PCA / PRA

Lien : https://innov-systems.com/formation/pca-pra

DURÉE
5 jours (35h)

RÉFÉRENCE
MSI242

CATÉGORIE
Gouvernance et Pilotage de la DSI

OBJECTIFS DE LA FORMATION

À l'issue de cette formation, vous serez capable de :

- Comprendre les principes fondamentaux du PCA/PRA
- Être capable de concevoir une démarche complète de continuité d’activité
- Savoir réaliser une analyse d’impact métier (BIA)
- Identifier les menaces et les vulnérabilités affectant les processus critiques
- Définir des stratégies de continuité et de reprise adaptées à l’organisation
- Élaborer des plans documentés et opérationnels
- Organiser des exercices de test efficaces
- Mettre en œuvre des procédures de gestion de crise
- Garantir la conformité réglementaire en matière de résilience
- Promouvoir une culture de continuité et de résilience au sein de l’organisation

POUR QUI ?

- Responsables de la sécurité des systèmes d’information (RSSI)
- Responsables de la continuité d’activité ou de la gestion des risques
- Responsables informatiques et techniques (DSI, IT Manager)
- Responsables métiers impliqués dans les processus critiques
- Membres des cellules de crise ou comités de direction
- Consultants en cybersécurité, gestion de crise ou gouvernance SI
- Auditeurs internes ou externes spécialisés en PCA/PRA
- Responsables qualité ou conformité
- Responsables d’infrastructures critiques ou sensibles
- Toute personne chargée de préparer l’organisation à un sinistre

Programme détaillé

1 / Introduction au PCA/PRA : définitions et enjeux

- Comprendre la différence entre PCA (Plan de Continuité d'Activité) et PRA (Plan de Reprise d'Activité)
- Identifier les enjeux stratégiques liés à la résilience organisationnelle
- Analyser les obligations réglementaires et normatives (ISO 22301, RGPD, etc.)

2 / Gouvernance du PCA/PRA

- Définir les rôles et responsabilités dans la mise en place d'un PCA/PRA
- Mettre en place un comité de pilotage dédié
- Définir une politique de continuité d'activité alignée sur la stratégie

3 / Analyse d'impact sur les activités (BIA - Business Impact Analysis)

- Identifier les processus critiques et les ressources associées
- Évaluer les impacts financiers, opérationnels et réglementaires
- Prioriser les activités en fonction de leur criticité

4 / Analyse des risques et scénarios de crise

- Identifier les menaces internes et externes pouvant perturber l'activité
- Évaluer la probabilité et la gravité des risques
- Élaborer des scénarios de sinistre réalistes

5 / Définition des stratégies de continuité et de reprise

- Choisir les stratégies de mitigation adaptées (redondance, télétravail, externalisation)
- Définir les niveaux de service minimum (RTO, RPO)
- Intégrer les exigences de sécurité de l'information

6 / Élaboration du plan de continuité et de reprise

- Rédiger des procédures détaillées et accessibles
- Organiser les ressources humaines et matérielles nécessaires
- Définir les plans de communication de crise

7 / Mise en œuvre opérationnelle

- Intégrer les solutions techniques (sauvegarde, PRA IT, systèmes redondants)
- Former les équipes aux rôles définis dans les plans
- Mettre en place des outils de suivi et de pilotage du PCA/PRA

8 / Tests, exercices et simulations

- Organiser régulièrement des tests de continuité et de reprise
- Analyser les résultats et les écarts constatés
- Ajuster les plans selon les retours d'expérience

9 / Maintien et amélioration continue

- Mettre en place un dispositif de veille réglementaire et technologique
- Réaliser des audits internes et des revues périodiques
- Mettre à jour les plans en fonction des évolutions internes et externes

10 / Retour d'expérience et études de cas

- Étudier des cas réels de sinistres et de gestion de crise
- Identifier les bonnes pratiques et les erreurs à éviter
- Partager les enseignements tirés de projets de PCA/PRA dans divers secteurs
- Responsables de la sécurité des systèmes d'information (RSSI)
- Responsables de la continuité d'activité ou de la gestion des risques
- Responsables informatiques et techniques (DSI, IT Manager)
- Responsables métiers impliqués dans les processus critiques

- Membres des cellules de crise ou comités de direction
- Consultants en cybersécurité, gestion de crise ou gouvernance SI
- Auditeurs internes ou externes spécialisés en PCA/PRA
- Responsables qualité ou conformité
- Responsables d’infrastructures critiques ou sensibles
- Toute personne chargée de préparer l’organisation à un sinistre

Approche pédagogique

- Support Ecrit et Projection
- Exposés Interactifs, Podcasts et Vidéos
- Brainstorming et Jeux de Rôle
- Cas Pratiques et Labs inclus pour leur impact opérationnel
- Test de Validation des Acquis des Connaissances

Prochaines dates programmées

27 au 31 Juil. 2026	Présentiel -
07 au 11 Sep. 2026	Présentiel -
28 Sep. au 02 Oct. 2026	Présentiel -
02 au 06 Nov. 2026	Présentiel -
23 au 27 Nov. 2026	Présentiel -

Autres dates possibles sur demande. Contactez-nous pour organiser une session intra-entreprise.

Réservation & Renseignements

Téléphone : +212 522 247 210
Email : contact@innov-systems.com
Web : https//www.innov-systems.com