

Séminaire de 2 jour(s)
Réf : PDS

Participants

Responsable Continuité,
Risk Manager ou RSSI.
Directeurs ou responsables
informatiques, correspondants
Sécurité, chefs de projets
MOA et MOE, auditeurs
internes ou externes,
consultants.

Pré-requis

Bonnes connaissances des
architectures SI.

Prix 2012 : 1775€ HT

Dates des sessions

Paris

12 avr. 2012, 21 juin 2012
27 sep. 2012, 6 déc. 2012

Plan de secours et de continuité se préparer et faire face à la crise

OBJECTIFS

Ce séminaire vous propose une démarche méthodologique et les meilleures pratiques pour mener à bien un projet de secours informatique et/ou de continuité d'activité en accord avec les normes et standards du domaine (ISO 27001/27002, BS25999, ITIL V3...). De l'analyse des risques et de la conception des plans jusqu'aux tests et la cellule de crise.

1) Pourquoi gérer la continuité

2) Définitions et concepts

3) Le projet et sa gestion

4) Analyse des risques

5) L'identification des activités critiques

6) Les moyens pour la conception des dispositifs

7) Plans de continuité

8) Procédures d'escalade et cellule de crise

9) L'organisation et le suivi des tests

10) La continuité d'activité en tant que processus ITIL

1) Pourquoi gérer la continuité

- L'évolution des entreprises et de leur stratégie.
- L'importance stratégique de l'information.
- Les enjeux pour l'entreprise d'une stratégie de continuité : lois et réglementations, normes et standards.

2) Définitions et concepts

- Définir la stratégie de continuité.
- Les différences entre plan de continuité d'activité (BCP), plan de secours informatique (DRP), plan de reprise.
- Rappels de sécurité : critères DICP et les 11 thèmes ISO.
- La feuille de route de la continuité.

3) Le projet et sa gestion

- Rappels sur la conduite de projet.
- Les phases d'un projet plan de continuité.
- Les particularités du projet plan de continuité.

4) Analyse des risques

- Les composantes du risque.
- Les principes des différentes méthodes.
- Les autres standards (COBIT, ISO...).
- La notion de matrice d'incertitude.
- L'analyse des risques pour le plan de continuité.

5) L'identification des activités critiques

- Déterminer les activités critiques (BIA) d'une entreprise.
- Les paramètres fondamentaux de l'analyse d'impact.
- La notion de Service Delivery Objectives.

6) Les moyens pour la conception des dispositifs

- Les éléments et le budget pour élaborer les scénarios.
- Les différents sites de repli (hot, warm, cold sites, reciprocal agreement...) en interne ou externalisés.
- Les critères de décision.

7) Plans de continuité

- La construction des procédures.
- Les équipes de secours : constitution, rôles...
- Un exemple de canevas d'un plan de secours.

8) Procédures d'escalade et cellule de crise

- La gestion de l'escalade en phase avec le RTO.
- La constitution de la cellule de crise.
- Les principes de déclenchement du plan de secours.

9) L'organisation et le suivi des tests

- Tests et entraînement des équipes de secours.
- Les différents niveaux de tests selon les standards.
- Le suivi des recommandations.

10) La continuité d'activité en tant que processus ITIL

- L'importance du maintien en condition opérationnelle du plan au quotidien : le cycle de vie PDCA.
- Le processus continuité et autres processus.