

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 17799, BS25999, ITIL V3...). De l'analyse des risques et de la conception des plans jusqu'aux tests et la cellule de crise, cette présentation couvre tous les aspects organisationnels et réglementaires (SOX, règlements internes et du personnel...) relatifs au sujet ainsi que les moyens pour concevoir les solutions techniques appropriées.

[1\) Pourquoi gérer la continuité](#)

[2\) Définitions et concepts](#)

[3\) Le projet et sa gestion](#)

[4\) Comment mener une analyse des risques et le concept de désastres](#)

[5\) Une étape-clé : l'identification des activités critiques](#)

[6\) Les moyens nécessaires à la conception des dispositifs](#)

[7\) La production des plans et la constitution des équipes de secours](#)

[8\) Les procédures d'escalade et la constitution de la cellule de crise](#)

[9\) L'organisation et le suivi des tests](#)

[10\) La continuité d'activité en tant que processus ITIL](#)

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.

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 (ISO, BSI, NIST, ITIL) gouvernance d'entreprise.

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.
- Quelques rappels de sécurité : critères DICP et les 11 thèmes ISO.
- La feuille de route de la continuité.

3) Le projet et sa gestion

- Quelques rappels sur la conduite de projet : étude d'opportunité, l'identification des acteurs, le plan qualité, les comités de suivi.
- Les phases d'un projet plan de continuité.
- Les particularités du projet plan de continuité.

4) Comment mener une analyse des risques et le concept de désastres

- De la menace au risque et du risque au désastre : comment mener l'analyse des risques.
- Les composantes du risque.
- Les principes des différentes méthodes : qualitatives ou quantitatives.
- Panorama des méthodes répandues.
- Les autres standards de contrôles des risques (COBIT, ISO...).
- La notion de matrice d'incertitude.
- L'analyse des risques pour le plan de continuité : le choix des scénarios des désastres ou risques majeurs retenus.

5) Une étape-clé : l'identification des activités critiques

- Comment déterminer les activités critiques (BIA) d'une entreprise.
- Les paramètres fondamentaux de l'analyse d'impact.
- Comment mener les interviews d'analyse d'impact : les données à recueillir.
- La notion de Service Delivery Objectives.
- Comment déterminer les besoins informatiques à partir de l'analyse d'impact et déterminer les RTO, RPO.

6) Les moyens nécessaires à la conception des dispositifs

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

7) La production des plans et la constitution des équipes de secours

- Les plans composant la continuité d'activité (informatiques, logistique, de communication...).
- Comment bâtir le Gantt plan de continuité.
- La construction des procédures.
- Points-clés pour gérer la documentation du plan.
- Les équipes de secours : constitution, rôles, coordination, les aspects réglementations du personnel.
- Un exemple de canevas d'un plan de secours.

8) Les procédures d'escalade et la constitution de la cellule de crise

- Les différents niveaux de la gestion de l'escalade en phase avec le RTO.

- La constitution de la cellule de crise et du poste de commandement: son rôle, ses acteurs, ses responsabilités.
- Les principes de déclenchement du plan de secours, d'exploitation en mode secours et du retour à la normale.

9) L'organisation et le suivi des tests

- L'importance des tests et de l'entrainement des équipes de secours.
- Les différents niveaux de tests selon les standards (desk tests, simulation...).
- L'organisation des tests et les différents participants (acteurs, auditeurs, contrôleurs...).
- Les points de vérification des déroulements des tests.
- 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 suivi des évolutions et les facteurs déclencheurs.
- Le processus continuité en relation avec les autres processus.

Dates des prochaines sessions

| Centre / Mois | Juil. 10 | Aoû. 10 | Sep. 10 | Oct 10 | Nov 10 | Dec 10 | Jan. 11 | Fév. 11 | Mar. 11 | Avr. 11 | Mai 11 | Juin 11 |
|---------------|----------|---------|---------|--------|--------|--------|---------|---------|---------|---------|--------|---------|
| Paris | | | | 14 | | 9 | | | | | | |