Gestion de la continuité des activités

La Chocolatière 26
CH - 1026 Echandens

Tél. +41 21 706 06 06
Fax +41 21 706 06 00

info@acomm.ch
www.acomm.ch

Vue synthétique

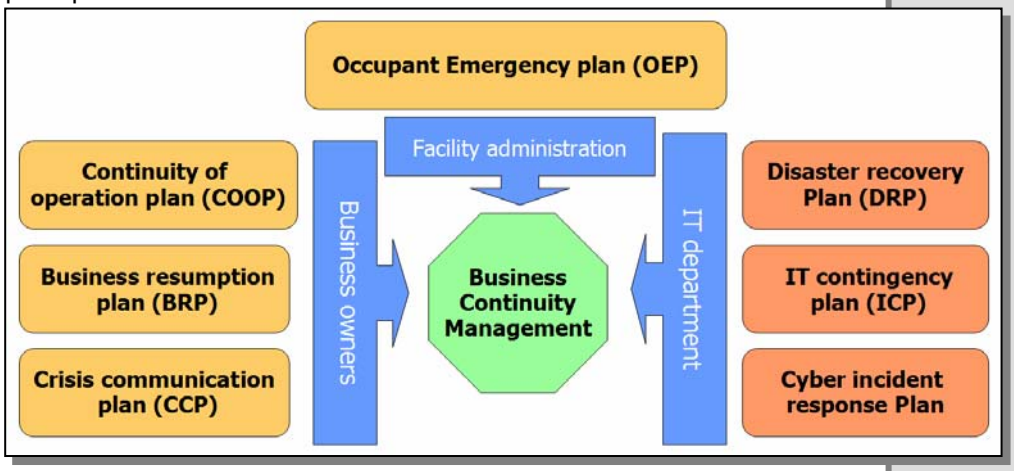
La planification de la continuité et du recouvrement en cas d'événements perturbateurs, d'urgences ou de désastres est resté longtemps à l'état embryonnaire dans beaucoup d'entreprises. Cela n'est pas surprenant considérant que le plan de continuité et de recouvrement ne reçoit en général qu'une attention réduite de la part de la direction d'entreprise. Les exigences de rentabilité accrue et la concentration des moyens qui en résulte couplé à de nouvelles menaces ainsi qu'a la pression du législateur (Sarbane-Oxely, Bâle II) demande aujourd'hui la mise en place de plan de continuité formalisé et documenté.

Les entreprises dépendent de manière croissante de la disponibilité sans failles de leurs systèmes d'information. C'est pourquoi le département informatique est souvent l'initiateur d'activités consistant à assurer le maintient des services critiques du système d'information. Toutefois le plan de recouvrement informatique est une composante qui s'insère dans un ensemble bien plus large de plans préparant l'entreprise à fournir une réponse adéquate en cas de perturbations ou de désastres. En fin de compte, une organisation qui désire assurer sa pérennité est amenée à développer une suite de plans incluant tous les aspects d'organisation, des processus d'affaires, de gestion des infrastructures et du personnel. Parce qu'il existe une relation intrinsèque entre le système d'information et les processus d'affaires qu'il soutient, les différents plans d'urgences doivent être conçus et développés en bonne intelligence avec le plan d'urgence du système d'information (ICP : IT Contingency Plan) de sorte à éviter les contradictions ou les duplications.

La première étape dans l'élaboration d'un système de gestion de la continuité consiste à évaluer l'impact potentiel de différents types d'incidents. Cette analyse est traditionnellement réalisée par le biais d'une analyse d'impact sur les activités. La planification de la continuité dépend d'une compréhension limpide des processus et des données critiques de l'entreprise et des risques qui y sont associés. Une analyse d'impact sur les activités (BIA : Business Impact Analysis) est ainsi un moyen d'estimer systématiquement les conséquences potentielles de différents incidents conduisant à la non disponibilité d'un service ou d'une prestation. L'analyse d'impact permet d'estimer les pertes et autres effets produits. Les pertes financières ne sont pas seules prises en compte, mais aussi les pertes de réputations, les effets législatifs, etc.

Une fois l'analyse d'impact sur les affaires réalisée, il est important de considérer la probabilité du risque. La gestion du risque (RM: Risk Management) est la seconde étape permettant de déterminer quels sont les scénarios les plus probables en pratique afin de définir les priorités du plan de continuité. Le rôle de l'analyse de risques ne dois pas être sous estimé. Au final la gestion de la continuité est en elle-même un exercice d'atténuation du risque.

En troisième lieu, il s'agit de développer des stratégies et des scénarios permettant d'assurer la continuité. Des procédures formelles et des plans documentés sont à mettre en place puis à exercer périodiquement.



Gestion du service

La continuité des activités est un service qui doit être conduit en fonction d'un niveau de service à atteindre. Cela inclus la description des plages d'activités continues (pas d'interruption de service autorisée) et des plages d'activités en mode résilient (interruption de service autorisé) comportant des paramètres de temps-de-restauration et point-de-restauration définis.

Types de plans

Il n'existe pas de définitions universellement acceptée de plan d'urgence du système d'information ou des autres plans qui s'y rapporte. Cela porte à confusion.

Le terme « *Business Continuity Plan* » et « *Disaster Recovery Plan* » sont parfois utilisés, par exemple, de manière interchangeable. Mais cela ne couvre pas les mêmes choses.

Le « Disaster Recovery Plan » doit être vu dans une perspective hiérarchique, c'est un élément important du plan de continuité des affaires, mais il faut considérer plusieurs autres type de plans de secours si l'on cherche à ce prémunir contre les conséquences d'événements inattendus.

A fin de fournir une base commune, ce document identifie quelques types de plans de secours en décrivant leurs buts et leurs champs d'action.

Le modèle proposé ci-dessous permet une gestion et une amélioration continue de la disponibilité des processus d'affaires. Il est inspiré des meilleures pratiques telles que consignées par différents organismes ou standards tels que ISO/IEC 17799 (sécurité de l'information) ou BSI 29555 (Draft : Business Continuity Management). Aucun standard universel n'est toutefois reconnu dans ce domaine. Les plans effectivement développés par les entreprises peuvent par conséquent différer.

Plan	Objectif	Champ d'action
Plan de reprise des activités « BRP »	Préciser les ressources, actions, tâches et informations nécessaires à la reprise des activités faisant suite à un désastre.	Processus d'affaires. Affecte l'IT seulement en qualité de support pour les processus d'affaires.
Plan de continuité des activités « COOP »	Fournir les moyens et les procédures permettant à l'organisation de maintenir les activités essentielles sur un site de secours.	S'adresse au sous ensemble des activités les plus critiques de l'organisation. N'est pas centré sur le système d'information.
Plan d'urgence informatique « ICP »	Fournir les moyens et les procédures permettant une remise en service suite à une défaillance majeur d'une application ou d'un système.	S'adresse aux pannes informatiques. N'est pas focalisé sur les processus d'affaires.
Plan de communication de crises « CCP »	Fournir la procédure permettant de diffuser des points de situations au personnel et au public.	S'adresse à la communication avec le personnel et les employés. N'influence pas l'IT.
Plan de gestion des incidents informatique « CIRP »	Fournir les stratégies permettant de détecter de limiter, et de répondre aux conséquences d'une attaque informatique malveillante.	Focalisé sur les incidents informatiques et/ou réseaux.
Plan de recouvrement en cas de désastre « DRP »	Fournir les procédures détaillées permettant la remise en service des moyens critiques sur un site externe.	S'adresse au système d'information. Limité aux incidents majeurs ayant des effets à long terme.
Plan de secours des occupants « OEP »	Fournir les procédures permettant de réduire les risques de blessures aux personnes et de dommages aux biens en cas de menaces physique.	S'adresse au personnel et bien lié à des infrastructures et des bâtiments. N'est pas focalisé sur l'IT ou les processus d'affaires.
Plan de continuité des affaires « BCP »	Fournis les procédures permettant de maintenir les processus d'affaires critiques lors du recouvrement suite à un incident majeur.	Processus d'affaires. Affecte l'IT seulement en qualité de support pour les processus d'affaires.

acomm
La Chocolatière 26
CH - 1026 Echandens

Tél. +41 21 706 06 06
Fax +41 21 706 06 00

info@acomm.ch
www.acomm.ch