

Formation « Sécurité des prestataires »

Réf : SECUPRESTA

L'externalisation de tout ou partie de vos systèmes d'information peut réduire les coûts et simplifier la gestion, mais elle comporte des risques. La sécurité des données peut être compromise si le prestataire n'est pas fiable. La dépendance à un fournisseur externe peut limiter la flexibilité et retarder les interventions et compromettre la continuité d'activité. Enfin, des problèmes de qualité ou de conformité réglementaire peuvent survenir si les services ne sont pas correctement encadrés contractuellement.

Objectifs

- Exposer, analyser et hiérarchiser les risques liés aux prestataires et services externalisés
- Proposer des solutions et des bonnes pratiques
- Permettre une maîtrise des enjeux contractuels et des clauses critiques
- Comprendre les limites des engagements fournisseurs

Cette formation permet d'appréhender ces enjeux dans une approche globale combinant organisation, sécurité opérationnelle et maîtrise juridique, afin de sécuriser la relation fournisseur en amont, pendant et en fin de contrat.

Durée & horaires

- 3 jours soit 21 heures
- Horaires : de 9h30 à 12h et de 13h30 à 17h30/18h00.

Nombre de participant

- Minimum 6 participants – Maximum 24 participants

Public visé

- Toute personne qui est ou envisage de devenir clients de services externalisés
- DSI, RSSI, chef de projet, responsable opérationnel
- Responsable métier, gestionnaire de contrats, gestionnaire de risque
- Consultant en sécurité
- Responsable juridique, juriste

Pré-requis

- Cette formation ne nécessite pas de prérequis particulier.

Méthode pédagogique

- Cette formation est proposée en mode présentiel et peut être accessible en mode distanciel via ZOOM pour les personnes qui ne peuvent ou ne veulent pas se déplacer
- Cours magistral avec de nombreux exemples anonymisés autour d'une étude cas multi contexte

Supports

- Support de cours au format papier en français
- 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
- Examen final à la fin de la formation (cf. certification)

Certification

À l'issue de cette formation, le stagiaire a la possibilité de passer un examen ayant pour but de valider les connaissances acquises. Cet examen de type QCM dure 1h00 et a lieu durant la dernière après-midi de formation. La réussite à l'examen donne droit à la certification SECUPRESTA par HS2.

Programme

Introduction et gouvernance fournisseurs

- Processus interne pour la gestion des fournisseurs
 - Intégration dans une gouvernance de type SMSI (ISO 27001)
- Définition et typologie des prestataires et services externalisés (Hébergement cloud, SaaS, IaaS, outsourcing du développement, infogérance...)
- Cartographie et criticité des fournisseurs
 - En relation avec les processus métiers
 - Selon la dépendance pour la cybersécurité et la protection des données de l'organisation
- Cadre réglementaires et responsabilités RGPD, NIS2, DORA, HDS, Data Act, IA Act, CRA...

Analyse des risques fournisseurs

- Principe de la gestion des risques vis-à-vis de la chaîne de sous-traitants (*supply chain*) et catalogue de risques (fuite de données, cyberattaques via prestataires, indisponibilité...)
- Risques juridiques, dépendance et verrouillage fournisseurs,
- Influence étrangère, souveraineté et maîtrise des lois extraterritoriales,
- Intérêt des certifications en sécurité de l'information et continuité d'activité, limites des certifications.

Due diligence et sélection

- Documents et garanties à exiger
- Lecture critique des engagements fournisseurs

Architecture contractuelle : contrat, CGV, annexes

- Rôle du contrat dans la gestion des risques
- Obligation de moyens / résultat
- Clauses de sécurité/Plan assurance sécurité, preuves de sécurité et auditabilité

Données personnelles & sous-traitance

- Clauses RGPD (art. 28)
- Sous-traitance ultérieure
- Transferts internationaux

Responsabilité & risques financiers

- Limitation de responsabilité
- Plafonds et exclusions
- Assurance et couverture des risques

Piloter, gérer et sortir de la relation fournisseur

- Pilotage de la relation fournisseur
- Comités de suivi
- Indicateurs (*SLA, KPI*)
- Gestion des écarts

Gestion des incidents et des crises

- Coordination client / prestataire
- Notification et communication
- Gestion contractuelle des incidents

Réversibilité et fin de contrat

- Dépendance technique
- Restitution et effacement des données
- Clauses de réversibilité

Négociation contractuelle

Stratégies face aux prestataires

- Clauses non négociables
- Arbitrage risque / coûts

Les outils à mettre en œuvre :

- Contrathèque
- Registre des sous-traitants
- Clauses contractuelles types
- Cartographie de l'écosystème et des solutions (inventaire *SBOM/HBOM/OBOM*)
- Questionnaires, portail fournisseur, agence de notation (*cyber-rating*)
- Programme d'audit

L'étude de cas introduit et présente pour chaque catégorie de risque les clauses contractuelles adaptées pour les maîtriser selon les 4 contextes présentés : Infogérance, hébergement cloud privé, sous-traitance de développement, service SaaS.

Exigences étudiées

- Obligations du client
- Prérogatives du prestataire
- Données personnelles et les obligations issues du RGPD
- Obligations générales de sécurité
- Communication des données
- Confidentialité
- Disponibilité
- Intégrité
- Audits de sécurité
- Réversibilité
- Résiliation
- Effacement des données
- Comptes à privilèges
- Comité de suivi sécurité
- Sous-traitance ultérieure
- Sous-traitance de données, violation de données
- Gouvernance et comité de suivi
- Maintien en Conditions de Sécurité : surveillance et correction des vulnérabilités (*scanner*)
- Gestion des incidents et des crises
- Gestion de la communication