Sécuriser la production et l'exploitation informatique

Fabien Cleuet (CISA) (fcleuet@diathese.fr)

Administrateur AFAI

DIATHESE © 04/2000

1 RISQUES ET ENJEUX

L'exploitation du système d'information est un peu à l'image des mécaniciens du navire ; ils sont au fond de la cale et on ne les voit que rarement à l'extérieur. Pour autant, le navire n'avance qu'avec leurs attention et expertise quotidiennes.

Ainsi, cette équipe permet aux serveurs de fonctionner, s'assure de la bonne fin des traitements lancés et du dispatching des états. En un mot nous leur sommes redevables du fonctionnement quotidien du système d'information.

Pour autant, ce fonctionnement impose des règles de fonctionnement (procédures) et des critères de qualité que nous appelons niveaux de service.

Cobit, en tant que référentiel des bonnes pratiques peut être un outil précieux évitant de laisser des zones d'ombre dans la définition des niveaux de service. Il convient cependant de préciser que l'audit de sécurité, qui est en fait le contrôle de la mise en œuvre des contrats de service, reste un travail de spécialistes de l'audit informatique.

2 NIVEAU DE SERVICE (VOIR COBIT DS1)

2.1 Problématique

Chaque organisation n'a ni les mêmes contraintes ni les mêmes exigences en terme de niveau de service attendu. En effet, si le système d'information ne présente aucun aspect stratégique, il n'est pas utile d'investir dans un bunker et dans un plan de back-up.

A contrario, toute organisation doit se poser la question du niveau de service attendu car de cette étude, découlera la qualité normative dans les différents domaines de la sécurité physique et logique. Il est du ressort de la Direction Générale de définir ses attentes voire ses exigences sur les différents points suivants :

- Le niveau de sécurité global de l'organisation et donc :
  - La sécurité des infrastructures informatiques (accès, protections diverses, back-up),
  - La sécurité logique qui détermine les modalités d'utilisation des systèmes,
  - La politique en matière de confidentialité des données (classification et comportement des utilisateurs),
- La performance et la capacité d'évolution des configurations :
  - Le temps de réponse attendu,
  - Le rythme général de l'exploitation qui conditionne les restitutions aux utilisateurs.

2.2 Le passage au contrat de service

L'existence de contrat de service se justifie de différentes manières.

Primo, il s'agit de principe d'organisation. Ainsi, l'expérience montre qu'une relation client-fournisseur entre un service informatique et les directions utilisatrices contribue à la clarification des rôles, des responsabilités et ce faisant, améliore la qualité du service délivré.

Secondo, il existe des raisons contextuelles et conjoncturelles qui militent en faveur d'une mise en place des contrats de service :

- Préparation du contexte pour une externalisation
- Découpage des activités permettant une adaptation de l'organisation de l'entreprise (fusion acquisition)

La déclinaison de ces contrats de service concerne les différents points évoqués ci après :

- L'infrastructure physique
- L'exploitation
- Les sauvegardes
- La mise en production

Pour ces différents points nous allons chercher à donner au lecteur des points de repère qui sont autant de zones de risques à « cadrer » dans un contrat de service.

3 INFRASTRUCTURE PHYSIQUE (VOIR COBIT DS12)

La sécurité physique regroupe l'ensemble des mesures visant à conserver les équipements informatiques en parfait état de marche. La continuité du système d'information impose un plan de back-up permettant de pallier une défaillance partielle ou totale du matériel informatique.

3.1 Infrastructure physique

Le matériel informatique est installé dans un bâtiment de construction solide à l'abri de toute source d'humidité (fleuves, lac, réserves d'eau, etc.).

La salle informatique est entourée de murs "en dur". Les fenêtres sont en double vitrage blindé. Les portes donnant sur l'extérieur du bâtiment sont blindées et disposent d'une détection d'ouverture reliée à une alarme.

Ces mesures sont plus ou moins indispensables suivant qu'il s'agit :

- d'un centre informatique devant être hautement sécurisé,
- d'une configuration de moindre importance,
- d'un système micro utilisé dans un service utilisateur.

3.2 Protection incendie

Il convient de s'assurer de l'existence et de l'efficacité des moyens de protection incendie. Les matériels informatiques importants (unité centrale, disques, contrôleurs) doivent être sous protection automatisée au Halon, Co2 ou eau pulvérisée. Dans tous les cas, le système de détection incendie coupe l'alimentation électrique avant de déclencher le dispositif d'extinction.

Si le matériel fonctionne en permanence, ce dispositif déclenche une alarme auprès d'un service de gardiennage interne ou externe.

Dans le cas d'un centre informatique devant garantir une disponibilité importante, le dispositif de détection est relié au centre des pompiers le plus proche.

Dans le but de limiter l'impact d'un sinistre, les réserves de consommables sont entreposées dans une annexe de la salle informatique répondant aux mêmes conditions de sécurité.

L'ensemble de ce matériel est entretenu et testé de manière régulière par un personnel compétent. Ces opérations sont consignées sur un registre.

3.3 Protection électrique

Un onduleur redresseur avec batterie-relais est l'équipement minimum permettant un arrêt "propre" de l'ordinateur. Toutefois, ce système doit être complété d'un groupe électrogène lorsque l'activité de l'entreprise impose une disponibilité permanente du système informatique.

Dans ce dernier cas, le centre informatique dispose généralement des équipements suivants :

- un groupe électrogène, éventuellement doublé, capable d'alimenter l'ensemble des moyens informatiques (unités centrales, périphériques, climatisation et réfrigération),

- alimentation électrique sécurisée par une ou deux lignes EDF enterrées,
- les lignes EDF arrivent dans un local sécurisé (infrastructure physique et contrôle d'accès),

L'ensemble de ce matériel est entretenu et testé de manière régulière par un personnel compétent. Ces opérations sont consignées sur un registre.

3.4 Climatisation / Réfrigération

Lorsque la configuration informatique est d'une certaine importance (mainframe ou gros mini), ou que les conditions climatiques l'exigent, un dispositif de climatisation régule la température et l'hygrométrie des locaux abritant le matériel informatique (unité centrale et périphériques).

Ce dispositif déclenche généralement une alarme lorsque la température ou l'hygrométrie ne sont plus dans les normes admises par le constructeur du matériel.

Certaines unités centrales refroidissent leurs composants par un circuit d'eau réfrigérée, en complément de la climatisation.

Dans le cas d'un site sécurisé, l'ensemble de ces équipements de climatisation / réfrigération est redondant et toute défaillance est transmise à un service de surveillance interne ou externe.

Dans tous les cas de figure, l'ensemble de ce matériel est entretenu et testé de manière régulière par un personnel compétent. Ces opérations sont consignées sur un registre.

3.5 Contrôle des accès

L'ensemble des équipements informatiques est installé dans une salle dont l'accès est limité et contrôlé (badge, clé, digicode, etc.).

Dans le cas d'un centre informatique devant garantir une sécurité optimale, les unités centrales, disques, contrôleurs sont dans une salle dont l'accès est limité au seul personnel de maintenance ainsi qu'à l'équipe système. Les équipements nécessitant une intervention manuelle régulière sont dans une salle machine classique (imprimante, dérouleurs de bandes ou cartouches).

3.6 Conditions d'hygiène

Tout matériel informatique impose une propreté certaine de l'environnement de travail. Il convient notamment de s'assurer que la salle machine est correctement rangée et nettoyée.

Si cette salle dispose d'un faux plancher, celui-ci est nettoyé régulièrement (une à deux fois l’an).

3.7 Maintenance du matériel

Lorsque les pannes matérielles pénalisent le fonctionnement du système d'information, différentes causes peuvent être identifiées :

- matériel obsolète, mal utilisé ou surchargé,
- maintenance préventive défaillante.

Dans le but de s'assurer de la maintenance régulière du matériel, l'existence des documents suivants est vérifiée :

- contrat de maintenance,
- registre permettant de retracer les interventions.

Un contrat de maintenance n'est pas indispensable pour une configuration micro mono-poste dès l'instant qu'il s'agit d'un matériel standard utilisé pour des applications non stratégiques.

3.8 Contrat d'assurance des biens informatiques

Le coût d'une configuration informatique nécessite qu'une assurance soit souscrite pour couvrir les risques suivants :

- incendie,
- dégâts des eaux,
- vol,
- vandalisme,
- catastrophes naturelles,
- pertes d'exploitation,
- reconstitution des média.

Cette police couvre l'ensemble des équipements. Une attention toute particulière doit être portée sur la mise à jour de la liste du matériel déclaré au fur et à mesure des évolutions de configuration (cet aspect administratif est souvent négligé par les informaticiens). Lorsque la valeur déclarée correspond à une valeur de remplacement, il importe de réévaluer au minimum une fois l'an la valeur déclarée de chaque bien car :

- des modifications de configuration impliquent d'entrer les nouveaux biens et de sortir les anciens,
- la valeur du matériel ayant tendance à baisser, la valeur de remplacement d'un matériel équivalent suit généralement une courbe descendante au fur et à mesure de son obsolescence.

3.9 Plan de back-up (Voir Cobit DS 4)

3.9.1 PROBLEMATIQUE :

Le système d'information est souvent un élément stratégique, voire vital, de l'organisation de l'entreprise. Aucun équipement ou centre informatique ne peut garantir une disponibilité de 100 % dans le temps. Lorsqu'il ne s'agit pas d'une insuffisance de sécurité physique, cela peut être simplement un mouvement de grève qui paralyse le centre de traitement. Pour exemple, les grèves de 1981 ont bloqué totalement le CTI parisien d'une grande banque durant plusieurs semaines. Le plan de back-up n'est donc pas un exercice intellectuel mais une démarche de bon sens destinée à prévoir un risque qui, aussi faible soit-il, existera toujours.

Lorsqu'un décideur ne perçoit pas l'utilité d'une telle démarche posez lui les questions suivantes :

- Si ce soir votre équipement informatique est hors service, combien de temps votre entreprise peut-elle fonctionner ?
- Quelles sont les applications les plus indispensables à l'entreprise ?
- Comment, et à quel prix, les informaticiens et les utilisateurs vont ils restaurer le système d'information ?
- Existe-t-il des procédures dégradées pour fonctionner temporairement en mode manuel ?

Aucun décideur prudent et avisé ne peut rester indifférent à cette problématique. Mais il est assez fréquent de constater que cette éventualité n'a jamais donné lieu à une ébauche de solution, et même plus, à la mise en place d'une procédure réaliste et formalisée.

Les solutions reposant sur la confiance envers un fournisseur et sa promptitude à dépanner son client dans les meilleurs délais ne sont que feu de paille. En effet, un sinistre informatique déstabilise les hommes et l'organisation de l'entreprise. Dans un tel contexte, l'improvisation et la créativité se révèlent généralement insuffisants. Les gens inconséquents comptent souvent sur la chance mais c'est rarement l'approche idéale.

Toute la difficulté de cet exercice consiste à prévoir une situation de crise généralement inconnue :

- quels sont les moyens matériels, logiciels et humains nécessaires aux différents scénarios,
- comment préparer leur mise en œuvre rapide,
- quelles sont les applications à sauvegarder et selon quelles priorités (cette seule question est du ressort des différentes Directions de l'entreprise et en dernier lieu de la Direction Générale).

Toute cette démarche n'a de sens que si elle est formalisée et régulièrement testée.

3.9.2 PREMIERE ETAPE : LE SITE DE BACK-UP

La première question reste la plus délicate : sur quel matériel de secours va-t-on fonctionner ?

Solutions	Remarques
Utilisation d'un autre CTI de l'entreprise	C'est la meilleure solution car la plus maîtrisable (encore faut-il avoir des sites de puissance comparable)
Passer un contrat de back-up avec une firme spécialisée	C'est une solution coûteuse mais un professionnel du back-up apporte des conseils sur le plan technique et impose des tests périodiques (souvent 2/an)
Passer un contrat avec une entreprise disposant de matériel similaire	C'est souvent scabreux et inopérant car cela suppose beaucoup de rigueur et de volonté de part et d'autre
Disposer d'une salle machine externe (vide) et négocier une livraison rapide avec les fournisseurs de matériels	Cette solution suppose un temps de mise en œuvre relativement long

Toutes ces solutions supposent une charte voire un contrat précis indiquant les modalités et obligations des parties.

Tout plan de back-up suppose l'existence de sauvegardes externes récentes et complètes (données, programmes et système d'exploitation)

3.9.3 SECONDE ETAPE : LA DEMARCHE DU PLAN DE BACK-UP

Passée cette première étape, il reste la mise en œuvre opérationnelle de ce plan ce qui suppose :

- la détermination des applications prioritaires dans le cadre du plan,
- l'évaluation périodique des applications pouvant être secourues sur le (les) site(s) de secours et éventuellement la mise à niveau des performances de leurs équipements ainsi que des moyens de télécommunications,
- le contrôle périodique de la compatibilité des systèmes d'exploitation et de leur paramétrage,
- la rédaction et la mise à jour des procédures de mise en œuvre,
- éventuellement la négociation d'un contrat de livraison rapide pour certains équipements informatiques.

Cette démarche de remplacement des ressources matérielles du système d'information peut être complétée par des procédures, dites "dégradées", permettant aux utilisateurs de travailler manuellement en l'attente d'une remise en service du système informatique.

Certaines entreprises intègrent le plan de back-up (informatique) dans une démarche de plan de secours de l'entreprise. Celui-ci constitue une approche plus globale de substitution d'une "unité administrative" (qui peut être le siège de la société) en cas de sinistre grave.

4 CONDITIONS D'EXPLOITATION (VOIR COBIT DS 10 11 13)

Les procédures appliquées lors de l'exploitation des applications ont une influence directe sur l'exactitude et les délais des traitements et donc sur la qualité du service.

4.1 Planification et suivi de l'exploitation

Toute exploitation suppose un enchaînement de trois phases :

- planification,
- préparations,
- lancement et suivi.

La planification consiste à ordonnancer les travaux à lancer compte tenu :

- des besoins des utilisateurs,
- des contraintes de charge machine (CPU / disques / bandes, etc.),
- de certaines incompatibilités (2 jobs ne peuvent pas mettre à jour simultanément le même fichier ou encore certains travaux batch ne peuvent pas "passer" si le fichier à traiter est utilisé par une application fonctionnant en temps réel).

La préparation consiste à recenser et mettre à disposition des pupitreurs l'ensemble des moyens nécessaires au lancement des traitements :

- bande, cartouches, pré-imprimés,
- paramètres des JCL.

Le lancement et le suivi des traitements sont le travail principal du pupitreur qui doit :

- lancer les job préparés conformément au planning et aux possibilités matérielles,
- suivre leur exécution et surtout leur bonne fin,
- mettre à jour le planning après exécution des traitements,
- ranger les supports magnétiques utilisés et dispatcher les états.

L'objectif de qualité consiste donc à s'assurer que ces étapes sont respectées, contrôlées et formalisées.

Si les utilisateurs lancent l'exploitation en temps réel , cette approche par étape n'est pas possible.

4.1.1 CONTROLE DE LA PLANIFICATION

S'assurer que le planning transmis au préparateur ou au pupitreur est élaboré de manière cohérente (on sait quel job on va lancer) et de manière formalisée (ce document doit être suffisamment clair et explicite).

Souvent un document pré-renseigné indique les traitements récurrents, ainsi seuls les travaux exceptionnels restent à planifier. Lorsqu'un tel système n'existe pas ou que l'exploitation n'est pas récurrente, comment s'assurer de l'exhaustive de la préparation ?

Pour les travaux exceptionnels, comment le préparateur s'assure-t-il que cette demande est autorisée par la hiérarchie?

4.1.2 CONTROLE DE L'EXECUTION DES TRAITEMENTS

Le pupitreur doit s'assurer que:

- les travaux sont lancés conformément au planning,
- les fichiers utilisés par le traitement sont bien ceux prévus par le planning ou la préparation. Ce problème est particulièrement important lorsqu'il s'agit de bandes magnétiques,
- les traitements se terminent sans code erreur, sinon voir la procédure "incidents d'exploitation",
- le planning / cahier pupitre est tenu en inscrivant les heures de début et de fin de traitement.

Un responsable d'exploitation doit assurer une supervision de ces travaux.

4.1.3 CONTROLE DES INCIDENTS D'EXPLOITATION

Toute exploitation, qu'elle soit sur bande ou sur disque comporte nécessairement des incidents pour lesquels il convient de s'assurer que :

- ces incidents sont consignés sur un registre supervisé quotidiennement par le responsable de l'exploitation,
- pour chaque incident, le pupitreur dispose d'une documentation d'exploitation suffisamment complète, exhaustive et à jour pour savoir comment reprendre le traitement (point de reprise),
- le pupitreur ne débloque pas certaines situations au moyen d'un utilitaire permettant de modifier :
    - les données d'exploitation (pour éditer un fichier et annuler l'enregistrement qui pose problème),
    - le source ou l'objet du programme "planté".
- le pupitreur ne dispose pas des commandes permettant d'ignorer certains messages système
- les fichiers d'exploitation sont catalogués, leur durée de péremption est correctement établie,
- les bandes magnétiques sont stockées sans anneau d'écriture.

4.2 Contrôle des traitements

Un contrôle de qualité d'exploitation est mené selon deux axes.

Un contrôle de continuité des traitements doit permettre de s'assurer que l'ensemble des enregistrements devant être traités par une chaîne, l'ont été effectivement. Pour cela on utilise soit des fichiers de chiffrier afin de suivre les volumes (souvent en nombre et en flux) à chaque étape d'une chaîne. Certains progiciels permettent d'automatiser ce contrôle en vérifiant des règles paramétrées pour chaque traitement.

Un contrôle après exploitation vise essentiellement à s'assurer de la cohérence des états de sortie.

La diffusion des états auprès des utilisateurs doit être suffisamment fiable pour garantir :

- l'arrivée au destinataire,
- la confidentialité de certains états.

Afin de préserver la piste d'audit, les documents de préparation et exécution sont archivés. Dans un même esprit, le mouchard système (loging) doit être sauvegardé régulièrement.

5 PROCEDURE DE SAUVEGARDE

Il n'est pas nécessaire de rappeler l'importance de la sauvegarde des fichiers (programmes, données, JCL, système..). Toutefois, avant de "plonger" dans la procédure nous devons garder à l'esprit certains principes généraux.

La procédure de sauvegarde peut avoir trois approches qui sont :

- la sauvegarde applicative suppose une procédure mise en œuvre au niveau de chaque application (fichier, mode de stockage, rétention); cette approche est typiquement l'héritage des systèmes batch,
- la sauvegarde globale consiste à copier des bibliothèques entières,

Toute sauvegarde n'a d'intérêt que si elle est réutilisable et donc il est impératif de procéder à des vérifications de relecture.

Les sauvegardes sont faites notamment pour permettre de restaurer les fichiers en cas de sinistre grave. Il est donc **indispensable** qu'un jeu de sauvegarde des fichiers stratégiques soit périodiquement stocké en un lieu externe (hors usine ou siège social). En effet, les sauvegardes sont nécessaires en cas de destruction totale du site informatique (et donc des armoires plus ou moins ignifugées) ainsi qu'en cas d'indisponibilité. Pour mémoire la grève des centres informatiques d'une grande banque a empêché un réel back-up car le stockage externe des sauvegardes était insuffisant.

L'ensemble de ces supports magnétiques fait l'objet d'une rotation entre le CTI et le site de sauvegarde externe. Il est donc impératif qu'un logiciel ou un registre conserve la tracœ de cette rotation.

En fin d'exercice comptable des mesures toutes particulières doivent être prises dans le cadre du contrôle des comptabilités informatisées.

5.1 Description générale

Une cartographie globale doit décrire la stratégie de sauvegarde : périmètre, type de sauvegardes, périodicité, applicative / générale, lieu de stockage.

5.2 Procédure régulière

Il convient d'analyser en détail cette procédure pour apprécier la qualité générale des sauvegardes. Pour chaque lot de sauvegarde (applicative / générale) il est nécessaire de recueillir les informations suivantes :

- quels fichiers sont concernés,
- les sauvegardes sont faites en copie intégrale / incrémentale/ différentielle
- sur quel supports,
- conservé où et pour quelle durée,
- comment tous ces volumes de stockage sont ils gérés ?

5.3 Procédure de fin d'exercice

En fin d'exercice, diverses sauvegardes spécifiques doivent être effectuées. Elles ont pour objectif de figer, à des fins d'archivage, les données essentielles de comptabilité et de gestion. Au delà du bon sens, cette mesure est imposée par la loi.

Il est nécessaire de conserver, durant trois exercices, les sauvegardes des fichiers au 31 décembre afin de pouvoir satisfaire à un éventuel contrôle de l'administration fiscale (art 54 du CGI décret 82-1148 du 29/12/82). Ces textes font référence à la fourniture par l'entreprise contrôlée "*des informations, données et traitements automatiques de toute nature dès lors que ces informations, données ou traitements concourent directement ou indirectement à la formation des résultats comptables ou fiscaux de la période vérifiée*" (art 2 du décret 82-1148).

De surcroît, ces dispositions ont été renforcées par la loi de finance 1990 (art L102B et L74 du Livre de Procédures Fiscales). Lorsque, faute d'avoir conservé les fichiers et la documentation, l'entreprise ne peut satisfaire aux demandes de l'administration, celle-ci peut appliquer une évaluation d'office pour opposition à contrôle. Voir aussi à ce sujet l'instruction du 24/12/96.

6 MISE EN PRODUCTION (VOIR COBIT AMP5)

6.1 Enjeux et risques : La mise en production est une étape sensible dans la vie d'un projet

En effet, c'est un changement de phase dans le cycle de vie d'une application. Les principes du contrôle interne conduisent à une analyse selon deux axes.

C'est un point critique car on passe entre deux environnements réputés étanches, celui des études et celui de l'exploitation (principe de séparation des fonctions). En outre, cette « bascule » peut être irrémédiable même en cas de difficultés. Enfin, une migration de données plus ou moins lourde et complexe peut être nécessaire.

C'est une étape qui souvent marque un changement de procédures et de mode opératoire pour les utilisateurs. Enfin, on constate souvent une rupture en matière d'organisation des données par la modification ou la mise en place de nouvelles bases de données

C'est pourquoi, un découpage en étapes successives est nécessaire au succès de la mise en production :

- Préparation
- Mise en œuvre
- Surveillance

Compte tenu du caractère technique de ce sujet nous n'abordons que les têtes de chapitre de cette procédure.

6.2 l'étape de préparation a pour objet de

- Constituer la documentation d'exploitation
- Identifier les procédures de reprise nécessaires en cas d'incident
- Mettre à jour l'ordonnanceur d'exploitation ou le planning, afin d'y intégrer les nouveaux traitements
- Paramétrer les fichiers ou base de données
- Prendre en compte les nouvelles données dans la procédure de sauvegarde globale
- Préparer les étapes ultérieures du plan de mise en production (migration des données notamment)

6.3 mise en œuvre

- Référencer tous les composants devant passer en production,
- Mise en œuvre de la migration

- Cette étape est souvent indispensable lors de la mise en place d'une nouvelle application
- Une migration est en soit un sous projet qu'il convient de préparer dès le début du projet

- Contrôle final et supervision
- Mise en production effective

6.4 surveillance

A la suite d'une mise en production, il convient d'être particulièrement vigilant et de maintenir sous surveillance les nouveaux composants afin de prévenir les dysfonctionnements.