Continuité informatique / PRA

Référence : **SEA116** Durée : **2 jours** Certification : **Aucune**

CONNAISSANCES PREALABLES

• Aucunes.

PROFIL DES STAGIAIRES

• Toutes personnes devant gérer ou mettre en place un plan de continuité d'activité informatique.

OBJECTIFS

• Illustré de nombreux exemples et cas pratiques, ce séminaire fait le point complet des meilleures pratiques permettant la mise en œuvre d'une solution de continuité informatique réaliste et durable.

CERTIFICATION PREPAREE

Aucune

METHODES PEDAGOGIQUES

- Mise à disposition d'un poste de travail par stagiaire
- Remise d'une documentation pédagogique papier ou numérique pendant le stage
- La formation est constituée d'apports théoriques, d'exercices pratiques, de réflexions et de retours d'expérience
- Le suivi de cette formation donne lieu à la signature d'une feuille d'émargement

FORMATEUR

Consultant-Formateur expert Etats de l'art

METHODE D'EVALUATION DES ACQUIS

- Auto-évaluation des acquis par le stagiaire via un questionnaire
- Attestation de fin de stage adressée avec la facture

CONTENU DU COURS

Problématique et acteurs de la continuité informatique

Continuité informatique, cas concrets et retours d'expérience

• Examen de situations concrètes de pertes de centres informatiques : pertes de données, perte de sites, interruption télécom, malveillance informatique, perte de confiance et corruption de données
• Best practices, méthodologie, revue des facteurs clés de succès. Étude de cas. Enseignements en matière de préparation et d'étude des principaux scénarios

Les grands risques informatiques

• Catastrophe naturelle, incendie sur un demi-site, sur un site, panne majeure, pelleteuse, etc. Comment faire face à l'imprévu en cas de survenance d'une crise brutale au plus mauvais moment
• Carence énergétique de courte et moyenne durée. Rupture télécom : conséquences et repli instantané
• Retours d'expérience sur de tels événements. Comment anticiper

PRA, PSI, : les fondamentaux

La terminologie, les acteurs, le cadre normatif

• Plan de Reprise d'Activité (PRA), Plan de Secours Informatique (PSI). Les définitions, les normes
• Mise en place d'un cadre dans l'entreprise, gestion des interfaces avec les métiers et leurs PCA. Les aspects réglementaires et financiers (Bâle II, SOX, LSF, CRBF, Solvency II, etc.) : que conclure pour la construction d'un PRA/PCI ?

Le plan type d'un PRA

- Les objectifs d'un PRA. Le contenu et le plan type. Comment faire collaborer DG, métiers et informaticiens. Comment aboutir à un consensus sur la forme et le fond
- Principaux pièges dans la mise en place d'une stratégie PRA. Points clés pour bien lancer le projet. Éléments de timing et coût. Comment viser juste et raisonnable dès la première itération

Le sponsor

- L'importance d'un bon sponsor dans l'entreprise. La direction générale, l'audit, la DSI : comment résoudre les éventuels écarts de vue entre les parties, notamment vis-à-vis des coûts
- Mettre en place un langage commun sur les risques d'indisponibilité informatique : comment aboutir rapidement en déjouant les principaux pièges

Élaborer et mettre en place un PCI/PRA

La démarche

- L'analyse d'impact (Business Impact), l'analyse de risques (Risk Analysis), comment réaliser rapidement cette étape sans se noyer dans les détails
- Classification rapide des enjeux et des applications : comment obtenir rapidement une bonne cartographie des priorités de l'entreprise et des systèmes d'information

Choix et stratégie d'architecture de secours

- Les grandes options techniques, avantages et inconvénients. Revue des évolutions majeures : le Cloud Microsoft, les solutions conteneurs, la virtualisation, la 4G, etc : vers une révolution du secours ?
- Comment envisager une solution mobile : panorama du marché. Les solutions livrables sur site : containers spécialisés
- Revue des dispositions techniques et des possibilités de repli par système et par technologie : panorama de l'offre internalisable et externalisable. Premiers arbitrages, comment se préserver des voies de retour ? Panorama des solutions Cloud
- Conséquences juridiques des principales options, les contrats de secours, la négociation et les principaux points clés

Les secteurs du plan de secours

- Mobilisation des ressources, gestion des priorités, timing, organisation et suivi
- Aspects logistiques et matériels, comment prévoir l'imprévisible sans surcharger les dossiers de préparation
- Téléphonie, télécoms, réseaux, check-list des principaux points à ne pas oublier
- Ressources humaines de la DSI avant, pendant et après la crise : anticipation des besoins de délocalisation partielle et temporaire des équipes, accompagnement des situations personnelles

La construction pratique du PRA

- Construction de la documentation, annuaire du plan de secours, planning et phasage, pose des jalons, les fiches des tâches, annexes. Construire une documentation pour les imprévus : les fiches réflexes
- La maintenance d'un plan de secours
- Les tests : à la conception, tests techniques unitaires, tests d'intégration, non-régression, tests en réel, en réel simulé. La formalisation des tests : objectifs, scénario, préparation, rôles, acteurs et observateurs
- La communication vers les collaborateurs informatique, vers la cellule de crise, vers les tiers. Préparation des éléments de langage pour une DG
- Que faire quand la DG pousse l'informatique devant les médias suite à un incident. Media training pour informaticiens

Les options techniques et leurs conséquences

Les serveurs et l'architecture technique

- Les clusters et la synchro simple, la virtualisation, avantages, mise en œuvre technique et inconvénients
- Retours d'expérience et bénéfices attendus de la mise en œuvre d'une stratégie de virtualisation du point de vue du secours

La stratégie en plusieurs salles

- La proximité moyenne et la longue distance. Les enjeux sur les débits et les coûts télécoms. Choisir sa stratégie télécom intersite : vers l'objectif de redondance, rapidité et fiabilité
- Sauvegardes : la gestion des volumes et de la synchronisation. Le transfert des données : comment sécuriser les opérations tout en gagnant du temps. Le transfert en urgence des très gros volumes
- La salle blanche : équipement d'une salle en condition d'urgence : comment tenter de gagner du temps en simplifiant l'architecture. La salle blanche comme solution durable après l'échéance du contrat de secours, avantages et inconvénients d'une stratégie en deux étapes.
- L'externalisation : panorama de l'offre, des prestataires et des contrats types : éléments clés à prendre en compte. Le contrat de secours externalisé. Les salles et moyens mobiles : bureaux, énergie, froid, télécom, CPU, disques, etc. Panorama des solutions mobiles
- Sécurité des systèmes d'information : la construction du PRA avec le RSSI : maintien des objectifs de sécurité avant, pendant et après le basculement : audit à froid et à chaud du niveau de sécurité
- Les tests : développement et élaboration des tests. Cas concrets de tests réussis et examen des causes d'échecs. Check list des campagnes de tests des PRA. Gestion des utilisateurs et interfaces applicatives

La stratégie Cloud

- Le risque de discontinuité interne face au risque Cloud : quelle réalité et quels enjeux ?
- Le Cloud comme solution de secours des SI et du management : état du marché et perspectives
- Les enjeux sécurité du Cloud en tant que solution de secours

La situation de crise informatique

Début de crise

- Comment installer une méthode de travail : examen de la situation générale et évaluation des scénarios court et moyen terme. Prise de décision : comment sécuriser la prise de décision et ne pas enclencher une

machine à attendre. Relation DG/DSI face aux incertitudes informatiques
- Les outils de la gestion de crise : précautions juridiques, système d'information, réseau, communication. Revue des aspects pratiques. La messagerie dans le Cloud pour gouverner quand les infrastructures tombent

Le déroulement de la crise informatique

- Déclenchement du PRA, basculement, transfert des équipes, accompagnement des équipes dans la durée
- Mise en place des jalons techniques, comment garder un tableau de bord précis et lisible. Les points de situation et le démarrage sur le site de repli
- Préparation d'une solution plus durable. Gérer le moyen terme en relation avec les métiers. Éléments de communication avec la DG
- Exercices : examen des check-lists pratiques d'une opération de basculement en situation d'urgence jusqu'au retour à la normale
- La sortie de crise : quand et comment organiser le débriefing ? Positionnement de la DSI en période tendue : éléments clés d'une bonne maîtrise d'une situation de crise

Les tests métier

La construction de tests PRA

- Vision pragmatique et réaliste d'un test intégré. Comment préparer un exercice de crise informatique avec les fonctions métier
- Mise en place des scénarios, recherche d'un exercice réellement pertinent : comment aboutir rapidement et proposer un exercice ayant du sens
- Comment construire un exercice réaliste et en tirer les leçons sans compromettre la confiance avec les utilisateurs

Installer la culture de l'exercice en testant PRA et PCA

- Démarche et planification : comment tester par parties les fonctions clés de l'entreprise
- Le télétravail est-il une illusion en cas d'indisponibilité du site ? La mise en situation réelle d'une fonction clé : comment ne pas aller trop loin et risquer de décrédibiliser l'ensemble PCA/PRA
- Le facteur humain : comment capitaliser sur les tests et bâtir une culture "exercices". Comment mettre en place un réseau de pilotes dans les services. Vers une collaboration intelligente et constructive Informatique-PCA