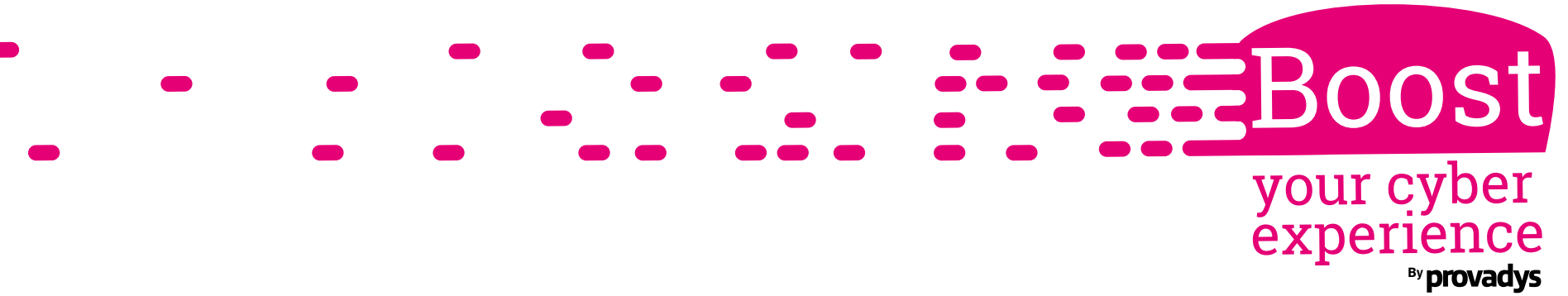
IT Maker
provadys

PROVADYS INSTITUTE

"Nous avons une solution de formation adaptée à votre besoin"

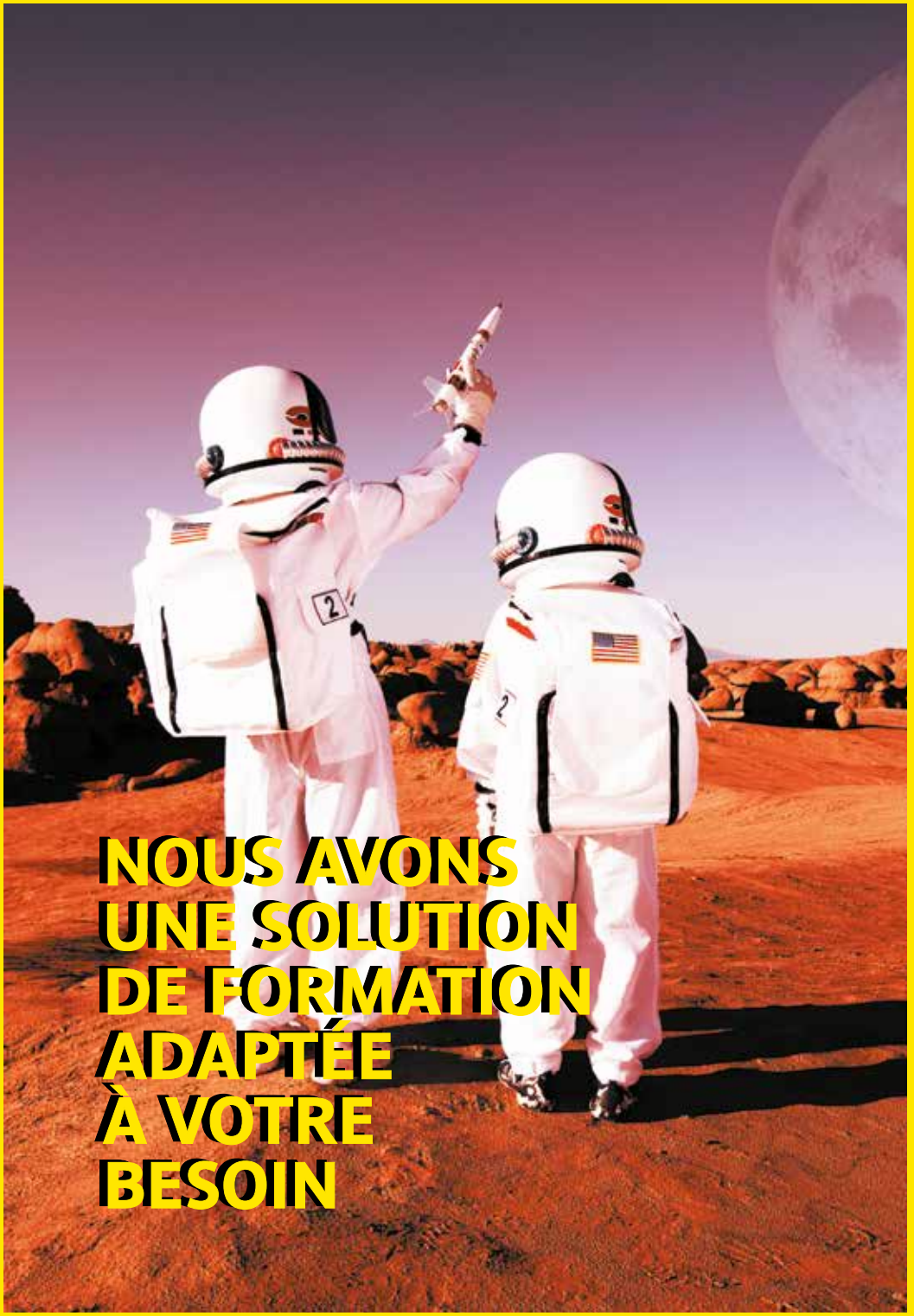

Boost
your cyber
experience
By provadys

Nous avons créé Provadys Institute, en complément des prestations de conseil, pour vous proposer des formations construites et dispensées par nos experts.

Vous souhaitez :

- Affronter les nouveaux enjeux stratégiques IT ?
- Anticiper les Cyber réalités à venir et avoir un temps d'avance ?
- Dépasser vos acquis et envisager des projets jusqu'alors jamais appréhendés ?

Toutes nos formations s'adaptent à votre situation. Enrichis d'exemples concrets, issus de nos expériences de consultant, nous contextualisons, au besoin, nos supports et discours pour répondre au plus juste à votre problématique !



Nos experts certifiés

Afin d'être un acteur de référence sur le marché français du conseil et de l'audit, Provadys a fait le choix d'une politique de formation lui permettant de bénéficier d'experts formés et certifiés aux dernières innovations dans leurs domaines de compétences

Pour former et certifier nos clients, nos formateurs disposent des meilleures compétences et certifications :

SYSTÈME D'INFORMATION

- ISO 22301 Lead Implementer
- ITIL V3 / ISO 20000
- COBIT

CYBER SÉCURITÉ

- ISO 27001 Lead Auditor, Lead Implementer
- ISO 27005 Risk Manager
- CISSP / CISM

TRANSVERSE

- PMP
- Formation de formateur

Être un « learner » Provadys Institute c'est choisir

LA QUALITÉ
L'EXPERTISE
L'ENGAGEMENT

Nos savoir-faire

FORMATION

Formez-vous, auprès de nos consultants, aux problématiques Cyber, aux enjeux de la transformation digitale, aux projets IT.

SENSIBILISATION

Sensibilisez vos utilisateurs, chefs de projet et métiers, aux enjeux de la sécurité, à vos référentiels et à vos pratiques.

E-LEARNING

Boost
your cyber
experience

COACHING

Coaching individuel ou collectif. Améliorez vos performances et déployez vos talents, afin d'atteindre vos objectifs opérationnels.

Nos formations

Nos formations sont construites et dispensées par nos consultants. Ils se mobilisent pour vous transmettre leurs connaissances et expériences de terrain autour des sujets d’actualité.
Cyber Sécurité, transformation digitale, gestion de crise, suivez nos différents cursus et gagnez en compétences techniques et humaines !

Accompagnement au changement

Objectifs

- Intégrer la transformation métier et l'évolution des systèmes d'information (SI)
- Anticiper et traiter le changement dans le domaine de la sécurité des SI à travers des cas réels
- Gérer les changements de votre organisation : métiers, systèmes d'information, sécurité…

Publics

- Direction métier
- Chef de projet

Programme

Comprendre les enjeux d'un changement

- Le contexte du changement dans les organisations
- Les facteurs déclencheurs du changement
- Le changement comme projet
- Le changement comme mouvement permanent

Découvrir les attitudes et dispositifs à adopter pour une conduite réussie du changement

- Les points de vigilance de la conduite du changement
- Mieux comprendre le contexte humain
- Les outils de communication et de formation
- Les types de méthodes de conduite du changement
- Pour une planification efficace du changement

Le changement dans le cadre de l'évolution de la sécurité des SI

- Le domaine de la sécurité des SI
- Les types de changement dans la sécurité des SI
- Étude de cas concrets de changement dans le domaine de la sécurité des SI

Partager ses bonnes pratiques

- Ateliers d'échanges sur des cas pratiques vécus par des participants
- Retours d'expérience et jeux de rôle

DURÉE : 2 JOURS (16H)
PRIX : 1 480 € HT

Piloter la sécurité des données et des SI externalisés

Objectifs

- Maîtriser les enjeux de la sécurité des SI lors de l'externalisation
- Exercer votre responsabilité sur la sécurité des SI externalisés
- Choisir l'outil d'évaluation de votre fournisseur
- Intégrer la sécurité des SI dans les projets d'externalisation

Publics

- Reponsable sécurité des systèmes d'information
- Direction des risques
- Direction des systèmes d'information
- Direction de la conformité

Programme

Identifier les besoins en sécurité

- Connaître son niveau de sécurité interne
- Définir les besoins en termes de sécurité
- Identifier ses responsabilités face au mode d'externalisation choisi
- Sélectionner les mesures et les exigences de sécurité

Contractualiser avec un fournisseur de services

- Rédiger et lancer la consultation
- Choisir le mode d'externalisation et le fournisseur de services
- Intégrer les clauses de sécurité de l'information dans le contrat
- Coordonner les directions métier et juridique

Piloter la relation avec les fournisseurs

- Choisir la méthode appropriée pour évaluer ses fournisseurs
- Déclencher la clause d'auditabilité
- Valoriser l'audit pour construire une relation gagnant/gagnant
- Assurer sa résilience face à une défaillance d'un fournisseur
- Être en capacité de changer de fournisseur

DURÉE : 1 JOUR (8H)
PRIX : 990 € HT

Faire face aux Cyber Crises, développer la Cyber Résilience

Objectifs

- Décrypter les spécificités des Cyber Crises
- Mettre en place une cellule de crise spécifique Cyber
- Déployer les process spécifiques à la Cyber Crise
- Déjouer les pièges de la communication de crise

Publics

- Responsable des plans de continuité d'activité, responsable sécurité… et tout responsable opérationnel soucieux de mettre en place la Cyber Résilience
- Profil technique et profil organisationnel
- Toute personne intéressée par les principes de prévention et de réaction en cas de Cyber Attaque

Programme

Sensibiliser aux Cyber Crises

- L'importance de la sensibilisation des utilisateurs
- Les questions à se poser pour une campagne de communication réussie
- Construire un message de sensibilisation

Anticiper la continuité d'activité

- Les principes des plans de continuité d'activité
- Construire un plan de continuité d'activité

Se préparer à la gestion de crise

- Comprendre la gestion de crise : organisation, moyen, communication de crise…
- Retours d'expérience : les impacts d'une bonne et d'une mauvaise gestion de crise
- Préparer son plan de gestion de crise
- Les nouvelles exigences en matière de notification en cas de compromission des données à caractère personnel
- Organiser des exercices de Cyber Crises : de la création à la réalisation

DURÉE : 1 JOUR (8H)
PRIX : 990 € HT

Conduite et coordination d'une campagne de tests d'intrusion

COACHING OPÉRATIONNEL RECOMMANDÉ

Objectifs

- Acquérir les bonnes méthodes pour anticiper un test d'intrusion (TI)
- Maîtriser l'évaluation automatisée de la sécurité des infrastructures
- Connaître les techniques manuelles et spécifiques des TI
- Appréhender les techniques de hacking en vue de protéger le SI de l'organisation

Publics

- Analyste sécurité des systèmes d'information
- Auditeur interne
- Risk manager
- Responsable sécurité des systèmes d'information
- Direction des systèmes d'information
- Développeur

Pré-requis

- Connaissance des principaux protocoles Internet (DNS, DHCP, http, etc.)

Programme

Se prémunir des attaques

- Cartographier le périmètre visible par les agresseurs potentiels
- Identifier les accès et les vulnérabilités potentielles

Techniques d'intrusion basiques

- Mettre en œuvre des outils d'analyse automatique
- Théorie des failles « système »
- Mettre en œuvre des techniques d'attaques applicatives

Techniques d'intrusion avancées

- Attaques des applications web
- Attaques des applications non web

- Coaching en tests d'intrusion

LES +

DURÉE : 1 JOUR (8H)
PRIX : 990 € HT

Techniques d'intrusion spécifiques aux réseaux internes

Objectifs

- Maîtriser les outils et les techniques des « insiders »
- Éprouver concrètement la sécurité des SI face aux agresseurs internes
- Comprendre et évaluer les faiblesses du SI

Publics

- Analyste sécurité des systèmes d'information
- Auditeur interne
- Risk manager
- Responsable sécurité des systèmes d'information
- Développeur

Programme

Spécificités des tests d'intrusion interne

- Tests du stagiaire
- Trophées ou cibles identifiées
- Préparation des tests

Récupération de données

- Cartographie des données directement accessibles (disques, partages, bases de données, etc.)
- Analyse de la protection des données directement accessibles
- Contournement d'authentification

Les différents types d'attaques

- Attaques du poste de travail local
- Attaques du réseau interne
- Attaques physiques (USB, Firewire)
- Attaques sur les autres protocoles (Wifi, Bluetooth, etc.)

DURÉE : 2 JOURS (16H)
PRIX : 1 900 € HT

Certification ISO 27001- LEAD IMPLEMENTER

Objectifs

- Mener à bien un projet ISO 27001
- Développer ses connaissances en SMSI
- Planifier et animer un projet de mise en conformité ISO 27001
- Acquérir des compétences pour implémenter un SMSI

Publics

- Chef de projet qui souhaite mettre en œuvre un système de management de la sécurité de l'information (SMSI)
- Implémenteur qui souhaite acquérir la culture ISO dans le cas d'un projet de reprise de système de management de la sécurité de l'information
- Toute personne intéressée par les principes d'un système de management de la sécurité de l'information

Programme

Jour 1 : Modèle normatif et système de management

- Processus de certification ISO 27001
- Principes fondamentaux de la sécurité de l'information
- SMSI

Jour 2 : Planifier le projet de mise en conformité

- Choisir le périmètre du futur SMSI et conduire l'appréciation des risques
- Établir sa déclaration d'applicabilité

Jour 3 : Mettre en œuvre le SMSI

- Établir les processus clés et améliorer l'existant
- Implémenter les contrôles et les dispositifs de suivi
- Former et sensibiliser les utilisateurs du SMSI

Jour 4 : Améliorer le SMSI et se préparer à l'audit de certification

- Animer le plan d'amélioration continue
- Capitaliser sur les incidents de sécurité et prendre en compte les résultats d'audit
- Préparer la Direction, le responsable de SMSI et les utilisateurs à l'audit
- Outiller le SMSI pour l'audit

Jour 5 : Animer le SMSI

- La revue de Direction et les leviers de décision
- Examen de certification ISO 27001 Lead Implementer (3H)

LES +

- **Vos compétences valorisées par un référentiel mondialement reconnu**
- Support et examen écrits en anglais ou en français
- Exercices pratiques analogues à l'examen de certification
- Offert : Norme ISO 27001 : 2013

DURÉE : 5 JOURS (40H)
PRIX : 3 000 € HT

Certification ISO 27005-RISK MANAGER

Objectifs

- Comprendre les concepts, approches, méthodes et techniques permettant une gestion efficace du risque selon ISO 27005
- Interpréter les exigences d'ISO 27001 concernant la gestion du risque
- Comprendre la relation entre un système de management de la sécurité de l'information, des mesures de sécurité, et la conformité aux exigences des différentes parties prenantes d'une organisation
- Acquérir les compétences pour mettre en œuvre, maintenir et gérer un programme continu de gestion du risque dans la sécurité de l'information
- Acquérir les compétences pour conseiller efficacement une organisation sur les meilleures pratiques en gestion du risque dans la sécurité de l'information

Publics

- Gestionnaire de risques
- Personne responsable de la sécurité de l'information ou de la conformité au sein d'une organisation
- Membre d'une équipe de sécurité de l'information
- Consultant en technologie de l'information
- Personnel de la mise en œuvre de la norme ISO 27001 ou cherchant à s'y conformer ou participant à un programme de gestion du risque

Programme

Jour 1 : Introduction, programme de gestion du risque, identification et analyse du risque selon ISO 27005

- Concepts et définitions liés à la gestion du risque
- Normes, cadres de référence et méthodologies en gestion du risque
- Mise en œuvre d'un programme de gestion du risque dans la sécurité de l'information
- Analyse du risque (identification et estimation)

Jour 2 : Évaluation du risque, traitement, acceptation, communication et surveillance

- Évaluation du risque
- Traitement du risque
- Acceptation du risque dans la sécurité de l'information et gestion du risque résiduel
- Communication du risque dans la sécurité de l'information
- Surveillance et contrôle du risque dans la sécurité de l'information

Examen Certified ISO/IEC 27005 Risk Manager

DURÉE : 2 JOURS (16H)
PRIX : 1 700 € HT

Foundation

VALORISER VOS COMPÉTENCES AVEC UNE CERTIFICATION ISO 27001

Objectifs

- Appréhender la mise en œuvre d'un SMSI conforme à ISO 27001
- Comprendre la relation entre un SMSI, incluant le management des risques et des contrôles et la conformité aux exigences des différentes parties prenantes d'une organisation
- Connaitre les concepts, démarches, normes, méthodes et techniques permettant de gérer efficacement un SMSI
- Acquérir les connaissances nécessaires pour contribuer à la mise en œuvre d'un SMSI tel que spécifié dans ISO 27001

Publics

- Auditeur
- Directeur de production
- Ingénieur innovation
- Responsable des opérations
- Chef de projet réseaux et sécurité
- Consultant en sécurité des technologies de l'information
- Administrateur réseaux

Programme

Jour 1 : Introduction au concept de SMSI

- Introduction à la famille de normes ISO 27000
- Introduction aux systèmes de management et à l'approche processus
- Principes fondamentaux en sécurité de l'information
- Exigences générales et mise en œuvre
- Amélioration continue de la sécurité de l'information
- Conduire un audit de certification ISO 27001

Jour 2 : Mettre en œuvre des mesures de sécurité de l'information conformes à ISO 27001 et examen de certification

- Principes et élaboration de mesures de sécurité de l'information
- Documentation d'un environnement de contrôle de sécurité de l'information
- Contrôle et surveillance des mesures de sécurité de l'information
- Exemples de mise en œuvre de mesures de sécurité de l'information basée sur les meilleures pratiques de l'ISO 27002

Certification

- Épreuve écrite d'une heure avec le support de stage et la norme ISO 27001
- Résultats transmis par le jury PECB

LES +

- **Vos compétences valorisées par un référentiel mondialement reconnu**
- Nos consultants experts animent les formations en anglais ou en français
- Support et examen écrits en anglais ou en français
- Tests pratiques analogues à l'examen de certification
- Offert : Norme ISO 27001

DURÉE : 2 JOURS (16H)
PRIX : 1 700 € HT

Lead Auditor

VALORISER VOS COMPÉTENCES AVEC UNE CERTIFICATION ISO 27001

Objectifs

- Acquérir l'expertise pour réaliser un audit interne ISO 27001 suivant les lignes directrices ISO 19011
- Acquérir l'expertise pour gérer une équipe d'auditeurs de SMSI
- Comprendre le fonctionnement d'un SMSI selon l'ISO 27001
- Améliorer la capacité d'analyse de l'environnement interne et externe d'une organisation, d'évaluation des risques d'audit et de prise de décision dans le contexte d'un audit SMSI.

Publics

- Auditeur de système de management de la sécurité de l'information (SMSI)
- Chef de projet ou consultant
- Responsable de la gouvernance des TI d'une organisation et de la gestion des risques

Programme

Jour 1 : Introduction au concept de SMSI

- Cadre normatif, légal et réglementaire lié à la sécurité de l'information
- Principes fondamentaux de la sécurité de l'information
- Processus de certification ISO 27001
- Présentation détaillée des clauses 4 à 8 de l'ISO 27001

Jour 2 : Planifier et initialiser un audit ISO 27001

- Principes et fondamentaux d'audit
- Approche d'audit basée sur les preuves et sur le risque
- Préparer un audit de certification ISO 27001
- Audit documentaire d'un SMSI
- Conduire une réunion d'ouverture

Jour 3 : Conduire un audit ISO 27001

- Communication pendant l'audit
- Procédure d'audit : observation, revue documentaire, entretien technique d'échantillonnage, vérification technique, corroboration et évaluation
- Rédaction des plans de tests d'audit
- Formulation des constats d'audit
- Rédaction des rapports de non-conformité

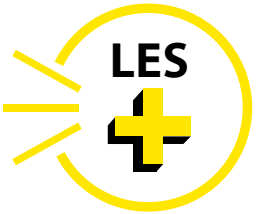
Jour 4 : Clôturer et assurer le suivi d'un audit ISO 27001

- Documentation d'audit et revue qualité
- Mener une réunion de clôture et finaliser un audit ISO 27001
- Évaluation des plans d'action corrective
- Audit de surveillance ISO 27001
- Programme de gestion d'audit interne ISO 27001

Jour 5 : Examen de certification

- Épreuve écrite de 3 heures
- Support de stage et Norme ISO 27001
- Résultats transmis par le jury PECB

- **Vos compétences valorisées par un référentiel mondialement reconnu**
- Nos consultants experts animent les formations en anglais ou en français
- Support et examen écrits en anglais ou en français
- Tests pratiques analogues à l'examen de certification
- Offert : Norme ISO 27001



DURÉE : 5 JOURS (40H)
PRIX : 3000 € HT

Les fondamentaux d'un projet IT Agile

Objectifs

- Acquérir des connaissances opérationnelles sur le déploiement des méthodes agiles
- Obtenir des éléments précis pour la gestion d'un projet agile
- Bénéficier de l'expérience de nos formateurs à la mise en place des méthodes agiles

Publics

- Direction métier
- Chef de projet
- Toute personne intéressée par les méthodes agiles et leur déploiement

Programme

Qu'est-ce que la méthode agile pour un projet ?

- Retour sur les méthodes traditionnelles et leurs limites
- Principes clés et valeur ajoutée des méthodes agiles
- État de l'art et adoption dans les entreprises de ces méthodes
- Présentation des déclinaisons : XP et Scrum

Comment réussir à mettre en œuvre ces méthodes ?

- La problématique du développement par itération
- Établir des bases solides
- Mettre en place les rôles clés au sein du projet
- Définir correctement ses tests en méthode agile

Les bonnes pratiques

- Gérer l'impact organisationnel des méthodes agiles
- Savoir répondre aux objections sur le projet pour lancer le projet vers le succès
- Éviter les difficultés courantes et identifier les facteurs clés de succès
- Vers l'entreprise agile

DURÉE : 1 JOUR (8H)
PRIX : 990 € HT

Maîtriser PCI DSS V3.2 et ses exigences

Objectifs

- Comprendre les risques des vols de données CB
- Comprendre à quoi servent les standards PCI
- Comprendre le périmètre à protéger
- Comprendre comment utiliser PCI DSS
- Éclairer les équipes projet PCI DSS
- Comprendre les exigences de PCI DSS

Publics

- Directeur, Responsable sécurité des systèmes d'information, Direction des systèmes d'information, Directeur financier, Acheteur, Juriste, Direction des ressources humaines, ...
- Chef de projet PCI DSS, Correspondant sécurité, Auditeur, Architecte technique, Exploitant, ...

Programme

Jour 1 : L'essentiel du standard PCI DSS

- Comprendre la fraude
- Le PCI SSC et les autres acteurs du modèle PCI
- Le standard PCI DSS
- Le périmètre PCI DSS
- La conformité à PCI DSS
- Les exigences PCI DSS (généraliste)

Jour 2 : Réussir son projet de mise en conformité PCI DSS

- La gestion d'un projet PCI DSS (build)
- La gestion d'un projet PCI DSS (run)

Jour 3 : Maîtriser les exigences PCI DSS

- Les exigences PCI DSS (expert)

DURÉE : 3 JOURS (24H)
PRIX : 2 990 € HT

Optimisez vos infrastructures avec le Cloud

Objectifs

- Se familiariser avec les différents concepts liés au Cloud
- Détenir les arguments et les solutions à la mise en place d'une infrastructure dans le Cloud
- Acquérir des connaissances opérationnelles sur le Cloud
- Bénéficier de l'expérience de nos formateurs en sensibilisation au Cloud

Publics

- Direction des systèmes d'information
- Responsable d'exploitation
- Service Delivery Manager

Programme

Présentation des offres Cloud

- **IaaS :** Infrastructure as a Service (concepts et fondamentaux, typologies de Cloud, typologies d'IaaS...)
- **PaaS :** Platform as a Service (développer dans le Cloud, panorama des offres du marché)
- **SaaS :** Software as a Service (concepts et fondamentaux, typologies d'application, notion d'écosystème...)

Opportunités du Cloud pour l'entreprise

Bénéfices vs Risques :

- Disponibilité, fiabilité, extensibilité, maîtrise du budget : les grands bénéfices du Cloud
  VS Réversibilité, sécurité et perte de contrôle : les risques à évaluer
- Dimensionnement du service
- Répondre aux exigences métiers
- Partager avec les clients, fournisseurs et partenaires

Gérer la transition vers le Cloud

- Vers quel modèle faire évoluer son système d'information ?
- Point d'attention pour leur mise en œuvre (sécurité, protection des données, migration)
- Gérer la migration (évolution des infrastructures, planification de la migration, anticipation de l'ensemble des adhérences fonctionnelles et techniques)

DURÉE : 1 JOUR (8H)
PRIX : 990 € HT

Protection des données personnelles : maîtrise du cadre règlementaire (RGPD)

Objectifs

- Sécuriser les données à caractère personnel (DCP) manipulées par l'organisme
- Maîtriser le traitement des DCP en France et à l'international
- Construire une organisation adaptée à la protection des DCP
- Appréhender les enjeux de la protection des DCP dans un environnement en construction

Publics

- Direction des systèmes d'information
- Responsable sécurité des systèmes d'information
- Chef de projet

Programme

Comprendre et connaître les obligations et les responsabilités

- Les notions autour des données à caractère personnel
- Les nouveaux droits et les nouvelles obligations
- Rôles et responsabilités des dirigeants et des intervenants dans le traitement des données

Appréhender les autorités de contrôle et la dimension européenne et internationale

- La CNIL et sa jurisprudence
- Le groupe 29 et la Commission européenne
- Les DCP à l'étranger

Gérer le risque lié aux données personnelles

- Analyser et quantifier les risques liés aux données personnelles (cartographie, Privacy Impact Assessment (PIA)…)
- Risques spécifiques aux familles de données (données bancaires, données médicales, images/vidéos, géolocalisation, profilage, etc.)

Définir une stratégie de protection des DCP

- Les actions prioritaires pour la mise en conformité (organisationnelles, techniques et juridiques)
- Choisir une organisation et définir les rôles et responsabilités (Data Protection Officer (DPO) dédié, DPO mutualisé, poste dédié…)

Sélectionner les outils et systèmes de protection des DCP

DURÉE : 2 JOURS (16H)
PRIX : 1 480 € HT

Résilience : gestion de crise et continuité d'activité

Objectifs

- Maîtriser les enjeux et les approches du maintien en conditon opérationnelle (MCO)
- Établir une démarche MCO adaptée à son dispositif de continuité
- Piloter le plan de continuité d'activité (PCA) et suivre les indicateurs clés
- Promouvoir une culture de la continuité d'activité

Publics

- Responsable sécurité des systèmes d'information
- Responsables des plans de continuité d'activité
- Responsable infrastructure
- Gestionnaire PCA ou toute personne en charge d'un PCA

Programme

Méthodologie de mise en œuvre du PCA/cycle de vie du PCA

- Définition du périmètre et des scénarios de crise
- Identification des besoins en continuité et formalisation de la stratégie de continuité
- Mise en place des solutions de secours techniques, fonctionnelles et organisationnelles
- Maintien en condition opérationnelle
- Sensibilisation des collaborateurs et développement d'une culture de la continuité d'activité
- Organisation de tests et exercices

Gouvernance associée à la mise en œuvre du PCA

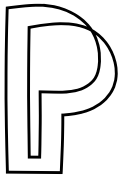
- Définition des instances de pilotage
- Suivi des performances du PCA
- Dispositif d'amélioration continue
- Identification des acteurs et définition de leur rôle
- Mise en place d'une communauté PCA

Mise en place d'un outil de gestion PCA

- Intérêts et objectifs d'un outil de gestion PCA
- Les principaux outils proposés sur le marché
- Évaluation de la maturité du dispositif

DURÉE : 1 JOUR (8H)
PRIX : 990 € HT

Information
Security



CIO
Advisory

Business
Transformation

Provadys
Institute

provadys

Paris | Sophia-Antipolis | Nantes

provadys.com


IT Maker
provadys