Mémento
Revue Générale Informatique

1 OBJECTIF DU MEMENTO RGI

Le présent mémento est un document de travail pour le CAC devant réaliser une revue générale informatique (RGI). L'objectif d'une telle mission est de mettre en évidence les forces et les faiblesses des contrôles généraux informatiques. La RGI vient en complément de la collecte d'informations du dossier permanent (première partie de la feuille de travail de RGI).

Le présent document vous permet de mettre en œuvre la feuille de travail de RGI pour sa seconde partie relative à la sécurité. Cette partie étant relativement technique, il convient de mettre à disposition du CAC un support lui permettant de mieux comprendre le contexte, les objectifs de contrôle et les moyens de les mettre en œuvre.

En conséquence, ce document a pour objectifs :

- de mettre en place une approche standardisée servant de squelette à toutes les revues de sécurité,
- faciliter la tâche des auditeurs non habitués à ce travail en leur indiquant, pour chaque domaine étudié, l'objectif et les moyens de le réaliser.

Ce document est générique, les cas de figure sont innombrables suivant la taille, l'organisation et la culture de l'entreprise… sans parler de son informatique. Par principe, il n'est donc pas adapté à « votre mission ».

Remarque relative au niveau d'exigence attendu.

Ce document procède par assertions fondées sur des bonnes pratiques de haut niveau qui ne s'imposent pas nécessairement chez « votre client ».

Relativisez tout cela avec le caractère stratégique du système d'information et la capacité de l'entreprise à le remettre en marche après un sinistre. Une PME ne dispose pas (en général) d'une vraie salle sécurisée pour ses serveurs (accès, incendie, etc). Cette situation ne constitue pas nécessairement une faiblesse. A l'auditeur d'apprécier ce risque en fonction des impacts et du niveau de sécurité attendu.

Le document de RGI vous assiste dans cette évaluation du risque inhérent lié au SI selon deux axes :

- l'exigence de disponibilité du SI => que se passe-t-il si on n'a plus accès aux applications ou données en fonctions de leur importance opérationnelle et de l'existence de procédures dégradées[1].
- l'exigence de confidentialité des données selon qu'il s'agit de données qui relèvent du confidentiel défense, de la loi informatique et liberté[2], des brevets et secrets de fabrication.

Dernière remarque préalable, la revue de sécurité peut se dérouler à plusieurs « niveaux de profondeur » comme toute mission d'audit, selon les objectifs et le budget assignés. Il n'est pas nécessairement utile au CAC de PME de vouloir valider le contrôle interne qui lui est décrit.

Dans de telles conditions et avec l'expérience, il lui est possible de réaliser une RGI avec le support joint en une journée environ.

2 RAPPEL HISTORIQUE DE L'INFORMATIQUE DE LA SOCIETE

Objectif de travail :

[1] Aussi appelées des « contournements », il s'agit d'une organisation manuelle ou semi-manuelle pour pallier une indisponibilité du SI

[2] Et tout particulièrement les données de santé

La connaissance de l'informatique de la société permet d'apprécier la situation actuelle d'une manière circonstancielle et de la situer dans une perspective historique. Enfin, cette prise de contact permet de situer les principales zones de risque (démarche type Revue Analytique Générale).

Moyens :

Entretien avec la direction informatique et les utilisateurs. On retiendra les dates clés, les échecs et les principales évolutions.

3 SECURITE PHYSIQUE

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 éventuellement un plan de back-up permettant de pallier une défaillance partielle ou totale du matériel informatique.

Dans le domaine de la sécurité physique, le bon sens doit naturellement conduire l'auditeur à se poser les questions relatives aux exigences de sécurité :

- Quelle est la dépendance stratégique et financière de l'entreprise vis-à-vis de son système d'information ? A titre d'illustration celui d'un cabinet d'expertise comptable est tout aussi indispensable que celui d'une banque ou d'une assurance… s'il ne fonctionne pas les journées des collaborateurs sont quasi perdues, les saisies non faites, les déclarations non transmises, etc.
- Utilisation de matériels standards ou atypiques ? Un réseau construit autour de PC standardisés et de serveurs aisément disponibles dans la plus proche ville ne se reconstruit pas comme celui qui dispose d'un mini-ordinateur plus sophistiqué et ou d'équipement réseau complexes.
- Capacité de l'équipe interne à reconstruire un SI même dégradé.
- Equilibre de la situation, des mesures de réduction[1] de risque et de réduction d'impact[2].

3.1 Infrastructure physique

Objectifs de travail :

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.) ou autre risques (poussières, explosifs, sources de chaleur).

La salle informatique est entourée de murs "en dur", l'idéal étant une pièce aveugle donc sans fenêtre. Les éventuelles 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 selon les exigences de sécurité :

- d'un centre informatique devant être hautement sécurisé,
- d'une configuration de moindre importance,

[1] Cette mesure réduit le risque de survenance telle la surveillance des paramètres techniques des disques ou encore l'utilisation d'une architecture RAID pour prévenir une perte de données.

[2] Cette mesure permet de pallier le risque comme la sauvegarde des données qui n'empêche pas un disque de tomber en panne, mais limite ses conséquences.

- d'un système micro utilisé dans un service utilisateur.

Moyens :

- entretien avec le responsable informatique,
- observation.

Sur ce dernier point, faites confiance à votre bon sens et observez. Un plafond (ou des murs) où il y a des traces d'humidité doit déclencher des questions : pourquoi ? quand ? Quelles mesures ont été prises ?

Sur la qualité des locaux, observez murs pleins ou simples cloisons, fenêtres simples avec ou sans barreaux, en rez de haussée ou sous un toit-terrasse…

3.2 Protection incendie

Objectifs de travail :

Pour une installation stratégique et complexe, s'assurer de l'existence et de l'efficacité des moyens de protection incendie. Les matériels informatiques importants[1] doivent être sous protection automatisée au Halon[2], Co2 ou eau pulvérisée, gaz FM 200 ou autre.

Dans tous les cas, le système de détection incendie coupe l'alimentation électrique avant de déclencher le dispositif d'extinction. Il est à noter que le Halon est progressivement interdit et que les dispositifs à Sprinkler sont une alternative crédible en la matière.

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

Si le matériel fonctionne en permanence ou selon le niveau d'exigence de sécurité, ce dispositif déclenche une alarme auprès d'un service de gardiennage interne ou externe (télésurveillance).

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

Pour une configuration PME, avec des serveurs « classiques », un tel dispositif ne s'impose pas nécessairement, car ce type de serveur peut être remplacé aisément dès l'instant que des mesures conservatoires sont prises par ailleurs (sauvegardes, organisation du back-up…). Ici encore, tout dépend de l'exigence de disponibilité du SI.

Moyens :

- entretien avec le responsable sécurité ou le responsable de la salle machine :
- description du dispositif,
- revue des contrats d'entretien,
- fait-on régulièrement des essais du système de détection / extinction ?
- observation (affichage des consignes),
- entretien avec un pupitreur[3] pour savoir si le personnel sait ce qu'il doit faire en cas de sinistre.

3.3 Protection électrique

---

[1] L'importance doit être appréciée tant sur des critères financiers que stratégiques.

[2] Les installations d'extinction au Halon sont interdites depuis janvier 2003 et doivent être démantelées depuis janvier 2004.

[3] Ce sont les techniciens qui surveillent les serveurs et interviennent en salle machine si nécessaire.

Objectifs de travail :

Un onduleur redresseur avec batterie-relais est l'équipement minimum permettant une protection contre les microcoupures et les écarts de tension d'alimentation. Les batteries assurent par ailleurs une autonomie minimale puis un arrêt "propre" de l'ordinateur en cas de coupure. Toutefois, ce système peut être complété par 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 (valider infrastructure physique et contrôle d'accès de ce local).

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

Remarques :

- Dans la grande majorité des cas, il suffit d'onduleur avec batterie relai qui coutent de 100 à 200€ et permettent de faire fonctionner le serveur sur une durée proportionnelle aux capacités de la batterie.
- La connexion[1] onduleur / batterie permet au serveur de s'arrêter proprement lorsque les batteries ont atteint un seuil critique.
- L'utilisation d'un ordinateur portable permet de s'affranchir des coupures et microcoupures.
- Attention, pour faire fonctionner l'ensemble du SI en cas de coupure électrique, il faut que l'ensemble des équipements (serveurs, équipements réseau, poste de travail) soient en réalité sur un réseau secouru.

Moyens :

- entretien avec le responsable sécurité ou le responsable de la salle machine,
- description du dispositif,
- revue des contrats d'entretien,
- observation.

3.4 Climatisation / Réfrigération

Objectifs de travail :

Si l'entreprise utilise des serveurs micro classiques, une climatisation de bureau suffit amplement, surtout si le matériel est isolé dans une pièce sans fenêtre.

Lorsque la configuration informatique est d'une certaine importance (mainframe ou gros mini), ou que les conditions climatiques[2] 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.

[1] Souvent via un câble USB et un logiciel installé sur le serveur

[2] Par exemple 3 serveurs dans un réduit d'un mètre carré, matériel situé derrière une baie vitrée exposée sud, etc

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.

Moyens :

- entretien avec le responsable sécurité ou le responsable de la salle machine :
- description du dispositif,
- revue des contrats d'entretien,

3.5 Contrôle des accès aux équipements

Objectifs de travail :

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'une sale aveugle, ce contrôle d'accès est plus facile à mettre en place.

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).

Moyens :

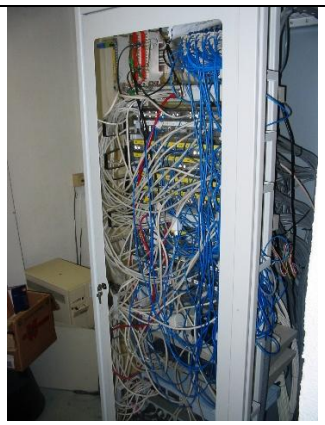
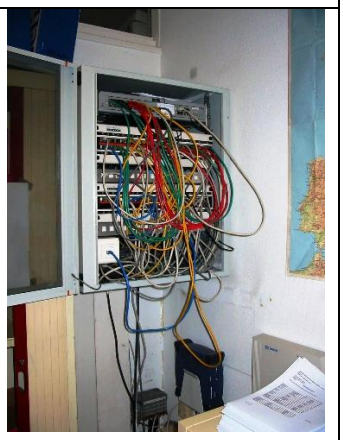
- entretien avec le responsable de la salle ordinateur,
- observation.

3.6 Conditions d'hygiène

Objectifs de travail :

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. Le fait que des câblages réseaux ou électriques donnent l'impression d'une organisation défaillante est souvent le résultat d'une incompréhension (voir ci-après).

Si cette salle dispose d'un faux plancher, celui-ci est nettoyé régulièrement. Il convient d'éviter la présence de matériels inutilisés, de stock de papier, bref de toute chose sans objet. Un contrôle visuel permet de déceler des traces d'humidité, de poussière excessive ou d'autres risques. Il est préférable que cette salle soit dédiée aux matériels informatiques sans nécessiter un accès régulier. Dans cet esprit, les imprimantes sont installées à l'extérieur de cette salle.

Exemple d'une baie de brassage des postes informatiques qui donne une impression de fouillis, mais c'est normal pour un câblage réseau. L'important est le repérage des prises et la documentation de ce câblage. Ici sont brassés quelque 50 postes et autant de téléphones.	
Autre exemple de brassage avec moins de postes	
Exemple d'une configuration basique 1 Box, 5 postes, 1 imprimante et 1 NAS, cela fait déjà pas mal de câblage et toujours cette même impression de fouillis.	

Moyens :

- entretien avec le responsable sécurité ou le responsable de la salle machine,
- observation.

3.7 Maintenance du matériel

Objectifs de travail :

Dans le but de préserver la disponibilité du SI, il importe de vérifier l'existence de conditions de maintenance régulière du matériel[1] , l'existence des documents suivants est vérifiée :

- contrat de maintenance établi avec un professionnel de cette activité,
- registre permettant de retracer les interventions.

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.

Un contrat de maintenance n'est pas indispensable pour une configuration micro monoposte dès l'instant qu'il s'agit d'un matériel standard utilisé pour des applications non stratégiques. A contrario, des serveurs de production hébergeant des applications stratégiques doivent bénéficier de contrat de support (assistance réparation intervention) avec des délais (intervention + réparation) cohérent avec les exigences de sécurité (disponibilité) des applications concernées.

Moyens :

- entretien avec le responsable système ou le responsable informatique,
- analyse du registre des interventions afin d'évaluer leur nombre et leur impact,
- revue des contrats d'entretien.

3.8 Contrat d'assurance des biens informatiques

Objectifs de travail :

Cet objectif de contrôle apporte une forte valeur ajoutée pour le dirigeant, car on traite d'un sujet sensible. Hélas, ce travail d'épluchage de contrat consomme du temps. On peut procéder comme suit :

- le périmètre du contrat (ce qui est couvert et pour quels risques),
- le contrat est actualisé en cas de mouvement significatif du parc ; de quand date le dernier inventaire et le dernier avenant ? Quelle est la procédure ?
- les exclusions sont cohérentes et connues par la direction.

Remarques ;

- La décision de s'assurer (ou pas) est un acte de gestion qui relève de la direction.
- En règle générale, ce domaine n'est pas couvert pour une RGI dans un contexte CAC

Objectifs de travail :

[1] Serveurs, réseau et d'une manière générale tout ce qui est critique

Le coût des équipements peut nécessiter qu'une assurance soit souscrite pour couvrir les risques suivants :

- perte d'exploitation,
- reconstitution des données (remplacement des supports et non ressaisie des données),
- incendie,
- dégâts des eaux,
- vol,
- bris et vandalisme,
- catastrophes naturelles.

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.

Autre point important qui impose une lecture attentive du contrat, existe-t-il des obligations de sécurité à la charge de l'assuré qui n'étant pas appliquées, diminuent la valeur du contrat. Ainsi, il arrive qu'un contrat impose la mise en œuvre de mesure de sécurité « conforme à l'état de l'art. » sans spécifier concrètement le contenu de ces mesures. Une lecture attentive appuyée d'une dose de bon sens peut permettre la mise en évidence de ce type de piège.

Moyens :

- revue du contrat d'assurance pour recenser les risques couverts,
- revue de la procédure de mise à jour,
- vérification de la liste du matériel déclaré sur le dernier avenant.

3.9 Plan de back-up[1] (ou plan de secours informatique)

3.9.1 Problématique :

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. Les causes rendant un site inopérant peuvent être très variables :

- Accès au site impossible : grèves, émeutes, épidémie, inondation, éboulement, incendie
- Site non connecté en termes de réseau ou d'électricité

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. Cette étude doit naturellement tenir compte de l'évaluation des exigences de disponibilité faite en début de mission.

[1] On parle aussi de Disaster Recovery Plan

A ne pas confondre :

Quand une entreprise utilise une application hébergée dans le Cloud, c'est l'hébergeur qui garantit la permanence et la disponibilité du système. C'est d'ailleurs un des grands avantages du Cloud, pas de soucis de back-up. Il importe cependant de vérifier les niveaux de qualité de service prévus au contrat (voir Garantie de Temps de Rétablissement).

Le back-up ne remplace pas les sauvegardes. Si le matériel est volé ou détruit, les sauvegardes seront nécessaires à la remise en marche des nouveaux serveurs. Si l'application est hébergée, le fournisseur fait son affaire des sauvegardes et du back-up.

Le back-up ne remplace pas les disques RAID qui ne sont que des dispositifs de tolérance de panne[1] pour maintenir l'accès aux données.

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 éventualités du style : on fait confiance à notre fournisseur pour nous dépanner 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.

Car 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).

A retenir :

Le back-up informatique est une démarche d'analyse et de prévention des risques afin de pallier toute indisponibilité partielle ou totale du système d'information par une combinaison de mesures de prévention et de réduction d'impact.

Un plan de back-up n'a de sens que s'il est formalisé et régulièrement testé.

Toute organisation n'a pas le même besoin en la matière selon son exigence de disponibilité de son système d'information. Certaines n'en ont pas besoin du tout.

[1] L'information est répartie sur plusieurs disques de manière à ce que la panne d'un disque soit transparente pour l'utilisateur. Il doit seulement mettre dans le bon emplacement un disque neuf. Dans la version la plus simple, il ne s'agit que d'un mirroring entre deux disques.

3.9.2 Première étape : définir le besoin

Les serveurs hébergent différentes applications informatiques, mais toutes n'ont pas la même importance. Il est donc nécessaire de déterminer celles qui sont suffisamment stratégiques pour nécessiter d'être secourues par le back-up informatique[1].

Le site de back-up

Pour les applications devant être secourues, la question la plus délicate est : 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 comparables => réservé aux grandes entreprises)
Passer un contrat de back-up avec une firme spécialisée	C'est une solution couteuse, 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 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). Enfin, toutes ces mesures nécessitent des tests et un processus de suivi-amélioration.

3.9.3 Seconde étape : La démarche 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.

3.9.4 Les mesures dégradées

[1] Dans une organisation au SI complexe, on commence par analyser la dépendance vis-à-vis de chaque application métier afin de déterminer celles à secourir en cas de besoin.

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.

La procédure dégradée est une organisation qui prévoit l'organisation du travail en cas d'arrêt partiel ou total du SI. En d'autres termes, on va éventuellement fonctionner en manuel durant 2 jours, mais cela a été conçu, organisé et documenté.

Les options du mode dégradées sont multiples :

- Seules les applications critiques sont accessibles afin de limiter la charge des serveurs,
- Des applications sont mises en place sur de nouveaux serveurs (après installation de ceux-ci),
- En PME on peut installer une application en mono poste sur un PC,
- Enfin, il y a le mode réellement manuel qui consiste à diffuser des états aux utilisateurs. Les transactions sont initiées par des documents papier (ou par un formulaire transmis par messagerie).

Pour approfondir le sujet du plan de secours informatique, lisez l'étude réalisée par la CLUSIF[1] : http://www.clusif.asso.fr/fr/production/ouvrages/pdf/PlanContinuiteActivite.pdf

Certaines entreprises intègrent le plan de back-up (informatique) dans une démarche de plan de secours de l'entreprise souvent appelé Plan de Continuité d'Activité. 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.

Objectifs de travail :

Prendre connaissance du contexte et des modalités retenues pour en apprécier l'efficacité potentielle au regard des niveaux de sécurité attendus.

Moyens :

- entretien avec le responsable sécurité ou le responsable informatique,
- éventuellement consulter la Direction Générale.

[1] Club de la Sécurité de l'Information Français : http://www.clusif.asso.fr/

4 SECURITE LOGIQUE

La sécurité logique est constituée de l'ensemble des mesures destinées à protéger les données et les logiciels qui en assurent le traitement. Elle conditionne fortement la confidentialité des données et la séparation des fonctions de l'entreprise.

Des comptes utilisateurs collectifs et des mots de passe connus de tous sous-entendent que tout utilisateur peut consulter les données, passer des transactions, modifier des tarifs bref qu'il n'y a aucune séparation des fonctions et que le contexte favorise la fraude.

4.1 Limitation des accès aux données et programmes

Contexte :

L'accès aux données et aux logiciels est fondamental pour le respect du contrôle interne. Certains documents de doivent pas être publics à l'ensemble des collaborateurs ; il en est de même de certaines applications. Tout cela relève d'un choix de la direction générale qui doit donc valider a minima les objectifs, même si elle délègue les modalités de mise en œuvre et de contrôle. Autrement dit, la direction générale doit normalement savoir un minimum de chose sur le contrôle d'accès. La réalité est tout autre.

Autre manière de voir le sujet. Si le management abandonne ce sujet en laissant l'informaticien interne (ou pire externe) définir les règles de sécurité qu'il considère comme bonne, il ne faudra pas lui tomber dessus en cas de manquement.

Organisation concrète du contrôle d'accès

Ce contrôle d'accès se réalise généralement à deux voire trois niveaux :

1. L'accès au poste de travail et l'ouverture d'une session sur le réseau (contrôle assuré par Windows, TSE, Citrix [1]..). Chaque utilisateur est rattaché à un ou plusieurs groupes d'utilisateurs qui lui accordent des droits en lecture et écriture sur des disques réseau[2]. Ce mécanisme contrôle l'accès aux fichiers. Il peut aussi être utilisé pour filtrer l'accès aux logiciels.
2. L'accès aux différentes fonctions au sein d'un logiciel. Ce contrôle est généralement assuré par le logiciel en question qui a pu pour cela demander à l'utilisateur un code utilisateur et un mot de passe lors de son lancement. Toutefois, cette organisation impose à chaque utilisateur de mémoriser des codes d'accès pour chaque application.
3. Pour éviter cette situation qui incite les utilisateurs à inscrire leurs mots de passe sur des papiers, des logiciels dénommés Single Sign On (SSO) agissent comme un véritable serveur d'authentification vis-à-vis de chaque logiciel ayant besoin d'une autorisation d'accès. Cela fait un logiciel de plus dans l'entreprise, mais il présente le grand avantage de permettre une administration centralisée et sécurisée des mots de passe applicatifs. Autrement dit, le SSO permet à l'utilisateur de ne plus avoir à retenir et gérer individuellement les mots de passe applicatifs. Certains SSO sont gratuits.

<u>Objectifs de travail :</u>

[1] Ces deux systèmes d'exploitation permettent de faire fonctionner des serveurs de traitement Windows alors que l'utilisateur ne dispose plus d'un PC, mais d'un terminal (clavier + écran).

[2] Aussi appelées ressources

Au cas présent, comment l'entreprise s'assure-t-elle que seuls les utilisateurs "autorisés" ont accès aux programmes et données qui les concernent ?

Point de contrôle :

- La mise en œuvre du contrôle d'accès est administrée et documentée
- L'affection des droits des utilisateurs (groupes) est approuvée par la hiérarchie de l'entreprise
- Chaque départ ou changement de fonction de collaborateur donne lieu à une information écrite à l'administrateur de la sécurité pour application
- Chaque utilisateur dispose d'un code utilisateur public du type <première lettre prénom><nom> et d'un mot de passe, tous deux individuels
- La sécurité du poste de travail, celle du SSO et celle des logiciels métier imposent des mots de passe complexes
- Ces consignes sont rappelées et expliquées dans la charte des utilisateurs.

Moyens :

- entretien avec le responsable sécurité ou le responsable système,
- entretien avec un utilisateur pour confirmer,
- observation.

4.2 Séparation des environnements études / exploitation

Cet objectif n'a de sens que pour les organisations d'une « certaine taille » disposant donc de ressources informatiques qui permettent une séparation de fonction a minima. En PME, dans 98% des cas, il y a qu'un seul administrateur réseau qui traite les aspects techniques de la fonction informatique. Si tel est le cas, l'objectif est sans objet.

Objectifs de travail :

Les principes généraux du contrôle interne imposent que les personnes qui développent les applications ne puissent pas accéder aux fichiers de "production".

Cette séparation des environnements sous-entend que le personnel des études ne peut :

- accéder (même en consultation) aux fichiers de production,
- transférer ou modifier un programme en production (ce qui normalement suppose une procédure de recette en exploitation).

De même, le personnel d'exploitation ne peut pas avoir accès aux programmes en exploitation.

Deux cas de figure viennent limiter l'application de ce principe :

- lorsque le service informatique est composé de trop peu de personnes pour qu'une telle séparation des taches soit envisageable,
- lorsque les procédures de maintenance des applications ou de gestion des incidents d'exploitation autorisent les personnes concernées à intervenir directement sur les données de production.
- Dans tous les cas de figure, il faut être conscient que les administrateurs des serveurs et bases de données peuvent y intervenir, sinon ils ne peuvent travailler.

Moyens :

- entretien avec le responsable sécurité ou le responsable système,
- entretien avec un programmeur pour confirmer.

Points de contrôle :

- Comment sont organisés les groupes d'utilisateurs pour le personnel informatique
- Qui administre les groupes et sous quel contrôle
- Valide ton régulièrement le « contenu » des groupes, comment ?

4.3 Limitation des accès aux utilitaires et fichiers système

Certains utilitaires systèmes sont dangereux quand ils sont utilisés par des personnes incompétentes ou mal intentionnées. De plus, ces utilitaires ont souvent la propriété d'outrepasser les protections instaurées par un logiciel de sécurité. En conséquence, l'accès à ces utilitaires doit être strictement limité aux personnes qui en ont besoin (équipe système).

Il est fréquent que ce point ne soit pas traité en PME.

Objectifs de travail :

En premier lieu il s'agit d'évaluer la réalité et l'efficacité des mesures de sécurité pour limiter l'erreur ou la malveillance dans l'utilisation des outils du poste de travail.

Au-delà de ces mesures préventives, la grande majorité des systèmes peut conserver la trace des principaux événements passés (mouchard ou log système). Un tel dispositif, constitue une piste d'audit bien utile pour trouver l'origine de problèmes systèmes ou des fraudes. Les responsables sécurité informatique ou les audits "système" l'analysent sur différents critères. Il est donc impératif que ce mouchard soit sauvegardé périodiquement.

Point de contrôle :

- La configuration des postes de travail (sécurité Windows) et/ou le contrôle d'accès aux ressources réseau permettent de filtrer l'accès à ce type d'outil dans le but de prévenir le risque.
- La journalisation des évènements des postes de travail permet de retrouver l'historique des actions réalisées.
- Des outils de surveillance ou des contrôles (ponctuels ou systématiques) sont réalisés.

Moyens :

- entretien avec le responsable sécurité ou le responsable système,
- entretien avec un programmeur pour confirmer.

5 CONDITIONS D'EXPLOITATION

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

Dans les petites organisations, ce thème ne nécessite pas d'être traité, car les seuls traitements de nuit relèvent des sauvegardes et autres fonctions quotidiennes. Ce chapitre est alors sans objet.

5.1 Contexte et enjeux

Pour le néophyte, on peut résumer la problématique comme suit. Faire exécuter des centaines[1] de traitements chaque nuit suppose la mise en place d'une organisation pointue autour de deux objectifs :

1. La **planification** :

Chaque nuit les traitements[2] à lancer sont « différents » de par les conditions et paramètres de lancement. La précision de ces « réglages » conditionne l'exactitude et la bonne fin du traitement. Ainsi une chaine lancée pour un traitement hebdomadaire ne produit pas les mêmes résultats qu'en configuration quotidienne. L'omission d'un traitement comme l'erreur d'un paramètre vont changer le résultat ou produire une erreur.

Concrètement, cela peut se traduire par le fait qu'un fichier de virement fournisseur est généré (ou non), qu'un état est produit (ou non), qu'un fichier d'écritures est transmis au logiciel comptable (ou non). Ces considérations techniques ont donc des impacts très concrets sur les opérations quotidiennes et indirectement sur la qualité des informations comptables.

2. Le **contrôle** :

Quelle que soit l'attention portée à la planification, des incidents d'exploitation se produisent pour un ensemble de raisons. A titre d'illustration et sans être limitatif, citons :

- La taille maximum autorisée d'une table de la base de données est dépassée
- Un serveur de traitement ou de stockage de données n'est plus « accessible » (incident réseau, droit d'accès non mis à jour et/ou insuffisants) ou est physiquement défaillant
- Un paramètre de chaine de traitement est erroné ou incohérent
- Une donnée d'entrée de chaine est non conforme

Il est donc indispensable de surveiller en temps réel ou a posteriori les codes retour des traitements.

Explication sur les codes retour : avec votre explorateur Windows vous copiez un fichier macomptabilité.xls d'un répertoire D :\répertoire1 vers D :\répertoire2. Concrètement il suffit de faire copier-coller. La même chose faite en traitement automatisé consiste utiliser le langage de commande de Windows pour lui faire faire la même chose soit : *copy D:\répertoire1\ macomptabilité.xls D:\répertoire2.*

Après l'exécution d'une commande, il est possible de demander à Windows le « code retour » de la commande qui est 0 si tout s'est bien passé ou qui peut prendre différentes valeurs pour indiquer la nature des difficultés rencontrées.

Si cette commande doit être exécutée régulièrement, elle sera inscrite dans un fichier de commande, par exemple copie_fichier.bat.

---

[1] Voire des milliers dans les grandes organisations

[2] Les techniciens parlent de chaine ou de batch qui enchainent les programmes (ou étapes)

Jusqu'au milieu des années 1990, l'exploitation était principalement manuelle. Ceci signifie que des techniciens lançaient les traitements surveillaient leur déroulement et géraient les incidents. À peu près à la même époque, l'ordonnancement automatique a pris le pas progressivement. Il s'agit en l'occurrence de logiciels qui sont capables :

- De lancer des traitements en fonctions de condition logiques aussi variées que
  - Le traitement « x » est terminé avec un code retour à 0 (aucune erreur)
  - La date de traitement est (jour en cours) correspond à un mardi
  - La base de données « Vente » est disponible pour un traitement batch
  - La variable w789 (initialisée par le traitement x789) a une valeur à « 1 » ou « 2 »
- Mémoriser différentes séquences de traitements
- Surveiller les codes retour (erreur d'exécution du traitement) et prendre les mesures adéquates programmées en cas d'erreur. Ces *mesures* consistent à revenir à ce que l'on appelle **un point de reprise**, c'est-à-dire un point de l'enchainement des traitements où il est possible de reprendre ces derniers. En règle générale, un point de reprise correspond à une étape où l'ensemble des fichiers en mise à jour a été sauvegardé.
- Journaliser les paramètres d'exécution des traitements.

5.2 Contrôle de planification d'exploitation

Objectifs de travail :

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 va indiquer 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 ?

Moyens :

- revue des plannings (observation),
- entretien avec les utilisateurs,
- entretien avec le responsable exploitation et le préparateur.

5.3 Contrôle des incidents d'exploitation

Lorsque de nombreux traitements sont exécutés chaque nuit, il n'est pas rare que certains n'aillent pas jusqu'au bout pour diverses raisons techniques qui peuvent paraitre déconcertantes pour le profane.

Il est donc essentiel que les techniciens de l'exploitation surveillent (généralement chaque matin) la situation des traitements lancés la nuit afin de repérer tous les incidents qu'il faut rattraper.

Objectifs de travail :

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[1] 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 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,

Moyens :

- revue des statistiques d'incident ou du cahier de pupitre,
- entretien avec le responsable exploitation et le pupitreur,
- observation.

5.4 Contrôle des traitements

A la différence de ce qui précède, ce n'est pas un contrôle simplement technique, mais plutôt orienté métier. Il n'existe que dans les organisations importantes

Objectifs de travail :

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 bien 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 ces contrôles en vérifiant des règles paramétrées pour chaque traitement.

Un contrôle après exploitation vise essentiellement à s'assurer de la cohérence des états de sortie. Un exemple vécu, si votre traitement trimestriel synchronise des base de données puis produit environ 1 million de lettres qui seront mises sous plis puis affranchies avant d'être postées, il est prudent de mener des contrôles avant de « lancer » la mise sous plis afin de prévenir toute erreur de mise à jour des adresses. Dans un contexte de ce type, on peut faire un contrôle de cohérence des nombres de courriers émis par code postal.

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 (logging) doit être sauvegardé régulièrement (Cf. 4.2).

[1] Le format papier devient rare au profit du tableur ou des outils web de gestion d'incident tel Mantis

Moyens :

Entretien avec le responsable exploitation et le préparateur.

6 PROCEDURE DE SAUVEGARDE

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

6.1 Rappel de quelques principes

Commençons par la définition même de la sauvegarde : il s'agit de la recopie sur un support externe de données, programmes ou paramètres en vue du rétablissement d'un fonctionnement normal après une défaillance (détérioration du disque), une erreur (effacement), un accident (incendie) enfin, une malveillance (altération volontaire d'une base de données).

Eu égard à ces objectifs, les procédures de sauvegarde revêtent un caractère vital : elles sont destinées à assurer la continuité du système d'information dont l'entreprise a besoin pour fonctionner chaque jour.

6.2 Sauvegardes ou Archives, de quoi parle-t-on ?

La sauvegarde ne peut être confondue avec la notion d'archive : une sauvegarde ne « vaut » plus rien quelques jours seulement après sa création ; une archive, au contraire, est justement créée pour durer.

Les systèmes informatiques utilisent trois techniques complémentaires couvrant des objectifs de sécurité différents :

La **redondance RAID**: Sur un disque classique, l'information n'est inscrite qu'un seule fois. L'altération du support implique une perte souvent difficile à récupérer[1]. Il est donc nécessaire de changer le disque puis de restaurer la sauvegarde. La technique du Redundant Array of Inexpensive Disk[2] consiste à utiliser différentes approches de duplication de l'information ou sa répartition sur plusieurs disques. C'est donc une fonction technique orientée vers un fonctionnement temps réel (aussi appelée mirroring). Ce mécanisme est transparent (intégré à la baie de disques) pour les utilisateurs comme pour les informaticiens. Cette technologie est peu onéreuse et donc accessible aux PME.

La **réplication entre serveurs** : les données sont copiées régulièrement et systématiquement afin de permettre un démarrage rapide en cas de dysfonctionnement sur des serveurs de secours. Cela ressemble à la synchronisation d'un Google Drive ou d'un DROPBOX mais en plus sophistiqué.

La **sauvegarde** : il s'agit de stocker différentes versions (ou images) d'un même fichier afin de pouvoir revenir sur la version -1,-2,…-n lorsque l'on constate une dégradation d'un fichier ou pour identifier les modifications entre 2 versions. Ici encore la fonction est technique. En l'absence de réplication c'est la sauvegarde la plus « fraîche » qui permet de garantir la continuité du service. La pertinence de la sauvegarde décroît au fil du temps.

L'archivage : l'objectif est de constituer un ensemble cohérent d'informations représentatif d'une période donnée. Le stockage est fait après validation « utilisateurs » de cette période et dans des conditions techniques qui garantissent une longue conservation. L'archive est atemporelle, son

[1] Des laboratoires spécialisés proposent de récupérer des disques endommagés.

[2] A l'origine un premier brevet d'IBM en 1978 puis des travaux de l'université de Californie à Berkeley en 1988.

utilité est indépendante de son antériorité. Elle doit être faite avec des outils et des supports facilement réutilisables dans le futur et donc le plus standard possible.

6.3 Périmètre de la sauvegarde

A priori, l'ensemble des données et programmes du système central doit être globalement sauvegardé, en optant pour une solution totale : la sauvegarde est la copie pure et simple de l'état du système à un instant **t**. Au cas où les volumes concernés excédent la capacité des supports de sauvegarde, on découpe les sauvegardes en unités logiques, mais il vaut mieux alors faire appel à des professionnels pour l'organisation de ces procédures. Enfin, si des données importantes sont stockées sur des stations du réseau, on exécutera des sauvegardes à distance de ces dernières.

6.4 Méthode de sauvegarde

La méthode la plus simple sera la plus efficace : un support = une sauvegarde totale du serveur. Les méthodes peuvent devenir plus complexes si la configuration y oblige : sauvegardes incrémentales, différentielles, etc. peuvent s'avérer utiles voire nécessaires; mais là encore on s'adjoindra impérativement les services de spécialistes.

Il est par contre important de se demander si la méthode utilisée permet une mise en œuvre facile de la restauration, même si celle-ci doit se faire sur un serveur, une version d'OS et des unités de disques légèrement différents de ceux d'origine.

6.5 Les logiciels de sauvegarde

Certains logiciels créent des sauvegardes dans un format de donnée propriétaire. Autrement dit, seul ce logiciel peut réutiliser la sauvegarde pour en faire une restauration. C'est un paramètre important surtout lorsque le logiciel est utilisé pour faire une archive généralement de longue durée. Il faut alors s'assurer que le logiciel en question sera toujours disponible et maintenu lorsque l'on aura besoin de restaurer l'archive dans 3 ou 4 ans, que l'on aura changé de serveur et de version de système d'exploitation.[1] Au jour d'aujourd'hui en TPE, le plus efficace peur être un disque dur externe connecté en USB pour une image complète des données.

6.6 Rotation des supports

Ancienne bande des années 1980	Les cartouches d'aujourd'hui et leur lecteur	Une cartouche = bande magnétique
		

Une organisation simple et classique consiste à faire correspondre les supports de sauvegarde avec les jours de la semaine : il y a la « bande du lundi », la « bande du mardi », etc. Cette rotation implique une durée de vie des jeux de sauvegarde d'une semaine ouvrée : une semaine et un jour

[1] En cas extrême, des laboratoires sont capables de restaurer les données sur un support.

après la sauvegarde, il n'y a plus aucun moyen de restaurer la situation antérieure d'une semaine. La constatation d'un incident étant parfois tardive, l'enjeu des sauvegardes est aussi de permettre de remonter dans le temps pour un fichier détérioré depuis plusieurs jours et donc sauvegardé en l'état plusieurs fois. Toutefois, le rythme de vie du fichier concerné peut être mensuel (paie) ou hebdomadaire. Dès lors, la sauvegarde quotidienne ne permet pas la restauration car les dernières versions sauvegardées contiennent la version de fichier dégradée. Ceci explique, la nécessité de disposer de cycles de sauvegarde cohérents avec celui d'utilisation des données.

Cette rotation minimale peut avantageusement être remplacée par des procédures plus sécurisées : rotations sur un mois, multiplicité et redondance des sauvegardes, copies de disque à disque, adjonction aux sauvegardes totales de sauvegardes différentielles, etc.

6.7 Stockage des supports

On voit trop souvent des bandes de sauvegarde « traîner » au voisinage des serveurs : qu'un incendie survienne et le support de secours brûle en même temps que le système tout entier. Immédiatement après toute utilisation, les supports récemment utilisés doivent être rangés dans des coffres ignifugés ou tout simplement dans un local suffisamment éloigné. Ils doivent être correctement étiquetés et datés.

Une organisation fréquemment rencontrée consiste à ce que le responsable des sauvegardes emporte à son domicile la copie la plus récente. C'est simple et très efficace dans une structure petite et moyenne.

6.8 Surveillance des opérations de sauvegarde

L'utilité d'une sauvegarde repose sur sa capacité à restituer des informations perdues ou altérées. Pour cela, il est particulièrement important de s'assurer de la bonne fin des opérations de sauvegarde. Autrement dit, chaque support de sauvegarde présente une valeur dès l'instant que l'on s'assure qu'il peut être relu et qu'il contient réellement l'information attendue. Il faut savoir que tout support magnétique peut être l'objet de défaillance.

Une sauvegarde sans test de relecture donne l'apparence de la sécurité, mais relève de l'inconséquence.

Une personne responsable doit être nommée pour veiller à ce que la sauvegarde a bien eu lieu et qu'elle s'est correctement déroulée. Le plus souvent, les sauvegardes ont lieu la nuit, quand la production informatique est la moins active. La plupart des logiciels de sauvegarde sont en mesure d'imprimer automatiquement un « fichier log » des opérations réalisées et de leur qualité; on ajoutera utilement à cette impression l'émission d'un message électronique aux personnes intéressées.

En résumé, il ressort clairement qu'une personne doit être nommément désignée pour surveiller au jour le jour ces procédures ; cette personne doit avoir un remplaçant désigné à l'avance pour les périodes d'absence. Le niveau technique du responsable peut, dans bien des cas, être relativement faible; d'une rigueur irréprochable, cette personne s'assurera des points suivants :

- les bons supports sont bien en place au moment choisi,
- la sauvegarde programmée a bien eu lieu et s'est bien déroulée,
- les supports sont bien rangés et étiquetés dans les lieux prévus à cet effet,
- les documents attestant du bon déroulement sont bien archivés.

6.9 Comment utiliser le support de RGI joint

6.9.1 Identification du périmètre de la sauvegarde

Généralement les cycles de sauvegarde sont quotidiens, hebdomadaires (plus rarement) et mensuels. Pour chaque cycle de sauvegarde (C1, …..C4), il est important de déterminer ce qui est sauvegardé :

Connaissez-vous le périmètre des fichiers sauvegardés et notamment	C1	C2	C3	C4
Les programmes des applications				
Les données permanentes des applications				
Les documents des utilisateurs				
Le système d'exploitation du serveur				

- Qui paramètre et contrôle ce périmètre de sauvegarde ?
- Comment s'assure-t-on que le périmètre est à jour compte tenu des installations / suppressions de logiciel sur le serveur ?

6.9.2 Résumer la situation par le tableau ci-après

Fréquence de sauvegarde	Cycle.	Nature : copie,	Nbre de jeux	Stockage : (lieu, accès, conditions, …)
Quotidienne	C1			
Hebdomadaire	C2			
Mensuelle	C3			
Annuelle	C4			

6.9.3 Déclenchement des sauvegardes

Les opérations de sauvegarde sont-elles déclenchées :

- automatiquement par un logiciel,
- manuellement par un utilisateur.

Si déclenchement manuel, comment contrôler la permanence des opérations ?

6.9.4 Identification des supports de sauvegarde

Quelle technique permet de différencier la sauvegarde du lundi de celle du mardi, celle de janvier de celle de juin ?

- un label informatique mémorisé sur la bande et contrôlé par le logiciel de sauvegarde,

- un étiquetage que l'utilisateur doit respecter.

Ce point est déterminant pour la qualité des opérations et l'identification du support à restaurer en cas de besoin.

6.9.5 Méthode de contrôle de la sauvegarde

Pour chaque fréquence de sauvegarde, décrire la méthode de contrôle permettant de s'assurer de la qualité de la sauvegarde.

Ce contrôle de qualité peut être réalisé par les approches suivantes :

- relecture et comparaison exhaustive du support de sauvegarde avec les fichiers sauvegardés (méthode recommandée car facile à mettre en place),
- même processus par sondage sur certains fichiers,
- vérification de l'index de la bande.

6.9.6 Stockage des supports de sauvegarde

- les supports anciens sont archivés dans un coffre ignifuge d'une salle sécurisée située dans un bâtiment dont l'accès est contrôlé. La sauvegarde la plus récente est stockée dans un bâtiment autre que celui abritant la salle informatique,
- les supports sont tous dans une armoire classique,
- les supports sont à proximité du serveur pour faciliter les manipulations.

6.9.7 Procédure de fin d'exercice

En PME, la sauvegarde de fin d'année est faite à des fins d'archivage fiscal. Nous avons expliqué les différences importantes entre sauvegarde et archive et il faut vérifier dans un tel cas de figure si les contraintes liées à l'archivage fiscal sont respectées :

1. le périmètre englobe :
    a. les données de gestion et la comptabilité,
    b. si les données ont été purgées ou agrégées, des sauvegardes préalables ont été réalisées,
    c. une image figée des programmes et paramètres des applications.
2. le moment de la sauvegarde : elle est réalisée après tous les travaux de contrôle de fin d'année si bien qu'elle présente l'ensemble des données validées de l'exercice.
3. la technique présente des garanties suffisantes de conservation (support) et de réutilisation (sauvegarde logique et test de relecture).

7 CONTRAINTES LEGALES

Le droit de l'informatique est un domaine nouveau qu'il convient d'aborder sous un éclairage propre à notre mission de commissaire aux comptes.

7.1 Loi informatique et liberté du 6/1/78

Objectifs de travail :

La loi 78-17 du 6/1/78 relative aux traitements automatisés de données nominatives concernant des personnes physiques impose à toute personne de déclarer ces fichiers à la Commission Nationale Informatique et Liberté (C.N.I.L).

Sont considérés comme nominatifs les fichiers identifiant les personnes :

- - soit directement par leur nom,
- - soit indirectement par un code ou numéro de matricule individuel.

Toutefois, bon nombre d'applications standards peuvent bénéficier d'une déclaration simplifiée dès lors qu'elles remplissent certaines conditions. Les autres traitements doivent faire l'objet d'une déclaration ordinaire.

Les principaux délits retenus par ce texte concernent :

- - la création de fichiers non déclarés,
- - enregistrement ou conservation illicite d'informations nominatives,
- - détournement de finalité d'information nominative,
- - divulgation illicite d'information nominative,
- - collecte d'information nominative sans avoir informé les personnes interrogées,
- - entrave à l'action de contrôle de la CNIL,
- - entrave au droit d'accès ou de rectification des intéressés.

Moyens :

Entretien avec le responsable informatique ou le responsable des études. Il est nécessaire de procéder à un recensement exhaustif de tous les fichiers concernés.

7.2 Appréciation du niveau de documentation

La documentation du système d'information de gestion est rendue obligatoire en raison du PCG et de la règlementation relative au contrôle fiscal des comptabilités informatisées.

Objectifs de travail :

La documentation des applications est une contrainte légale imposée par plusieurs textes.

Plan comptable général :

- 410-2. - Une documentation décrivant les procédures et l'organisation comptables est établie en vue de permettre la compréhension et le contrôle du système de traitement ; cette documentation est conservée aussi longtemps qu'est exigée la présentation des documents comptables auxquels elle se rapporte. ».
- 410-4. - L'organisation de la comptabilité tenue au moyen de systèmes informatisés implique l'accès à la documentation relative aux analyses, à la programmation et à l'exécution des traitements, en vue, notamment, de procéder aux tests nécessaires à la vérification des conditions d'enregistrement et de conservation des écritures. »

Obligations de sources fiscales

> Elles découlent de l'article L 13 du Livre de Procédures Fiscales (modifié par la loi de finance 1990 art L102B du Livre de Procédures Fiscales) qui prévoit la possibilité d'un contrôle de l'administration portant sur les "*informations, données et traitements informatiques qui concourent, directement ou indirectement, à la formation des résultats comptables ou fiscaux ... ainsi que sur la documentation relative aux analyses à la programmation et à l'exécution des traitements.*".

Ces mesures ont été complétées de sanctions fiscales lourdes (art L74 du Livre de Procédures Fiscales), notamment l'évaluation d'office pour opposition à contrôle, lorsque l'entreprise ne peut fournir à l'administration les fichiers ou documentation d'analyse-programmation.

Il convient donc de faire une revue limitée de quelques dossiers d'analyse (y trouve-t-on le minimum nécessaire ?) et de dresser un état de la documentation des applications.

A noter que des obligations sectorielles peuvent aussi s'appliquer comme dans les banques et établissements financiers avec le CRB 97-02.

Moyens :

- entretien avec le responsable des études, le DSI ou le DAF (selon contexte et sujet)
- revue de dossier,
- observation.

7.3 Appréciation du niveau de sauvegarde

En dehors des obligations sectorielles, c'est principalement le contrôle fiscal des comptabilités informatisées qui impose des mesures de conservation visant :

- La documentation des projets et celle d'exploitation des traitements
- Les données de gestion détaillées
- Les lots d'écritures comptables importées en comptabilité
- Les exportations d'écritures au format FEC rendues obligatoires par l'art LPF 47 A-1dans sa rédaction du 29/12/12)
- Les programmes exécutables et leurs versions successives (ainsi que les chaines de lancement)
- Idem pour les programmes sources s'ils sont disponibles

Le périmètre de conservation concerne l'ensemble des applications ayant un impact comptable ou fiscal sur une période de 3 exercices échus :

Lorsque la comptabilité est tenue au moyen de systèmes informatisés, le contrôle porte sur l'ensemble des informations, données et traitements informatiques qui concourent directement ou indirectement à la formation des résultats comptables ou fiscaux et à l'élaboration des déclarations rendues obligatoires par le code général des impôts ainsi que sur la documentation relative aux analyses, à la programmation et à l'exécution des traitements. (LPF L13 al IV)

Objectif de travail :

S'assurer de l'existence de sauvegarde des informations et documentations concernées.

Moyens :

- entretien avec le responsable informatique

7.4 Loi 85-660 du 3/07/85 relative à la protection des logiciels et progiciels

Cette loi protège la propriété intellectuelle des concepteurs de logiciels contre la copie ou l'utilisation non autorisée.

Objectif de travail :

L'entreprise a-t-elle pris des mesures préventives de sensibilisation du personnel et de contrôle des PC pour éviter la transmission et l'utilisation de copies pirates ?

Moyens :

- entretien avec le responsable informatique, éventuellement l'audit interne.