Plans de continuité des activités critiques de l'entreprise
de l'analyse des risques au plan de secours, une démarche complète

Séminaire de 2 jours - 14h
Réf : PDS - Prix 2024 : 2 090€ HT

Ce séminaire vous propose les démarches et les meilleures pratiques pour mener à bien un projet de continuité des activités métiers et informatiques en accord avec les normes (ISO 27001/27002, ISO 22301, BS25999, ITIL® V3). De l'analyse des risques et de la conception des plans jusqu'aux tests et à la cellule de crise.

OBJECTIFS PÉDAGOGIQUES

À l'issue de la formation l'apprenant sera en mesure de :

Comprendre les enjeux pour l'entreprise d'une stratégie de continuité

Connaitre les définitions liées au plan de continuité d'activité et les phases d'un projet de mise en place

Appréhender les normes et méthodes pour analyser les risques en vue d'établir un plan de continuité

Déterminer les activités critiques de l'entreprise

Définir les scénarii du plan de secours, les rôles afférents et les ressources utilisées

Rédiger les procédures et les fiches-actions du plan de continuité

Organiser les procédures d'escalade et le déclenchement du plan de secours

LE PROGRAMME

dernière mise à jour : 12/2019

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, etc.
- Rappels de sécurité : critères DICP et 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.

PARTICIPANTS

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

PRÉREQUIS

Connaissances des architectures SI.

COMPÉTENCES DU FORMATEUR

Les experts qui animent la formation sont des spécialistes des matières abordées. Ils ont été validés par nos équipes pédagogiques tant sur le plan des connaissances métiers que sur celui de la pédagogie, et ce pour chaque cours qu'ils enseignent. Ils ont au minimum cinq à dix années d'expérience dans leur domaine et occupent ou ont occupé des postes à responsabilité en entreprise.

MODALITÉS D'ÉVALUATION

Le formateur évalue la progression pédagogique du participant tout au long de la formation au moyen de QCM, mises en situation, travaux pratiques…
Le participant complète également un test de positionnement en amont et en aval pour valider les compétences acquises.

MOYENS PÉDAGOGIQUES ET TECHNIQUES

• Les moyens pédagogiques et les méthodes d'enseignement utilisés sont principalement : aides audiovisuelles, documentation et support de cours, exercices pratiques d'application et corrigés des exercices pour les stages pratiques, études de cas ou présentation de cas réels pour les séminaires de formation.
• À l'issue de chaque stage ou séminaire, ORSYS fournit aux participants un questionnaire d'évaluation du cours qui est ensuite analysé par nos équipes pédagogiques.
• Une feuille d'émargement par demi-journée de présence est fournie en fin de formation ainsi qu'une attestation de fin de formation si le stagiaire a bien assisté à la totalité de la session.

MODALITÉS ET DÉLAIS D'ACCÈS

L'inscription doit être finalisée 24 heures avant le début de la formation.

ACCESSIBILITÉ AUX PERSONNES HANDICAPÉES

Vous avez un besoin spécifique d'accessibilité ? Contactez Mme FOSSE, référente handicap, à l'adresse suivante psh-accueil@orsys.fr pour étudier au mieux votre demande et sa faisabilité.

- 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 et la rédaction 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.
- 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.

LES DATES

CLASSE À DISTANCE
2024 : 02 juil., 15 oct., 17 déc.

PARIS
2024 : 25 juin, 08 oct., 10 déc.