Échanger avec un expert sur l'alignement cybersécurité et stratégie, Discussion interactive + Retours d'expérience **Ressources types :** Template de cartographie des actifs à risque, Exemples concrets d'entreprises ayant subi des cyberattaques (études de cas), Checklist "Premières actions cybersécurité pour un dirigeant"

J1+ 1 semaine	**S2 – Sécurité SI : Mise en pratique d'une analyse de risques**	• Introduction à la notion de risque • Les grands écosystèmes de risques : Industriel & distribution / services / Finance & Assurance • Pourquoi analyser et évaluer les risques? • Comment identifier un risque et l'analyser : apports, avantages et inconvénients des méthodes clés • Choix approprié d'une méthodologie et de la personnalisation à votre entreprise. • Les solutions technologiques majeures (systèmes de détection d'intrusion, gestion des accès, chiffrement) • Les principes d'arbitrage (mitiger, transfer , accepter) et transfert à l'assurance • Stratégie de traitement des risques et mesures de sécurité : définir son plan d'action	**Apport théorique (0h30)** Comprendre l'enjeu stratégique de la gestion des risques et leur impacts sur le développement , la rentabilité et la pérennité de l'entreprise + Capsules vidéos courtes et quiz **Atelier pratique (2h30)** Construire la matrice des risques de son entreprise et initier son plan d'arbitrage stratégique de traitement des risques Travail guidé + Analyse de cas **Live Mentor (1h)** Échanger sur les stratégies de cybersécurité adaptées à son entreprise Session interactive avec retour sur les matrices des participants **Ressources types :** Template de matrice des risques, Étude de cas : Exemples concrets de gestion des risques en entreprise, Checklist "Évaluer et formaliser sa politique de sécurité"
J1+ 2 semaines	**S3 – Gouvernance & Conformité**	• Introduction : Eléments clés pour une gouvernance Cyber efficace (lignes de défense) • La Politique de Sécurité du Système d'Information (PSSI) au service du dirigeant pour exploiter et construire (security by design) • Les enjeux clés de la conformité & Réglementation (lois et des normes clés : RGPD, NIS2, ISO 27001, ...) • L'alignement stratégique Cyber sur les enjeux métiers : Les principales	**Apport théorique (0h30)** Assimiler les cadres réglementaires et la gouvernance en cybersécurité, identifier des indicateurs de performances. Capsules vidéos courtes et quiz + Construction une politique V1 de cybersécurité, **Atelier pratique (2h30)** Réaliser sa feuille de route cyber (Roadmap) et la matrice de responsabilité (RACI) de son organisation en intégrant ses travaux (matrices de risques et plan d'arbitrage v1) + Identifier 3 à 5 indicateurs clés stratégiques et opérationnels de sa

		orientations stratégiques Cyber pour votre entreprise • Comment mettre en place sa feuille de route (roadmap) Cyber d'entreprise comme un levier d'action et de soutien.	roadmap **Live Mentor (1h)** Valider les choix stratégiques en matière de conformité et gouvernance en lien avec les roadmaps, Session interactive avec retours **Ressources types** : Organisation type et RACI (par taille et écosystème) , Roadmap type, PSSI (light à lourde),Cadre réglementaire (NIS2, ISO 27001, RGPD, PME vs grands groupes) Checklist d'auto-évaluation RGPD, ISO 27001 et Benchmark CIS,
J1+ 3 semaines	**S4 - Incident et gestion sécurisée des parties prenantes**	• Introduction : l'incident cyber et sa genèse • De l'incident à la crise : les principes de collaboration des parties prenantes • Se préparer à une cyberattaque : Mise en place d'un plan de réponse (processus de communication) • Développer la résilience de son entreprise (PCA / PRA / BIA) • Evaluez et gérer les risques Cyber de vos tiers : un maillon "faible" de ma chaîne de valeur à sécuriser • Comment ajuster la gouvernance : les bonnes pratiques pour gérer les tiers : contrat et pilotage (audit et PAS)	**Apport théorique (0h30)** Comprendre comment évaluer, contractualiser et suivre les prestataires, Capsules vidéos courtes et quiz **Atelier pratique (2h30)** Construire (/adapter) son PCA/PRA pour renforcer votre résilience à un incident cyber (quelque soit sa provenance) Proposer 2 à 3 ajustements de ma roadmaps et RACI **Live Mentor (1h)** Débat autour de vos ajustements (roadmaps/raci) et Discussions with an expert on DRPs/BCPs and pratiques de gestion des prestataires, Session interactive avec feedback **Ressources types** : Template BIA, Plan de réponse type à un incident (cheklist), Plan de continuité et de reprise d'activité (PCA/PRA) , PAS type

			pour prestataire, modèle de grille d'évaluation des prestataires, exemple de clauses contractuelles essentielles pour la cybersécurité (PAS), guide pour structurer un comité cybersécurité.

ORGANISATION ET EXPÉRIENCE DE FORMATION

Équipe pédagogique

Upskilling accompagnent et forment les entreprises à tirer partie des nouvelles technologies comme un levier de transformation et d'amélioration. Notre objectif est d'accompagner les professionnels à ancrer les nouvelles compétences digitales durablement.

Nos intervenants (bac +5) et plusieurs années d'expérience de pratique et de formation accompagnent les stagiaires dans leur parcours de formation.

La formation est ainsi animée par des professionnels de la cybersécurité, dont les compétences techniques, professionnelles et pédagogiques ont été validées par des certifications et/ou testées et approuvées par les éditeurs et/ou notre équipe pédagogique.

- Le directeur du programme est - Thomas Blanc - t.blanc@upskilling.com

Contact

Administratif - formation@upskilling.com

Moyens pédagogiques

Un intervenant vous guide dans votre progression et converse avec vous tout au long de votre apprentissage.
L'intervenant utilisera les différentes méthodes expositives, démonstratives, interrogatives, actives et expérientielles permettant d'acquérir les éléments théoriques et méthodologiques pour les mettre en pratique en séance et entre les séances.

Le produit Skillpilot est mis à disposition pour accéder aux ressources de mission ainsi que le livret pédagogique.
Skillpilot est une solution logicielle accessible depuis internet, un LMS mis à disposition des stagiaires et intervenants.

Format : En distanciel (activités : asynchrones et synchrones)

Durée

- Une durée totale de formation de 16h30 dont 4h en distanciel synchrone avec un intervenant
- Intensité de formation de 4 heures par semaine sur 4 semaines
- 0h30 de bilan / coaching individuel en fin de formation

Lieu : Classe virtuelle

Dispositif de suivi de l'exécution et de l'évaluation des résultats de la formation

Les stagiaires sont accompagnés et suivis : suivi des présences lors de la journée de formation

Les stagiaires sont préparés par l'intervenant avec des mises en situation tout au long de la formation en pratiquant

- Cas pratiques
- Mise en pratique dans leur contexte

À la fin de la formation, le stagiaire reçoit ses résultats et obtient son attestation de fin de formation si

- le stagiaire a été présent et impliqué sur l'ensemble de la formation
- le stagiaire a présenté ses travaux de mise en pratique lors des rendez-vous synchrones permettant d'évaluer la montée en compétence et la validation des critères
- le stagiaire a acquis 75% de l'ensemble des critères d'évaluation lors du bilan individuel (ci-après)

Barème et critère(s) d'évaluation de la (des)compétence(s) visée(s)

- **Piloter la stratégie globale de cybersécurité**
  Critère d'évaluation : Définir et formaliser une stratégie de cybersécurité alignée sur les objectifs de l'entreprise, intégrant une analyse des menaces, des risques et des enjeux réglementaires : acquis (100%) ou non acquis (0%)
    - La stratégie est formalisée dans un document structuré, Une analyse des menaces et des risques critiques est disponible, Stratégie alignée avec les objectifs stratégiques de l'entreprise
- **Superviser et coordonner la mise en œuvre des solutions de cybersécurité**
  Critère d'évaluation : Garantir la mise en œuvre de solutions technologiques adaptées (pare-feu, chiffrement, détection d'intrusion), en coordonnant leur déploiement avec les équipes opérationnelles (IT et métiers). : acquis (100%) ou non acquis (0%)

  - Les solutions mises en place couvrent des risques identifiés, La collaboration avec les parties prenantes (IT/métiers , partenaire) elle structurée et suivie, Un suivi des performances et des vulnérabilités est-il réalisé régulièrement

- **Garantir un niveau de conformité réglementaires et normatives en matière de cybersécurité**
  Critère d'évaluation : Réaliser un audit de conformité annuel et mettre en place un plan d'action correctif pour assurer le respect des normes RGPD, ISO 27001 et autres réglementations en vigueur : acquis (100%) ou non acquis (0%)
  - Un audit de conformité a été réalisé et documenté, Les écarts identifiés ont été corrigés via un plan d'action, Un suivi des évolutions réglementaires et une mise à jour des processus sont mis en place

A la fin de la session de formation, le stagiaire recevra un formulaire d'évaluation à chaque fin de session de formation pour mesurer la qualité de la formation

Moyens techniques

Merci de bien vouloir vérifier que vous avez à disposition un environnement informatique :

- Ordinateur connecté à internet
- Webcam et micro

Accessibilité

UPSKILLING répond à la réglementation concernant l'accessibilité aux personnes en situation de handicap. Dans ce contexte, il veille à l'application des conditions d'accueil et d'accès des publics en situation de handicap.

Notre processus suit des étapes précises et concrètes : Identification d'un potentiel handicap, détermination de la typologie du handicap : moteur, auditif, visuel, intellectuel, psychique ou visuel, transmission d'un questionnaire pour mettre en place les compensations possibles et personnalisables en adéquation avec le besoin du stagiaire qu'il aura exprimé.

Dans le cas d'une formation en salle chez le client, celui-ci est sollicité pour garantir le respect de nos processus.

Référent Handicap avec adresse mail : Thomas BLANC t.blanc@upskilling.com

Modalité d'inscription et délais d'accès

Les inscriptions pour effectuer une analyse du besoin avec l'équipe formation auprès de formation@upskilling.com

1. Analyse du besoin
2. Validation du projet de formation
3. Contractualisation

En corrélation avec le délai de rétractation (10 jours L6353-5 du code de travail), le délais d'accès minimum est fixé à 10 jours (délais entre inscription et date de démarrage)

Effectif plafond / Plancher

Plancher : À partir de 5 personnes

Plafond : 10 personnes

Ces éléments respectent nos normes qualité pour garantir la meilleure expérience de formation.

Tarif(s)

Session Inter-entreprise : 1 250€ ht / stagiaire

Coût salle de formation si souhaité par le client à déterminer (lieux et tarifs proposés par Upskilling)

Les CGV et de règlement sont disponibles dans la rubrique informations pratiques du : https://upskilling.com