Passage à l'an 2000

Le jour J

SEPTEMBRE 1999

LE CIGREF

Le Cigref, Club informatique des grandes entreprises françaises, existe depuis 1970. Sa finalité est la promotion de l'usage des systèmes d'information comme facteur de création de valeurs pour l'entreprise. Il constitue un lieu privilégié de rencontre et d'échange d'informations entre les responsables des grandes entreprises françaises ou européennes utilisatrices d'importants systèmes d'information. Ce partage d'expériences vise à faire émerger les meilleures pratiques. Chaque année, le Cigref réalise des études sur des sujets d'intérêt commun.

Rapports publiés par le Cigref en 1999 :

Benchmarking informatique

Commerce électronique (en anglais et en français)

Contrat d'interchange EDI (en anglais et en français)

Coût de possession du poste de travail
Rapport d'étape

Maîtrise d'internet

Marketing de l'informatique auprès des décideurs

Nomenclature 2000
Les emplois-métiers du système d'information dans les grandes entreprises utilisatrices

Observatoire des télécoms

Retours d'expérience ERP

Ces rapports peuvent être obtenus en se connectant sur le site web du Cigref : www.cigref.fr

PARTICIPANTS DU COMITÉ DE PILOTAGE AN 2000

Elie Abiakle	Groupama
Corinne Akrour	Electrolux France
Pierre Argouarc'h	MMA
Joël Autié	Total
Jacques Auzat	CGU France
Albert Azuelos	La Poste
Alain Baillot	ANPE
Christophe Barbot	Accor
Jean-Michel Bardin	BNP
Jean-Claude Beauclair	MMA
Guy Bellot Champignon	Carrefour
Étienne Benevent	ANPE
Patrick Bielsa	CCF
Jacques Bisiaux	Crédit Foncier de France
Edith Bombarde	Manpower
Bernard Bonnet	Accor
Gérard Borel	France Télécom
Marc Bouhiron	France Télécom
Alain Boulet	Axa
Lounès Boumail	Michelin
Thierry Boyer	Hennessy
Marc Branchard	Snecma
Jean-Jacques Brehe	Bouygues
Patrick Brunel	Danone
Gérard Cardona	CNES
Hervé Cerede	MMA
Christian Chatelin	GAN
Jacques Chatelon	Bolloré
Jean-Claude Chausset	Cogema
Guy Chemoul	PSA
Patrice Chevy	BP France
Martine Chicault	Radio-France
Mimoun Chikhi	Rhône-Poulenc
Henri Claquin	Framatome
Jérôme Consigny	Axa
Philippe Coubard	CCBP
Éliane Coutable	RATP
Alain Daugé	Agirc
Pierre de Mengin Fondragon	Technip
Claude Delmas	Société Générale
Alain Delpech	Macif
Jean Desbizet	BNP
Jacques Desbrugeres	Electrolux France
Jacques Deydier	Hospices Civils de Lyon
Jean-Pierre Dorgans	Giat Industries
Bertrand du Boullay	AGF
Corinne Dupart	CGU France
Daniel Dupuis	CIC Paris
Véronique El Mernissi	Groupama
Bernard Ferrier	Elf Aquitaine
Christian Fourot	Michelin
Gérard Gaichet	Carrefour
Marie-Dominique Gendet	BNP
Michel Geneix	SMABTP
Nathalie Gouache	Technip
Sylvie Grandiere	Framatome
Véronique Grimonpont	Crédit Foncier de France
Michel Guenard	Danone
Laetitia Guicciardi	Cogema
Jean-Luc Guyot	CNCA
Frédéric Hallermeyer	La Poste
Martine Hanin	Elf Antar France
Jean-Jacques Henry	SNCF
Isabelle Herbert	Air France
Nicole Houzelot	CCF
Thierry Huchet	MMA
Jacques Hur	Renault
Yvette Julhes	Crédit Lyonnais
Yves Kuna	CNCA
Jean-Luc Lacoste	CIC Paris
Jean Laviolette	RATP
Christian Le Bars	Crédit Lyonnais
Alain Le Borgne	Société Générale
Guillaume Le Mee	MACIF
Vincent Le Saout	EDF-Gaz de France
Patrick Leroux	Aérospatiale
Marie-France Leroy	Cnam-TS
Gérard Lullier	Crédit Lyonnais
Michel Macaire	Elf Aquitaine
Olivier Marcon	BNP
Pierre Maroccelo	Seita
Christian Masson	Banque de France
Franck Mathis	France Télécom
Dominique Maumy	Informatique CDC
René Millette	Paribas
Christian Mingueneau	Mairie de Paris
Alain Monroche	Rhône-Poulenc
Eric Morlot	EDF-Gaz de France
Louis Moulin	Aérospatiale
Jacky Mousset	Danone
Danh Nguyen-Ngoc	Technip
Michel Pagès	EDF-Gaz de France
Michel Paumero	Hennessy
Jean-Luc Perichon	Parfums Christian Dior
Gia Bien Pham	Technip
Pierre Piétri	SMABTP

Jean-Jacques Pochet	Manpower
Joël Politanski	Générale des eaux
Hervé Pont	Azur GMF
Pierre Préneron	Cencep
Antoine Puerto	
Christine Quentin	Accor
Dominique Rachou	Manpower
Christine Raulin	France Télécom
Valérie Raymond	CCF
Rachel Rebois	Pechiney
Jean-Marc Reniè	La Redoute
Hélène Rentier	Société Générale
Didier Risch	CIC Paris
Jean-Christophe Robert	Amadeus Développement
Marc Rocher	Mairie de Paris
Jean-François Roux	Alstom
Serge Saghroune	Accor
Jean-Louis Sauvetre	Snecma
Pierre Savarit	Usinor
André Schwob	La Poste
Richard Stierlam	Cnam-TS
Michel Stievenart	SNCF
Jean-Alain Taupy	Elf Antar France
Maurice Thaï	Air Liquide
Philippe Tillet	Technip
Jean-Pierre Tomasi	Thomson-CSF
Jean-Maurice Tupin	CEA
Jean-Pierre Vassal	CCMSA
Jean-Paul Vincent	EDF-Gaz de France
Dominique Vuillemin	Groupama
Philippe Zanini	Mairie de Paris

L'étude a été rédigée par Jacques Fradin et Pierre-Yves Le Bihan (Cigref).

Comité de relecture :
Michel Macaire (Elf), Dominique Maumy (Informatique CDC), Hervé Pont (Azur GMF), Marc Branchard (Snecma), Joël Politanski (Générale des Eaux), Michel Pagès (EDF).

SOMMAIRE

PRÉAMBULE

Voici la nouvelle livraison du Cigref à propos du passage à l'an 2000. Dans nos rapports précédents sur ce sujet : « Opération An 2000 » 1re et 2e parties, nous avions décrit l'ensemble de la problématique depuis les études d'impact jusqu'aux aspects juridiques de partage de responsabilités.

Il s'agit maintenant d'évoquer les derniers préparatifs, les dernières précautions, les mesures de sauvegarde.

Les entreprises doivent privilégier le passage opérationnel à l'an 2000.

Nous recommandons à nos membres et à l'ensemble de la communauté des entreprises de privilégier clairement le passage opérationnel à l'an 2000 en ayant à l'esprit les trois priorités : d'abord la sécurité des personnes, puis celle des biens et enfin celle de la continuité du service à la clientèle.

Bien entendu, l'examen critique doit porter sur l'entreprise elle-même mais aussi sur son environnement (sous-traitants, fournisseurs, etc.). Le risque est « systémique ».

Cette priorité veut dire que le partage complexe des responsabilités ne devra être traité qu'après le passage, s'il y a lieu. Mais une élémentaire prudence veut que chacun conserve soigneusement les traces de l'historique du passage et soit en état de démontrer qu'il a fait ses meilleurs efforts face à un événement qui n'est ni imprévisible ni irrésistible, à condition que chacun fasse son devoir tant du côté utilisateur que du côté fournisseur.

Nous ne reviendrons donc pas sur les positions juridiques du Cigref. Celles-ci sont très connues même si, évidemment, elles ne sont pas partagées par les fournisseurs.

D'ici la fin de 1999, nous nous attacherons à entretenir les échanges, à publier le résultat de nos tests, à contribuer à maintenir le pays sous tension et à mettre en place une structure particulière de communication pour la période hypercritique du passage.

Enfin nous souhaitons rappeler avec insistance l'importance d'une véritable trêve des modifications — de quelque sorte qu'elles soient — lors des derniers mois de 1999. Tant les utilisateurs que les Pouvoirs publics et surtout les fournisseurs doivent, désormais et pour trois mois, s'interdire toute modification qui ne serait pas strictement indispensable.

Pierre-Yves Le Bihan, délégué général du Cigref

INTRODUCTION

Les moyens disponibles devront être mis en œuvre pour prendre le relais en cas de défaillance.

Les tests d'intégration verticale et horizontale, dont la majeure partie s'est terminée en juin, continueront jusqu'au dernier moment. Quels que soient leurs résultats, il est nécessaire de se préoccuper de l'organisation qui permettra de passer du 31 décembre 1999 au 1er janvier 2000. Les moyens disponibles devront être mis en œuvre pour prendre le relais en cas de défaillance, principalement si l'activité de l'entreprise est mise en difficulté.

Rappelons-le une fois encore, le passage à l'an 2000 est inéluctable et doit se faire au mieux des intérêts de chaque entreprise. La marche en avant est indispensable, il n'y aura aucun moyen de revenir en arrière.

Maintenant, le seul objectif à tenir coûte que coûte est de passer en l'an 2000. Il est trop tard pour envisager des modifications importantes et des tests. Ce n'est pas le moment, non plus, de se lancer dans des opérations juridiques de grande envergure envers les fournisseurs dont la façon d'agir de certains est pour le moins discutable. Nous rappellerons plus loin les précautions à prendre en attendant des actions plus officielles après le passage.

La situation telle qu'elle doit se présenter pour ceux qui s'y sont pris suffisamment tôt est la suivante :

- les tests d'intégration se sont terminés fin juin ;
- juillet et août ont été consacrés aux dernières corrections ;
- à compter de septembre, préparation du passage et des plans de continuité.

L'objectif de la préparation est triple :

- réduire la probabilité d'incidents résiduels ;
- être en mesure de limiter l'impact d'incidents qui pourraient apparaître, qu'ils proviennent de l'entreprise ou de l'extérieur ;
- avoir les moyens de faire face à leur accumulation éventuelle.

Rappelons que les priorités sont :

- la sécurité des personnes ;
- la sécurité des biens ;
- la continuité de l'activité ;

1. PLANNING THÉORIQUE

La diversité des entreprises dans leurs organisations et leurs activités ne permet pas d'établir un plan de passage unique et détaillé. En revanche, le principe général reste le même pour toutes et s'organise autour de trois grands principes : se préparer, passer et maintenir l'activité.

La phase de préparation peut s'étaler sur plusieurs semaines ou se limiter à quelques jours en fonction principalement des travaux exceptionnels et des décalages d'exploitation qui seront indispensables pour éviter une surcharge de dernier moment.

Se préparer

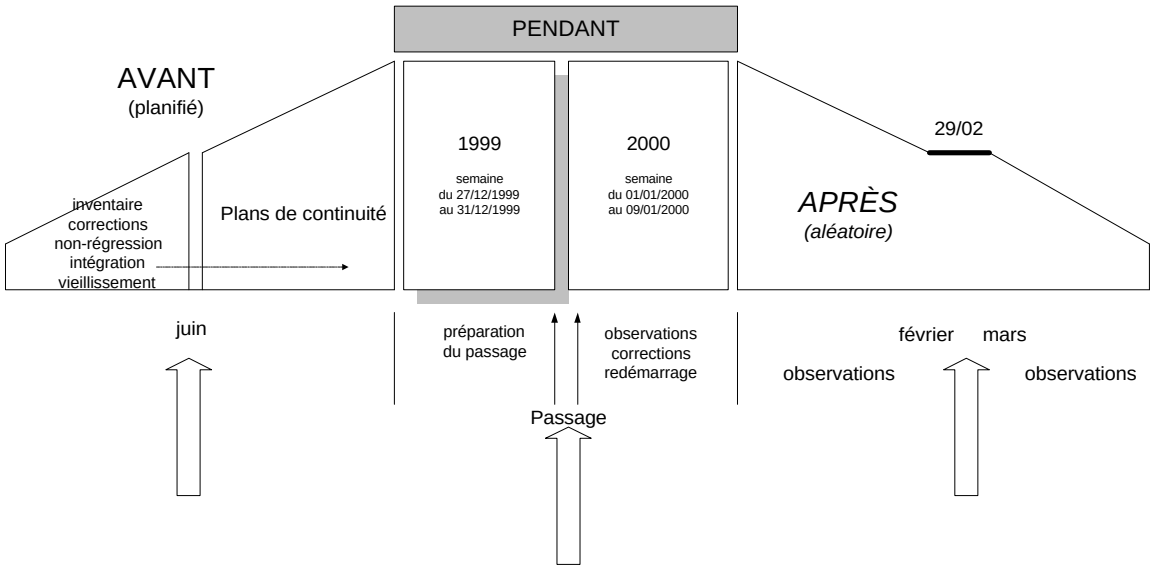
- septembre : arrêt des déploiements de mise à jour sur les grands parcs (plusieurs milliers de stations) ;
- novembre et décembre pas de livraison en production. Les systèmes et les applications sont stabilisés. Anticipation des traitements qui peuvent être décalés dans le temps ;
- les 30 et 31 décembre : arrêt des applications, sauvegarde des programmes et des données, tests des sauvegardes ;
- pour ceux dont la sécurité l'exige, démarrage des groupes électrogènes pour éviter toute surprise. Passage avec les groupes tournants ;
- le 31 au soir, libération de toutes les personnes non indispensables. Limitation des accès aux locaux aux seules personnes indispensables. Certaines entreprises prévoient d'interdire l'accès aux locaux entre 22 heures le 31 décembre et 10 heures le 1er janvier 2000 sauf aux équipes chargées de contrôler l'état technique des bâtiments et de l'environnement informatique.

Passer

- le 31 à minuit : observation de la situation ;
- le 1er janvier 2000 : après contrôle des infrastructures et de l'environnement, rechargement, démarrage progressif à froid des programmes et des applications, en présence de toutes les personnes nécessaires ;
- corrections éventuelles.

Maintenir l'activité

- Le 2 janvier : tests avec les utilisateurs pilotes ;
- Le 3 janvier : reprise d'activité, lentement, en gardant la possibilité d'arrêt partiel ou total si nécessaire ;
- Pendant tout le mois de janvier : exploitation sous contrôle renforcé.



Plan de passage théorique pour les entreprises.

Le planning doit tenir compte des impératifs métiers. Il est probable que des entreprises soient dans l'obligation de maintenir leur exploitation opérationnelle jusqu'au dernier moment, ce qui posera le problème du délai nécessaire aux sauvegardes.

2. *FAIRE DES CHOIX*

Les évolutions des logiciels et progiciels pourront théoriquement être envisagées jusqu'au dernier moment. Les éditeurs en ont les moyens, mais les utilisateurs ne seront pas en mesure de les déployer en quelques jours, voire quelques heures. Il faut se rappeler que toute modification faite en urgence, non testée correctement et remise en exploitation est souvent génératrice d'incidents dont les conséquences peuvent être plus graves que le mal d'origine.

Il faudra que les éditeurs justifient les modifications de dernière minute.

La seule solution sera de pouvoir disposer d'un maximum d'informations de la part des éditeurs pour juger de l'importance des dernières adaptations par rapport aux besoins de l'entreprise et prendre un minimum de risque en refusant d'intégrer les dernières modifications ou les dernières versions.

Il ne devra pas y avoir d'hésitation pour « harceler » les éditeurs, par tous les moyens, afin d'obtenir les raisons précises de leurs modifications et surtout les conséquences éventuelles de leur non-intégration.

En cas d'impossibilité de déploiement (trop de stations, applications trop complexes, problèmes d'interconnexion et, d'une façon générale, de manque de temps), l'entreprise, *via* le DSI assisté du service juridique, devra le faire savoir à l'éditeur par lettre recommandée avec accusé de réception.

La connaissance des procédures particulières d'assistance mises en place par chaque fournisseur sera indispensable. Le Cigref a transmis à certains éditeurs et constructeurs une liste de questions pour déterminer le niveau d'assistance auquel doivent s'attendre les clients (cf. annexe1).

La difficulté de mettre en œuvre des correctifs et de les déployer sera difficile voire impossible.

À titre indicatif, un rapport d'Infoliant (www.infoliant.com) au mois de juillet annonçait que plus de 2 300 statuts de conformité an 2000 auraient changé depuis janvier 1999 et que 20 % des statuts auraient changé en juin 1999… Plus la date fatidique approchera, plus les utilisateurs découvriront des incidents et plus l'effort des éditeurs et constructeurs sera grand pour rendre leurs produits conformes. La mise en œuvre des correctifs et de leur déploiement sera alors difficile voire impossible.

Ne pas oublier que toute nouvelle modification risque d'obliger à relancer une chaîne de tests (non-régression, intégration, vieillissement) et surtout de remettre en cause l'état de préparation annoncé en juin. Certaines entreprises ont déclaré un moratoire, ce qui signifie que toute modification entraînera la reprise de tests, donc doit être évitée autant que possible.

C'est là que non seulement les directeurs des systèmes d'information (DSI) devront apporter tout leur concours technique mais aussi les directions comme : DRH, commerciales, marketing, achats... pour la partie estimation du risque dans le cadre de la continuité de l'activité.

3. LES TROIS PHASES DE LA PÉRIODE CRITIQUE

- stabiliser les systèmes et applications ;
- préparer le passage ;
- organiser la continuité de l'activité de l'entreprise.

3.1 Stabiliser les systèmes et applications

Le Cigref a demandé une trêve des modifications.

Depuis plusieurs mois, le Cigref a demandé officiellement qu'une trêve des modifications soit observée, aussi bien au niveau interne des entreprises que chez les éditeurs et fournisseurs ou sur les aspects réglementaires (administrations). L'état de préparation d'une entreprise ne peut être pris en considération qu'à partir de logiciels stables et d'une exploitation industrialisée.

Plusieurs semaines avant le 31 décembre, les services de production devront faire « barrage » à toute livraison de nouvelles applications ou de modifications. Chez certains grands groupes, les niveaux les plus hauts de la hiérarchie s'impliquent totalement dans cette décision en exigeant d'une part d'être informés et d'autre part de signer toute nouvelle demande de mise en production.

Cela étant, une attention toute particulière devra être portée sur les évolutions des éditeurs : Microsoft, Oracle, SAP... qui considèrent trop souvent avoir fait leur devoir d'information *via* leur serveur internet. Une veille sera utile pour détecter toute nouvelle information et surtout celles qui sont contradictoires par rapport aux annonces précédentes et qui remettront en cause le travail fait et testé.

Pour faciliter la « découverte » des dernières modifications ainsi que les explications détaillées qui doivent leur être associées, le Cigref a demandé aux principaux éditeurs d'envisager la mise en évidence de ces modifications, en tête de leur service sur internet.

Certains éditeurs comptent faire évoluer leurs sites en ce sens pour la fin octobre, laissant ainsi un maximum de deux mois aux informaticiens et aux utilisateurs pour vérifier la stabilité de leurs systèmes et de leurs applications...

De là à penser que l'industrie du logiciel est immature, il n'y a pas loin. Mais peut-être les éditeurs auraient-ils pu corriger leurs produits dès 1995 quand tous les professionnels connaissaient l'impact de l'an 2000.

3.2 Avant : préparer le passage

Cette phase est celle qui précède le 31 décembre 1999, minuit.

Selon l'entreprise, elle peut se limiter à une seule journée, le 31 décembre, ou s'étendre sur plusieurs jours.

Ne pas oublier que cette période est de toute façon généralement encombrée puisqu'elle est, sur le plan comptable, à la fois une fin de mois, la fin d'année, la fin d'exercice, la mise en œuvre des *reportings*, les clôtures d'exercices… et que s'ajouteront deux projets : le passage à l'an 2000 et le régime des 35 heures.

Plusieurs stratégies : celle de ceux qui sont obligés de travailler en continu et celle de ceux qui peuvent temporairement stopper ou très fortement ralentir l'activité de l'entreprise.

Quelques précautions de base s'imposent quelle que soit la stratégie choisie :

Il faut diversifier les formats et les supports de sauvegarde.

- Il sera prudent de sauvegarder et dupliquer les fichiers importants pour l'activité de l'entreprise sous des formats simples (fichiers plats) et des supports utilisables par d'autres systèmes. Par exemple, un fichier clients pourra, si possible, être exporté en Ascii vers un CD-Rom en vue d'une réutilisation par un PC. Idem pour un fichier de livraisons ou de commandes.
- En fonction des plans standards, il sera prudent d'augmenter les fréquences des mises à jour et des sauvegardes.
- Les *reportings* et les traitements exceptionnels auront été décalés (si possible) pour éviter d'encombrer les derniers jours de 1999 et les premiers de 2000.
- Les consommables devront être surstockés en cas de ralentissement des chaînes d'approvisionnement. Pour éviter les ruptures de stocks chez les fournisseurs, il faut largement anticiper les commandes.
- Des impressions seront faites des fichiers de paramétrage des systèmes et des différents éléments indispensables aux services commerciaux, de paie, de comptabilité, de finance… Toute documentation indispensable et stockée sur disque sera imprimée ou dupliquée sur des supports permettant de diversifier les moyens de lecture.
- Les utilisateurs de stations portables, et d'une façon générale tous les utilisateurs qui ne sont pas sous contrôle de la DSI, doivent être prévenus des possibilités de dysfonctionnement à compter du 01/01/2000 et des moyens de se renseigner pour être aidés.

- Les partenaires qui assurent les activités sous-traitées seront sous veille permanente comme s'ils faisaient partie intégrante de l'entreprise.

Vérifier la validité des contrats au-delà du 31 décembre.

- Les services achats et juridique auront vérifié la validité des contrats au-delà du 31 décembre 1999.
- Ne pas sous estimer les besoins de coordination avec les services clients pour déterminer les priorités métiers et la communication vers les utilisateurs : date et heure de la dernière sauvegarde, heure d'arrêt des systèmes, heures de reprise, conditions de reprise, etc.
- Plusieurs jours à l'avance, par tous les moyens de communication possibles (messagerie, notes, journaux internes, affichage…) il sera précisé la date et l'heure d'arrêt de soumission à distance des travaux *batch* qui pourraient rester en fil d'attente ou être en cours d'exécution au moment du passage (pour ceux qui travaillent en continu) ou du lancement des procédures de sauvegarde et de mise en veille.

3.2.1 Pour ceux qui travaillent en continu

Cette préparation va consister à faire comme toujours un inventaire exhaustif de tous les éléments stratégiques et à mettre en face des moyens de contrôle et de contournement.

Les moyens de contrôle sont principalement basés sur les individus les plus spécialisés dans le domaine considéré et qui devront être présents.

Dans d'autres cas, le contrôle automatique est assuré par le doublement des matériels sous réserve qu'ils ne soient pas identiques : autres constructeurs, autres composants, programmes différents…

À toute fin utile, il sera défini des procédures d'arrêt d'urgence sous contrôle en tenant compte des incidences sur la globalité des processus.

Les moyens de contournement sont basés sur des procédures d'échange ou manuelles.

Les moyens de contournement sont basés sur des procédures d'échange ou manuelles. Un automate qui passe mal de 1999 à 2000 et qui est situé dans une chaîne de fabrication ne peut être rapidement remplacé que par un matériel de secours déjà prêt (paramétré) et stocké à proximité ou par une intervention manuelle ou par translation de *n* années en arrière.

3.2.2 Pour ceux qui ne travaillent pas en continu

La solution unanime : sauvegarder et mettre en veille ou arrêter (logiquement) tout ce qui peut l'être.

Le gain de temps n'est pas un facteur prioritaire par rapport à la sécurité.

La sauvegarde est en général prévue pendant la journée du 31 décembre. Toutefois, il n'est pas certain que tous les systèmes informatiques, surtout les très puissants, puissent être sauvegardés en une journée. La sauvegarde des système centraux seuls est estimée en moyenne à 6 ou 7 heures si aucun incident ne se produit. Les systèmes périphériques, dans certains cas, peuvent être sauvegardés en parallèle. Toutefois le gain de temps n'est pas un facteur prioritaire par rapport à la sécurité. Il est de plus en plus évident qu'il faudra souvent deux jours, c'est-à-dire que la production s'arrêtera le 29 décembre au soir pour laisser deux nuits et deux jours, du 29 au 30, le 30, du 30 au 31 et le 31 pour assurer :

- le passage des derniers traitements par lots (*batches*) ;
- l'arrêt des applications ;
- la sauvegarde des données ;
- la sauvegarde des programmes ;
- les tests de rechargement pour vérifier l'état des sauvegardes.

Deux points importants que les membres du Cigref ont très largement fait ressortir lors de leurs réflexions sur le sujet :

Deux sauvegardes, l'une avant le 01/01/2000 et l'autre après.

la sauvegarde des programmes, qui est très souvent oubliée. Les données sont couramment sauvées mais rarement les programmes. Or pour l'an 2000 les programmes auront été modifiés. À titre de sécurité, il est préconisé de faire deux sauvegardes, l'une avant le 01/01/2000 et l'autre après pour pouvoir disposer d'une version 1999 et d'une 2000 avant redémarrage, ne serait-ce qu'à titre de comparaison ;

- la vérification de l'état des sauvegardes. La qualité des sauvegardes repose très souvent sur « l'espoir » qu'elles se sont bien déroulées, que les données sont bonnes et que les supports sont en bon état pour être relus. À cet espoir s'ajoute le fait que la périodicité permet de penser que si le jour J est inexploitable, le jour J - 1 sera correct. Le fait de changer de millénaire élimine cette hypothèse.

Éviter les sauvegardes incrémentales. Privilégier les sauvegardes intégrales auxquelles s'ajouteront des sauvegardes sélectives de sécurité.

Les sauvegardes doivent tenir compte :

- des scénarios de reprise élaborés dans les plans de continuité ;
- des périodes de conservation réglementaires.

Non seulement à titre de sécurité mais aussi au titre de la disponibilité en cas d'incident, le nombre de copies devra être supérieur à la normale, d'où nécessité d'une gestion rigoureuse des dates et heures de création, des versions, des lieux de stockage.

On veillera à la mise à jour de l'historique des sauvegardes de données existantes pour être en mesure de choisir le niveau de restauration, principalement dans le cas de pollution ou de corruption des données qui pourrait apparaître plusieurs mois après le passage.

Si la durée de stockage des sauvegardes est automatisée, il faut ajuster les périodes.

Attention à l'espace disque et au nombre de bandes ou cassettes nécessaires.

L'arrêt des applications ne doit générer aucun problème si les précautions d'usage sont prises pour garantir la désynchronisation lorsqu'elles sont interdépendantes. Une attention toute particulière sera donnée aux applications du type EDI qui reçoivent ou transmettent des données vers des tiers.

Ces techniques ne sont pas nouvelles et doivent faire partie des procédures standards de sauvegarde et de reprise en cas d'incident en dehors de tout projet An 2000. Si ce n'est pas le cas, c'est le moment de les établir.

Les systèmes d'exploitation ne seront pas arrêtés mais simplement mis en veille.

Les systèmes d'exploitation (OS) ne seront pas arrêtés mais simplement mis en veille pour éviter toute surprise au redémarrage. Le redémarrage d'un système complexe et parfois interconnecté avec d'autres systèmes tout aussi complexes ne peut se faire sans risque, compte tenu du manque de documentation à jour ou de spécifications de synchronisation ou tout simplement d'erreurs humaines dans les paramétrages.

Les machines : Du côté des matériels de production (et aussi des OS), il est particulièrement difficile d'obtenir des engagements des constructeurs voire de simples recommandations ou informations. Seules les habitudes ou l'expérience guident la façon d'agir.

Les ordinateurs qui sont protégés par groupe électrogène ne seront pas arrêtés pour éviter, tout comme pour les OS, les

incidents au redémarrage. Chacun sait qu'il est très peu probable qu'un redémarrage se fasse sans qu'un contrôleur ou une alimentation soit en panne. L'incident n'est pas grave en lui-même mais risque de le devenir si le constructeur, pour cause d'afflux de demandes, est en rupture de stock pour « un certain temps ».

Un point nécessite une étude de criticité particulière au sein de l'entreprise. Il se peut que plusieurs gros systèmes existent mais que certains seulement soient protégés par des groupes électrogènes. L'expérience, comme dit précédemment, conseille dans la mesure du possible de ne pas débrancher. Toutefois on ne peut pas éliminer totalement la possibilité d'une coupure d'électricité, aussi faible soit-elle. Les machines non protégées par groupe électrogène sont donc en danger. Seule l'étude de leur importance dans l'activité de l'entreprise permet de juger de la gravité d'un problème au démarrage. Cette situation n'est pas liée à l'An 2000. Le risque est donc connu. Seule reste l'incertitude plus ou moins forte sur la fiabilité du réseau EDF qui sera en situation inhabituelle à ce moment-là (voir aussi au chapitre 4.5).

On peut considérer aussi que le choix fait par l'entreprise de ne pas secourir certains de ses sites en temps normal font de ceux-ci des points non stratégiques pour lesquels des risques peuvent être pris.

Il faudra disposer d'un ***help desk*** particulièrement formé et dimensionné pour assurer l'aide aux utilisateurs.

Les stations de travail à base de PC, non intégrées dans des chaînes, qui n'assurent pas de contrôles en temps réel ou qui ne sont pas indispensables doivent être arrêtées. Simplement parce qu'il est inutile de générer des problèmes supplémentaires à ce moment-là. Leur état sera connu à la reprise de l'activité. Il faudra disposer d'un *help desk* particulièrement formé et dimensionné pour assurer l'aide aux utilisateurs.

Les matériels réseau et bureautique, serveurs, *hubs*, routeurs, *switches*, etc., principalement pour les entreprises qui ont des implantations internationales et donc ayant à gérer des décalages horaires, resteront de préférence en ordre de marche pour assurer les messageries en secours éventuel de la voix et le transfert de données pour les corrections.

Ces matériels n'étant pas toujours secourus — ou moins que les systèmes centraux — il est nécessaire de prendre un minimum de précautions :

- éviter que les sauvegardes automatiques des serveurs se déclenchent au moment du passage ou dans les minutes qui suivront ;

- éviter que des automates lancent des travaux en différé à minuit y compris en liaison sur des systèmes centraux (*batch*, extraction de données, mise à jour…) ;
- éviter que des mises à jour d'annuaires de messagerie entre plusieurs sites soient en cours ;
- interdire tous les travaux habituellement exécutés en différé comme les mises à jour de tables, les « nettoyages » de fichiers, les compressions… ;
- verrouiller tous les accès utilisateurs aux messageries juste avant le passage et ne les réactiver qu'après s'être assuré auprès des équipes techniques que ce moyen de communication n'est plus stratégique ;
- laisser active la messagerie qui risque d'être l'un des rares moyens de communication disponibles pour les équipes techniques (sauvegarder les annuaires) ;
- pendant la période, disposer de la copie des tables de routage ;
- avoir toutes les coordonnées des services de maintenance des points d'accès aux réseaux de transport nationaux et internationaux ;
- avoir regroupé sur un seul CD-Rom les logiciels indispensables et leurs corrections éventuelles ;
- avoir sur chaque site des documentations, des CD-Rom et des sauvegardes au même niveau ;
- disposer de matériel de secours : lecteur et graveur de CD-Rom, modems, robots de sauvegarde ;
- etc.

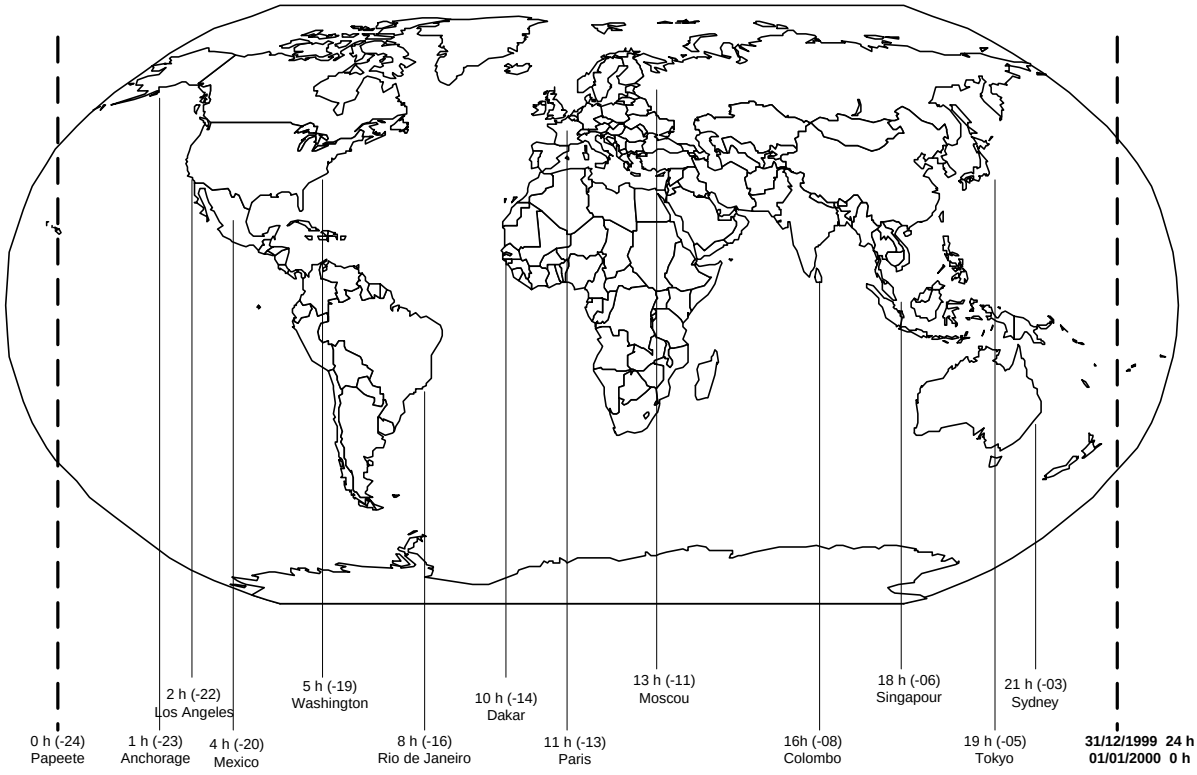
Les « ordonnanceurs » et d'une façon générale tous les systèmes en fonctionnement automatique devront être mis en veille au plus tard le 31 décembre à midi. Les travaux nécessaires entre le 31 décembre midi et la fin des tests de reprise seront lancés manuellement.

En résumé :

- réduire l'activité au strict minimum ;
- limiter le nombre d'utilisateurs ;
- sauvegarder les données, programmes et configurations ;
- rester vigilant.

Une fois ces dispositions prises, chacun pourra aller réveillonner et se préparer au lendemain.

3.3 Pendant : le passage et les observatoires



Passage à l'an 2000 en fonction des fuseaux horaires.

Dès le 31 décembre à midi, les sociétés qui disposent d'implantations internationales pourront commencer à suivre les conditions de passage et en déduire les conséquences éventuelles sur leurs systèmes en France.

Cette situation leur permettra aussi d'observer toute éventualité de pollution des données *via* l'interconnexion de leurs ordinateurs.

Dans le cas le plus simple par exemple un équipement situé à Paris et l'autre à Singapour, il faudra gérer correctement des informations déjà datées du 01/01/2000 (Singapour) qui viendront alimenter une application encore au 31/12/1999 (Paris).

Dans les cas les plus complexes, il faudra gérer une cascade de passages et de va-et-vient entre applications datées en 1999 et 2000.

Une attention toute particulière devra être portée sur les équipements dont l'heure système est fixée sur la base d'une moyenne des décalages horaires des filiales : non seulement il faudra gérer les passages successifs mais aussi celui de Paris qui ne sera pas standard.

Pour les réseaux il faudra veiller au mode de mise à jour de l'heure et de la date sous Windows NT qui peut être amené à se synchroniser automatiquement sur un serveur de temps (s'il existe sur le réseau).

Il conviendra de maintenir un contrôle permanent des systèmes restés opérationnels.

3.4 Après : observer, surveiller

Pour les équipements qui seront passés en mode continu on observera par rapport à la normale :

- leur disponibilité ;
- leurs performances.

Pour les autres :

- craindre les phénomènes d'accumulation d'incidents ;
- veiller très attentivement aux possibilités de pollution des données ;
- reprendre progressivement l'exploitation ;
- éviter de créer des situations inhabituelles.

3.4.1 Accumulation

Il y aura de 3 à 5 % (le Gartner Group annonce 5 à 9 % du code rénové et testé) de pannes résiduelles qui n'apparaîtront qu'après le passage quel que soit le degré de préparation. Leur gravité pourra être faible ou forte, peu importe ! seuls le nombre et la fréquence sont à craindre. La taille des équipes compétentes ne peut pas croître indéfiniment. Pour quelques jours ou quelques heures il y aura donc risque de surcharge importante.

Ce sera à la cellule de pilotage de déterminer la criticité des incidents et de donner les priorités en cas d'affluence.

3.4.2 Pollution des données

Une détection tardive peut demander plusieurs mois de travail.

La situation la plus « sournoise » sera la pollution de données. La pollution en elle-même n'est pas très gênante, sous réserve de la repérer rapidement. Une détection tardive peut demander plusieurs mois de travail pour remonter les chaînes polluées et apporter les corrections. Comment agir ?

- faire des contrôles par échantillonnage ;
- stocker temporairement sur disque avant d'introduire dans les chaînes de traitement ;
- vérifier les variations de flux ;
- développer des outils de tests ;
- etc.

3.4.3 La reprise progressive de l'exploitation

Après le passage, plusieurs recommandations :

1. observer le « comportement » des équipements : *mainframe,* serveurs, réseau, serveurs web, serveurs de fax, pare-feu, PC…

2. dans la mesure du possible, ne pas augmenter le trafic des télécommunications pour éviter d'aggraver la période de saturation prévisible de 0 h à 3 h le 01/01/2000. Dans cette fourchette horaire, il sera difficile de déterminer les causes de tentatives infructueuses de connexions : bogue ou saturation du réseau ?

3. ne pas réamorcer (*rebooter*) des machines ou des stations dans les premières minutes pour laisser le temps aux systèmes de mettre à jour les horloges ;

Tout incident n'est pas forcément dû à l'an 2000

4. analyser prudemment les incidents éventuels en gardant à l'esprit que tout incident n'est pas forcément dû à l'an 2000 ;

5. faire un état des lieux précis et le transmettre à la cellule de pilotage ;

6. ne pas considérer que tout est terminé après quelques heures de reprise ;

7. si tout semble normal, faire une sauvegarde complète.

Check-list

En tout premier lieu, contrôler l'environnement qui est stratégique dans le fonctionnement des ordinateurs et la sécurité des personnes :

- accès aux bâtiments ;
- éclairage de secours ;
- alarmes ;
- ascenseurs et monte charge ;
- GTB (gestion technique des bâtiments) ;
- GTC (gestion technique centralisée) ;
- état des groupes électrogènes ;
- alimentation électrique (connaître la puissance nécessaire) ;
- alimentation en eau ;
- climatisation, hygrométrie (connaître les plages de température) ;
- accès aux réseaux de télécommunications.

En priorité pour la messagerie et le transfert de fichiers, vérifier le réseau :

- état des serveurs ;
- modems ;
- routeurs ;
- contrôle des chemins ;
- ne pas faire de redémarrage à chaud dans les minutes qui suivront le passage ;
- vérifier par échantillonnage l'état des tables de routage.

Vérifier l'état des liaisons en établissant des connexions avec des utilisateurs tests situés dans les différentes zones géographiques représentatives de l'implantation de l'entreprise (Lan et Wan).

Pour le téléphone, contrôler l'autocommutateur (PABX) :

- liaisons internes : poste à poste ;
- liaison avec les opérateurs (liaisons locales, nationales, internationales) ;
- télémaintenance avec son modem et sa ligne ;
- système de taxation (fichiers de taxation, dates, heures) ;
- fax ;
- affichage sur les postes téléphoniques numériques et consoles de gestion ;
- faire des appels de tests vers certains utilisateurs répartis géographiquement et vers le *help desk,* ce qui présentera le

double intérêt de valider le PABX et l'assistance aux utilisateurs ;

- vérifier l'heure et la date dans l'enregistrement des messages ;
- tester l'acheminement des appels si le routage dépend de l'heure et de la date ;
- contrôler la validité des mots de passe sur les consoles des opérateurs ;
- contrôler la validité des dates dans le fichier historique des appels.

Attention à ce qui pourrait rester en file d'attente et se réactiver au redémarrage.

Pour les machines en veille, en suivant les procédures pas à pas, réactiver les systèmes d'exploitation et les applications et synchroniser les applications interconnectées. Attention à ce qui pourrait rester en file d'attente et se réactiver automatiquement au redémarrage.

Pour celles qui ont été électriquement arrêtées, on redémarrera progressivement et sous contrôle, en liaison étroite avec les services des moyens généraux qui assurent l'environnement : alimentation, climatisation…

Attention aux robots (bandes, cassettes) qui gèrent la durée de validité des supports magnétiques et aux ordonnanceurs qui gèrent le lancement automatique des applications. Ils devront rester « débrayés » jusqu'à ce que l'ensemble des processus ait été validé.

Vérifier l'évolution des dates dans les applications, surtout lorsque la technique du fenêtrage a été employée avec des dates pivots paramétrables. Deux applications peuvent travailler sur des dates pivots différentes, ce qui entraînera des conséquences non négligeables, principalement dans les tris.

Rappel du principe du fenêtrage : une valeur comprise ente 00 et 99 est choisie comme frontière (le pivot), toute valeur sur deux chiffres considérée comme une date et inférieure ou égale à cette frontière est considérée comme appartenant aux années 20xx et toute valeur supérieure est considérée comme appartenant aux années 19xx.

Par exemple si la date pivot choisie est 15 :

…	*09*	*10*	*11*	*12*	*13*	*14*	**15**	*16*	*17*	*18*	*19*	*20*	…
20xx								19xx					

Si deux applications utilisent des dates pivots différentes, la date d'origine xx/xx/12 devient soit xx/xx/2012 avec une date pivot à 15 ou xx/xx/1912 avec une date pivot à 10 :

Date pivots paramétrée	Date de départ Année sur 2 chiffres	Date interprétée comme
15	**xx/xx/12**	***2012***
	xx/xx/17	1917
10	xx/xx/08	2008
	xx/xx/12	***1912***
	xx/xx/17	1917

La date de 1912 est interprétée comme 2012 ou 1912 selon que la date pivot est 1915 ou 1910. Il est bien évident que le tri sur des dates de naissances par exemple peut donner des résultats surprenants… selon l'application et sa date pivot.

Mettre à jour les documents techniques et les plans de continuité en fonction des incidents et des corrections apportées. Informer tous les intervenants (internes et externes) des mises à jour et vérifier que tous restent bien en phase.

3.4.4 Gestion des situations inhabituelles

Il faut donner aux utilisateurs des instructions claires pour qu'ils ne créent pas involontairement des situations inhabituelles en se précipitant sur leur station, leur téléphone, leur fax et en essayant de tout tester dans les premières minutes de la reprise du travail, en principe le lundi 3 janvier 2000.

Les ***hot lines*** ne doivent être sollicitées que pour de réels incidents.

De même, il faut prendre les mesures adéquates pour éviter de saturer les moyens de communication de l'entreprise réseaux locaux, réseaux téléphoniques et moyens d'assistance : *(hot line* ou *help desk)*. Les moyens de communication peuvent être indispensables aux équipes techniques pour dépanner et les *hot line*, ne doivent être sollicitées que pour de réels incidents. Avant de faire appel à qui que ce soit, il faut éliminer les causes « naturelles » en testant localement tout ce qui pourrait être source de panne (cf. annexe 4). Éviter d'appeler pour une prise secteur débranchée…

Des numéros de téléphone supplémentaires, réservés aux équipes techniques et non diffusés aux utilisateurs peuvent éviter des situations de blocage.

La direction de la communication a, dans ce domaine, un rôle important à tenir.

4. ORGANISER LA CONTINUITÉ DE L'ACTIVITÉ

Il faut savoir s'arrêter. Les plans de continuité doivent prendre en considération toutes les possibilités d'incidents qui pourraient mettre en danger la bonne marche de l'entreprise mais il faut être conscient qu'au-delà d'une certaine dégradation de l'environnement, la seule solution sera d'attendre.

Il n'est pas raisonnable de prendre comme base de travail qu'il manquera pendant plusieurs jours d'eau, d'électricité et de télécommunications. Par conséquent il faut prendre comme principe que les incidents qui pourraient arriver sont les mêmes que d'habitude à la seule différence que leur nombre ou leur fréquence pourraient, dans le cas particulier du passage à l'an 2000, augmenter le temps de réponse des services d'assistance et de maintenance.

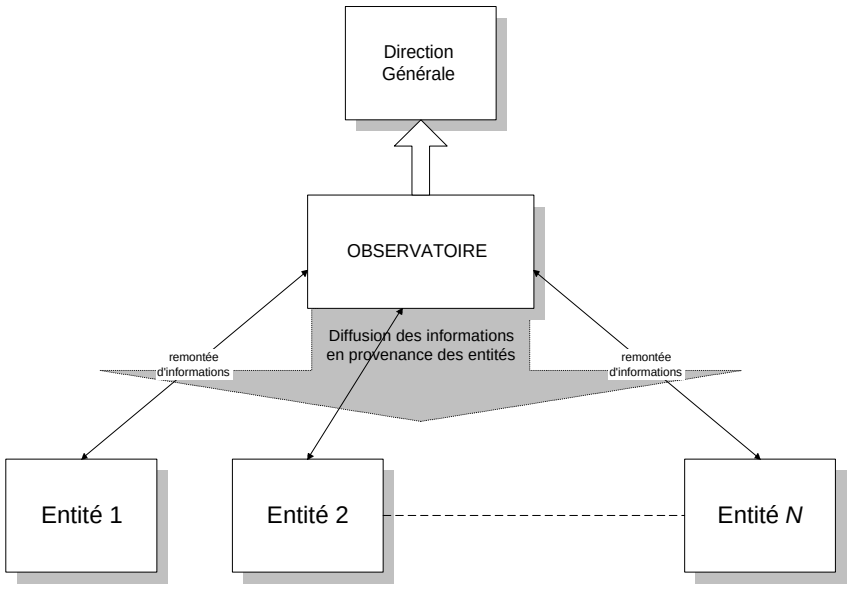
De toutes les façons, au-delà d'une certaine limite, tout le monde serait dans la même situation.

Un plan de continuité doit intégrer une notion de long terme.

Un plan de continuité doit intégrer une notion de long terme. Les conséquences peuvent n'apparaître que plusieurs mois après le passage, par exemple lors de traitements mensuels, trimestriels, annuels ou occasionnels. D'autre part, c'est l'occasion de mettre en place un plan de continuité pour ceux qui n'en disposaient pas avant l'an 2000.

4.1 Cellule de pilotage

En fonction de l'organisation des entreprises, cette cellule de pilotage sera centralisée ou, au niveau de chaque entité, décentralisée. Si l'organisation est décentralisée, les cellules de pilotage doivent rendre compte à un observatoire qui centralise les incidents et diffuse l'information. C'est l'observatoire qui informe la direction générale de la situation de chaque entité.



Organisation de la cellule de pilotage.

Plus on avance dans le temps en 1999 et plus les entreprises travaillent non seulement sur la mise en place d'un plan de continuité mais aussi pour créer une cellule de pilotage qui coordonnera les divers plans de continuité, jugera les dommages causés par le ou les bogues et coordonnera les travaux de correction. Ce n'est que depuis quelques mois qu'est apparu le besoin impératif de disposer d'une telle équipe dont l'objectif sera de maîtriser tous les aspects de ce type d'urgence.

Les centres de commandement ne sont pas systématiquement dirigés par la DSI.

À titre d'exemple, selon un rapport (Cap Gemini), les centres de commandement (aux États-Unis) ne sont pas systématiquement dirigés par la DSI mais en fonction des priorités. C'est ainsi qu'ils sont dirigés par la direction commerciale si la continuité commerciale est prioritaire. Une enquête précise que 62 % le seraient par la direction commerciale et 22 % par un prestataire extérieur travaillant pour la DSI mais la partie commerciale conservant le *leadership*.

Les responsables des services commerciaux ont pris conscience des conséquences éventuelles que pourraient créer la perturbation ou l'arrêt des systèmes informatiques. Ces cellules de pilotage devront agir en intégrant les dimensions de stratégies marketing et commerciale dont l'impact est déterminant sur l'avenir de l'entreprise. Il est bien évident que la partie détection et réparation des pannes incombe à la DSI.

Organisation de la cellule de pilotage

C'est la cellule de pilotage qui décide de la criticité de l'incident et de la mise en œuvre du plan de continuité correspondant. Elle gère les plannings.

Toutes les directions parties prenantes des plans de continuité doivent y être représentées et principalement :

- direction générale ;
- informatique ;
- moyens généraux ;
- commerciale ;
- communication ;
- DRH.

Chaque participant doit avoir une vue globale du fonctionnement de l'entreprise

Chaque participant doit avoir une vue globale du fonctionnement de l'entreprise et être en mesure de prendre des décisions conformes à la stratégie définie. Il doit aussi connaître son remplaçant potentiel et son remplaçant être au même niveau de compétence globale.

Les participants à la cellule de pilotage devront avoir délégation pour engager rapidement les budgets prévus avec des procédures accélérées.

Ils observeront les différents sites de l'entreprise qui sont en décalage horaire pour travailler en préventif plutôt qu'en correctif.

Ils ne devront pas se laisser déborder par des incidents mineurs ou des appels sans conséquence pour la continuité de l'activité de l'entreprise.

Ils devront connaître parfaitement les scénarios d'incidents possibles avec :

- les conséquences en interne et par rapport aux partenaires ;
- les solutions ;
- les délais de mise en œuvre ;
- les délais de reprise.

Ils disposeront de la liste de toutes les personnes sur sites et en astreinte avec leurs profils et leurs rôles.

L'historique détaillé des incidents sera conservé plusieurs mois pour des raisons techniques évidentes.

4.2 Plan de continuité

Tout d'abord, éliminons un problème de vocabulaire. Doit-on dire « plan de continuité » ou « plan de passage » ou « plan de secours » ou « plan d'accompagnement » ou « plan de contournement » ou « *back-up* », etc. ? Tout est bon sous réserve de savoir de quoi l'on parle et que la même chose ne porte pas plusieurs noms différents.

Il faut éliminer « *back up* » . Pour deux raisons :

- la première parce qu'un *back-up* est une solution technique qui consiste simplement (si on peut dire) à disposer, dans un endroit autre que celui où se trouvent habituellement les équipements informatiques, d'une configuration le plus proche possible de celle que l'on utilise couramment sur laquelle il est possible de recharger programmes et données pour assurer un service minimum ;
- la seconde parce que dans le cas précis de l'an 2000, si les programmes, malgré les tests, ne font pas ce pour quoi ils sont faits ou si les données sont polluées, les recharger sur une autre machine ne corrigera ni les programmes ni les données.

Pour les autres termes, la tendance aujourd'hui est de parler de « plan de continuité » parce qu'il est bien question de continuité de l'activité, que ce soit juste avant le 31 décembre à minuit ou que ce soit dans les jours ou les semaines qui suivront le 1er janvier 2000.

Le plan de continuité doit être validé par les plus hautes instances de la société.

L'établissement d'un plan de continuité demande une rigueur certaine puisqu'il envisage l'apparition de situations critiques pouvant mettre en péril la continuité partielle ou totale de l'activité de l'entreprise, d'où la nécessité de le faire valider par les plus hautes instances de la société qui doivent décider du nombre (restreint) de personnes devant y participer.

Le plan de continuité An 2000 doit être établi en partant du plan de continuité standard (s'il existe) pour bénéficier de l'acquis : personnel déjà sensibilisé, déjà formé, déjà entraîné.

Définition d'un plan de continuité An 2000

Il doit fournir les moyens de garantir la continuité de l'activité tout en réduisant au minimum les interruptions de fonctionnement. Il doit prendre en compte non seulement la possibilité d'incidents internes mais aussi toute possibilité de pollution en provenance de sociétés partenaires. Tous les moyens doivent être envisagés y compris la reprise manuelle de certaines

exploitations et d'activités sous-traitées à des partenaires pour assurer la continuité de l'activité principale de la société.

Le passage à l'an 2000 peut être l'occasion d'actions incontrôlées.

Sans être particulièrement pessimiste, il ne faut pas oublier que le passage à l'an 2000 est non seulement lié à des problèmes techniques connus mais qu'il pourrait être aussi l'occasion d'actions incontrôlées, de tentatives d'intrusion dans les systèmes informatiques et d'actions concurrentielles.

4.2.1 Les six phases pour établir un plan de continuité

1. Prendre la décision de la mise en place d'un plan de continuité, définir sa structure, les équipes, le périmètre, la structure hiérarchique.

2. Faire l'inventaire des cibles, définir les périmètres, déterminer les ressources clés (matérielles, logicielles, humaines).

3. Déterminer les priorités, les interdépendances entre applications stratégiques et sociétés partenaires, identifier les raisons qui pourraient mettre en danger les applications : par exemple le dysfonctionnement d'un horodateur par rapport au programme de gestion des horaires et de la paie.

   - Identifier les fonctions dans les missions critiques.
   - Identifier les axes d'activité de l'entreprise qui font partie des missions critiques.
   - Identifier les tâches indispensables dans chaque axe.
   - identifier celles qui pourraient être stratégiques dans l'interdépendance.
   - Évaluer quelles sont les dépendances les plus critiques qui pourraient être génératrices d'incidents graves si elles venaient à défaillir.
   - Évaluer ce qui est contrôlable et ce qui ne l'est pas.

4. Étudier les solutions et rédiger les procédures.

5. Tester la validité du plan.

6. Former les intervenants et faire évoluer le plan en fonction des observations des participants.

4.2.2 Liste des actions à mener

Ce qui suit est à considérer comme une *check-list* non exhaustive dont le but est de rappeler les principales actions pour la mise en place d'un plan de continuité. Il faut :

1. une présentation générale qui explique la nécessité et les moyens nécessaires pour que le plan soit efficace ;

2. la liste des personnes habilitées à connaître les composantes du plan ;

3. déterminer l'objectif et les limites ;

4. définir les hypothèses sur lesquelles les activités de reprises seront faites ;

5. établir la structure de management en définissant le rôle et les responsabilité de chacun ;

6. associer les procédures et les incidents qui peuvent être clairement définis ;

7. définir les procédures d'appel des intervenants et les documents descriptifs de ce que chacun doit faire ;

8. déterminer les lieux de regroupement des équipes avant action ;

9. définir qui évaluera l'étendue des dommages ;

10. lister les décisions à prendre suite à l'annonce d'un incident ;

11. établir la liste des intervenants, des remplaçants, des décideurs ;

12. disposer de tous les documents des sites de *back-up* et des moyens pour y accéder ;

13. établir la liste d'escalade hiérarchique dans les décisions à prendre ;

14. établir la liste des personnes qui ne font pas partie, *a priori*, de l'équipe du plan de continuité mais auxquelles il pourrait être nécessaire de faire appel ;

15. établir la liste des fonctions *business* les plus critiques et l'ordre dans lequel elles devront être traitées ;

16. établir la liste des fonctions stratégiques pour l'activité de l'entreprise, le temps objectif pendant lequel elles peuvent être arrêtées, le niveau et l'ordre dans lequel elles devront être relancées ;

17. faire la liste des tâches que chaque intervenant doit exécuter pendant les relances ;

18. établir la liste des fournisseurs les plus importants et qu'il faudra faire intervenir en urgence ;

19. avoir la liste des éventuels fournisseurs de remplacement ;

20. faire la liste du nombre minimum de stations de travail, de matériels divers et de fournitures nécessaires pour assurer la relance ;

21. définir les moyens techniques nécessaires en télécommunications : nombre, type, etc. ;

22. disposer de l'inventaire des logiciels avec leurs noms, versions, fournisseurs, liens avec d'autres logiciels, supports, documentation, etc. ;

23. connaître la liste des sites de stockage des sauvegardes de données, la liste des responsables avec leurs noms et numéros de téléphone, procédures d'authentification si nécessaire ;

24. disposer de tous les documents administratifs comme les contrats matériels et logiciels, infrastructures ;

25. disposer de toutes les documentations à jour ;

26. disposer de tous les moyens pour accéder aux locaux : accord, clé, badge…

Exemple de fiche d'interdépendance :

	Type de Ressources	Ressources	Risques associés
6	Les données	Fichiers clients, des ventes, historique Catalogue de prix	Pollution, suppression
5	Logiciels applicatifs	Application de vente, *call center, mailing*	Arrêt dû à un problème système
4	Logiciels système	OS, communication, impression	Problème de mise en conformité
3	Équipements	Système central, disques, contrôleurs, réseau local	Problème de mise en conformité
2	Environnement	Climatisation, énergie, PABX	Problème fournisseurs
1	Humaines	Techniciens	Maladie, sous-traitance

Chaque type de ressources dépend du niveau précédent.

Pour les ressources humaines, il faudra veiller à la possible rotation du personnel dans le cadre de contrats de sous-traitance, rotation due au renforcement des équipes d'un client par rapport à un autre.

4.3 Les moyens de contournement

Plusieurs méthodes :

- par redondance : doublement des équipements ;
- par remplacement : matériel de secours sur site avec la même logique de fonctionnement mais ne provenant pas du même fournisseur ;
- par allègement : les applications ou les équipements non indispensables sont arrêtés ;
- par reprise manuelle ;
- par translation de dates :
  - 1972 s'il faut tenir compte de la date, de l'année bissextile et du 1er janvier qui est un samedi,
  - 1994 si l'année bissextile n'est pas importante,
  - 01/05/1999 si seul le 1er du mois doit être un samedi ;

Translation vers	date	Année bissextile	samedi
1972 (-28)	x	x	x
1994 (-6)	x		x
1999 1er mai	x		x

- par des solutions simples, mais qui peuvent être efficaces un premier janvier, comme ventiler et abaisser la température en ouvrant des fenêtres si la climatisation ne remplit pas son rôle.

4.4 Les virus et les tentatives d'intrusion

Tout le monde s'accorde à penser que le moment du passage sera l'occasion d'une part de voir apparaître de nouveaux virus et d'autre part de subir des tentatives de violation des barrières d'accès vers les réseaux d'entreprises.

Pour les virus, la difficulté sera de pouvoir distinguer un virus d'un réel incident dû au passage à l'an 2000. Les utilisateurs devront faire immédiatement appel à leur équipe informatique qui fera le nécessaire.

Les éditeurs d'antivirus seront prêts à trouver le plus rapidement possible les corrections sous réserve que leurs clients leur transmettent une copie des fichiers ou programmes endommagés et un descriptif des symptômes (attention, dans la précipitation, à ne pas transmettre des fichiers confidentiels).

C'est l'occasion de vérifier que les contrats de licences et de mise à jour ne prennent pas fin le 31 décembre 1999…

Les tentatives d'intrusion *via* internet et les réseaux de télécommunications ne pourront être contrées que par les *firewall* (pare-feu), sous réserve qu'eux-mêmes ne soient pas en difficulté et perdent toute efficacité, ne serait-ce que pendant quelques minutes, au moment du passage.

Prévoir des solutions de contournement.

La solution la plus efficace reste, dans la mesure du possible, de déconnecter physiquement le réseau interne de tout accès entrant et sortant au moins au moment du passage lui-même et de prévoir quelques abonnements à des boîtes aux lettres chez des fournisseurs d'accès à Internet ou sur des réseaux publics accessibles par téléphone.

4.5 Les services universels : EDF-Gaz de France, France Télécom

Les systèmes informatiques ne pourront pas fonctionner longtemps s'il n'y a pas d'électricité et de moyens de télécommunications.

Les grands fournisseurs stratégiques comme EDF et France Télécom, ont annoncé que le passage du 31 décembre au 1er janvier 2000 se ferait comme les années précédentes tout en reconnaissant que le caractère particulier du passage à l'an 2000 nécessitait un renforcement des équipes pour pallier un éventuel plus grand nombre d'incidents simultanés. Ce sont des entreprises qui ont l'habitude de respecter des contraintes de fonctionnement 24 heures sur 24 et de garantir une certaine qualité de service.

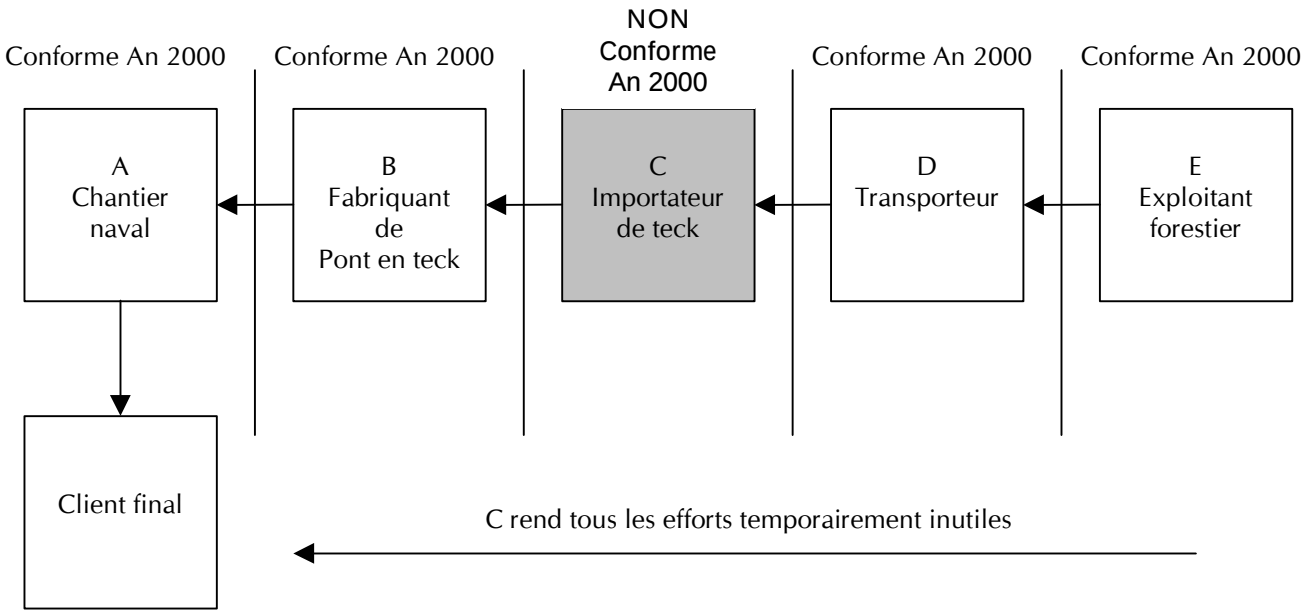
Du côté d'EDF, les moyens de contrôle ont été adaptés, les systèmes de délestage sont prêts et une entraide internationale est prévue. Sa seule préoccupation : connaître suffisamment bien la répartition de charge qui ne sera pas la même que les autres années. Par exemple, les immeubles où sont situés les centres informatiques seront beaucoup plus occupés que d'habitude alors que les locaux des entreprises qui ont choisi de tout arrêter au moment du passage seront inoccupés. D'où une modification dans la répartition des besoins par rapport aux autres fins d'années. C'est pour cela qu'EDF demande à tous ses clients de faire connaître, *via* leur correspondant commercial, quels seront leurs besoins en puissance électrique.

Les équipes seront dimensionnées en conséquence sur sites et en astreinte ainsi que les moyens de production adéquats.

Du côté de France Télécom, le réseau téléphonique fonctionnera, les systèmes informatiques ont été testés ainsi que des liaisons

inter-opérateurs. Dans la mesure du possible, il est souhaitable que les entreprises limitent leurs communications voix et données pendant les trente premières minutes après minuit, le réseau devant alors supporter la pointe de charge due aux appels des particuliers, que ce soit à partir de postes fixes ou de postes mobiles.

4.6 Les tiers



Interdépendance des acteurs face au bogue de l'an 2000.

La préparation du passage s'apparente à la conduite d'une voiture : il faut faire attention à ce que l'on fait et aussi à ce que font les autres.

Aucune entreprise ne vit en autarcie.

Aucune entreprise ne vit en autarcie, elle dépend de fournisseurs et elle est elle-même fournisseur pour d'autres. Ce n'est pas parce qu'à son niveau elle aura parfaitement fait tout ce qu'il fallait que son activité ne sera pas perturbée par des incidents venant de sa chaîne d'approvisionnement.

Il faut donc s'inquiéter du niveau de préparation de chaque fournisseur, y compris de son état de connaissance de ses propres fournisseurs (niveaux *n* - 1 et *n* - 2).

Comment déterminer les tiers particulièrement stratégiques ? En fonction du risque potentiel qu'ils introduisent dans la continuité de l'activité de l'entreprise par :

- le manque de maîtrise de techniques évoluées telle que l'EDI, Internet… ;
- la dépendance d'autres tiers dont la préparation n'est pas ou mal connue ;
- l'impossibilité de mettre en place des solutions de contournement ;
- l'insouciance dans la préparation au passage ou le retard dans la mise à niveau.

Les questions à se poser :

- combien de temps peut-on accepter un arrêt du système informatique ou d'une application critique ?
- combien de temps peut-on accepter l'arrêt d'approvisionnement en fonction des stocks et des surfaces de stockage ?
- quel est le minimum d'approvisionnement acceptable pour maintenir une activité considérée comme suffisante ?
- où est-il possible de sur stocker ?
- quels autres fournisseurs sont possibles ?
- quels surcoûts sont acceptables ?
- etc.

5. COMMUNICATION

Jusqu'à maintenant la communication est principalement restée au niveau interne des entreprises pour sensibiliser les utilisateurs en s'appuyant sur les différents moyens existants comme les journaux internes, par exemple.

Il ne faut pas faire reposer toute la communication de l'entreprise sur un intranet.

Un intranet a, la plupart du temps, été mis en place pour informer en interne sur les conséquences du passage à l'an 2000, les travaux de la DSI et l'état d'avancement par rapport aux plannings. Mais d'un avis général, ce n'est pas le seul moyen à retenir, compte tenu du manque d'habitude de consultation chez les utilisateurs. Dans le cas où l'information est transmise par intranet, elle est donc doublée par un document papier remis directement aux destinataires.

Les directions de la communication ont tendance à retarder le moment où il faudra aborder la préparation d'une éventuelle communication de crise. Trois raisons principales :

1. peu d'entre elles ont déjà eu l'occasion de traiter ce type de situation ;

2. imaginer le pire avant d'y être confronté est un exercice difficile ;

3. apparemment très rassurées par les équipes techniques, elles ne ressentent pas encore la nécessité d'en parler.

Ceci étant, il ne serait pas raisonnable de faire l'impasse sur cette possibilité et il faut se rappeler qu'une communication de crise doit répondre aux critères suivants :

- éviter le « *no comment* » ;
- être contrôlée : pas de communiqués contradictoires ;
- être réactive donc rapide ;
- avoir été anticipée.

Quelle que soit la cible, les employés, les actionnaires et surtout les médias, seule une personne préparée ou disposant d'un document réalisé par des professionnels doit intervenir. Parallèlement, une équipe dédiée doit être mise en place pour répondre aux forces commerciales qui auront à communiquer avec la clientèle.

Les messages doivent être clairs, sans ambiguïté et refléter la réalité.

Les conséquences d'une mauvaise communication, surtout dans le cas de l'an 2000, qui jouera un rôle d'amplificateur, ne sont pas mesurables dans leur amplitude et leur durée.

5.1 Le comportement des personnes

Jusqu'à maintenant, le comportement des personnes face au bogue de l'an 2000 est resté proche de l'indifférence.

Le rôle des médias sera déterminant dans l'évolution de ce comportement pour faire prendre conscience des risques sans exagération.

Le risque possible pourrait venir d'une prise de conscience tardive déclenchée sur un événement dont la présentation prêterait à confusion dans sa gravité.

D'une façon générale les salariés, considérant que c'est avant tout un problème de technique informatique, font confiance à leur DSI.

5.2 La veille

Les directions de la communication devront assurer une veille des médias : radio, télévision, presse écrite, pour prendre connaissance des incidents, les analyser et répercuter l'information vers la cellule de pilotage et les personnes concernées. Symétriquement, les responsables opérationnels devront alerter en temps réel la DSI en cas d'incidents ou d'accidents afin que l'ensemble des problèmes soit appréhendé.

5.3 Quelques questions à se poser

Cette *chek-list*, non exhaustive, a été présentée par le cabinet Fleishman Hillard International Communications.

- Pouvez-vous expliquer clairement et simplement la nature la dimension du problème général An 2000 ?
- Pouvez-vous expliquer clairement et simplement les défis An 2000 pour votre société ?
- Avez-vous un plan presse, tant proactif que réactif ?
- Avez-vous un plan de communication de crise pour gérer des situations critiques ? Prévoit-il un processus précis de prise de décision ?
- Avez-vous un porte parole désigné, clairement identifié en interne ?

- Êtes-vous prêts à gérer un nombre important d'appels de clients ou des médias ?
- Êtes-vous prêt à répondre à des critiques des pouvoirs publics à l'encontre de votre industrie ?

6. *RESSOURCES HUMAINES*

Y a-t-il une raison pour ne pas considérer le projet de passage à l'an 2000 comme tout autre projet ? Pourquoi nécessite-t-il des dispositions particulières ?

- Parce que l'activité de l'entreprise et peut-être son existence sont en cause.
- Parce qu'il est mondial.
- Parce qu'aucun autre projet informatique de même envergure avec les mêmes enjeux ne s'est jamais produit.
- Parce que tout le monde dépend de tout le monde.
- Parce que la date n'est pas négociable.

la période la plus tendue sera celle qui entoure le 31 décembre à minuit.

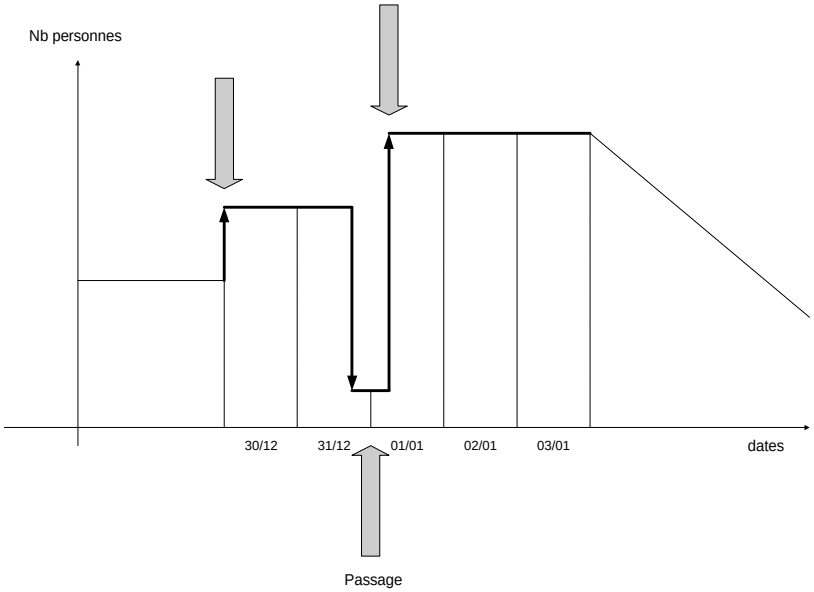
Bien que le commencement du projet An 2000 remonte à plusieurs années, il n'en demeure pas moins vrai que la période la plus tendue sera celle qui entoure le 31 décembre à minuit.

Comme on l'a vu, le planning théorique commence le 30 décembre 1999 pour se terminer le 3 janvier 2000. En fait, la période s'étendra sur une durée plus longue qui peut être découpée en 3 phases :

- avant le 30 décembre, phase étroitement liée au planning mis en place dans les entreprises ainsi qu'à leur état d'avancement et des travaux de fin d'année ;
- du 30 décembre au 3 janvier 2000, phase commune à toutes les entreprises ;
- après le 3 janvier 2000, phase liée aux incidents aléatoires ou à une mauvaise préparation, qui pourra s'étendre très largement au-delà du 3 janvier.

À ceci s'ajoutera le problème du 29 février 2000, l'année 2000 étant bissextile, ce que beaucoup oublient encore…

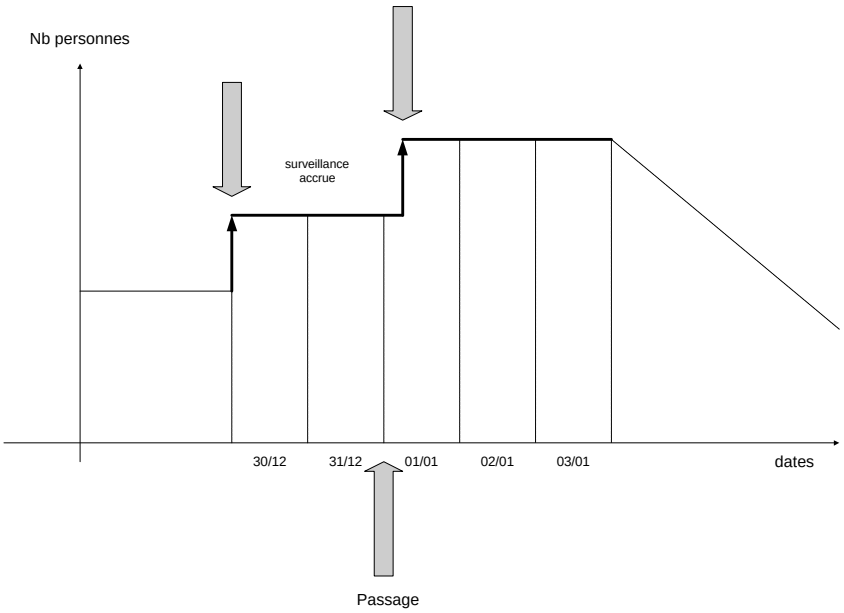
La charge sera malgré tout centrée sur les quelques jours qui précèdent et suivent le 31 décembre à minuit. On peut considérer que cette charge (en nombre de personnes) évoluera de la façon suivante :



Évolution des besoins en ressources humaines (mode non continu).

Au moment du passage, les entreprises qui auront mis leurs machines en veille disposeront d'équipes réduites : la cellule de pilotage et les quelques spécialistes indispensables. C'est à partir du 01/01/2000 à midi que des forces plus importantes seront réactivées.

Inversement pour les entreprises qui passeront en continu, le nombre d'observateurs sera important surtout pour toute l'informatique enfouie qui n'aura pas pu être testée.



Évolution des besoins en ressources humaines (mode continu).

Le groupe de travail Jour J-RH du Cigref qui a débattu des moyens d'avoir des ressources informatiques suffisantes autour du jour J a mis en évidence :

- que le problème était de taille ;
- que peu d'entreprises avaient désigné un responsable sur le sujet et qu'elles comptaient plus sur les relations directes DSI et DRH ;

La communication entre les chefs de projets an 2000 et les DRH n'est pas toujours évidente.

- que la communication entre les chefs de projets An 2000 et les DRH n'était pas toujours évidente, les uns attendant les autres ; Les DRH attendent les chefs de projet pour connaître l'étendue du besoin et les chefs de projets attendent les DRH pour connaître les compensations qu'ils pourront mettre en face des contraintes de présence ;
- que les compensations n'étaient pas définies car elles sont fortement liées à l'entreprise et se situent dans un contexte très particulier et très rare ;
- que certaines entreprises sont déjà organisées pour le travail en continu.

Quelles informations attendent les chefs de projet des DRH ?

- des règles de compensation simples ;
- une coopération dans la communication avec les personnes ;
- une assistance dans les relations avec les représentants du personnel.

Quelles informations attendent les DRH des chefs de projets ?

- des listes nominatives par fonctions ;
- des dates ;
- des relevés de présence pour les autorités administratives ;
- des justifications des débordements.

Les grandes entreprises et principalement les banques ont déjà acquis de l'expérience lors du passage à l'euro. Le nombre d'intervenants sera sans doute supérieur. Mais en grande partie ce seront les mêmes personnes qui interviendront lors du passage à l'an 2000.

6.1 Les dérogations

Le Cigref, participe au groupe « questions sociales » du Comité National an 2000 qui a pour mission de déterminer les problèmes éventuels causés par le passage à l'an 2000 et de proposer des solutions.

La charge de travail imposera certainement des dépassements par rapport aux bornes fixées par la réglementation du travail et qui sont rappelées dans le paragraphe suivant. La réglementation exige alors de faire une demande de dérogation auprès des autorités (préfecture, inspection du travail).

Dans le cas particulier du repos hebdomadaire, qui est en principe le dimanche, l'article L. 221-12 du code du travail permet de le suspendre pour exécuter des travaux urgents (cf. annexe 2).

6.2 Les compensations

Rappelons que le droit du travail repose sur les éléments suivants :

- la durée journalière légalement limitée à 10 heures ;
- la durée hebdomadaire légalement limitée à 48 heures ;
- la durée hebdomadaire « moyenne » sur 12 semaines limitée à 46 heures ;
- 11 heures de repos quotidien ;
- le respect du repos hebdomadaire qui, en principe, doit être le dimanche.

Le passage à l'an 2000 a un caractère indéfectible et irrémédiable.

Deux écoles s'opposent quant aux compensations : celle de ceux qui considèrent que le projet An 2000 ne mérite pas plus d'attention qu'un autre projet et celle de ceux qui intègrent le caractère indéfectible et irrémédiable du passage à l'An 2000.

Si la première école est basée sur un réflexe administratif et financier, la seconde repose sur un réflexe technique qui nécessite des efforts particuliers liés à des risques qui vont bien au-delà du simple retard de projet et qui touchent l'activité même de l'entreprise : il n'est pas possible d'envisager de ne pas passer en l'an 2000 !

Les idées de compensations exceptionnelles couvrent un large éventail de possibilités allant de l'appel à l'esprit civique, et donc au bénévolat, jusqu'aux récupérations.

Il semble que le fait d'être sur site au moment du passage et de faire partie des équipes réduites du plan de continuité soit un élément en mesure de compenser les efforts produits. Mieux, côtoyer la haute hiérarchie qui sera sur place pourrait être un élément important en ce qui concerne les aspects relationnels. Un caractère élitiste pourrait alors apparaître, le phénomène s'étant déjà produit pour le passage à l'euro : ceux qui y étaient et ceux

qui n'y étaient pas... Ce type de situation doit être géré avec précaution.

Le principe de la récupération est à utiliser avec prudence pour les raisons suivantes :

- ce sont, très certainement, les mêmes personnes qui vont cumuler les récupérations ;
- il y a donc risque de récupération de longue durée (plusieurs semaines) ;
- il sera impossible de libérer totalement et pour une longue période des spécialistes.

Chaque entreprise doit résoudre ce problème en fonction de sa propre culture, de ses habitudes et de ses propres contraintes.

6.3 Les intervenants

La liste des personnes indispensables et leur rôle pour la période du passage doivent être établis largement à l'avance pour pouvoir les informer et faire en sorte que ces personnes ne prennent aucune disposition personnelle d'absence pour cette période. Nombreuses sont les entreprises qui ont déjà annoncé la réduction voire l'interdiction de prendre des vacances pendant les mois de décembre et janvier.

Ces personnes devront être formées et fortement sensibilisées à leur responsabilité.

Pour assurer les possibles débordements du fait de la simultanéité des incidents, il faut prévoir des équipes de renfort spécialisées et ayant les moyens de se déplacer sur différents sites.

Toutes ces personnes devront pouvoir maintenir leur présence au-delà du 03/01/2000 en fonction des besoins.

Il y a aussi nécessité de préparer moralement le personnel pour cette période tendue et de veiller à son confort sur site (boissons, nourriture, logement à proximité, parking, moyens de communication avec leur famille...).

7. ASPECTS JURIDIQUES DU PASSAGE À L'AN 2000

Pour tous les aspects juridiques du passage à l'an 2000, le lecteur se reportera utilement aux rapports Opération an 2000 1er et 2e parties du Cigref et consultera le site Cigref2000.com

Il pourra aussi bientôt prendre connaissance d'un rapport du groupe de travail Droit et Assurances qui s'est réuni sous l'égide du Comité national An 2000 à Bercy et où se sont exprimées toutes les sensibilités des acteurs : utilisateurs, constructeurs, éditeurs, sociétés de services, assureurs, etc.

Enfin, il pourra aussi lire avec profit le rapport de la DG XXIV de la Commission européenne préparé par le Cabinet Berlioz & Cie.

À ce jour, le Cigref maintient ses positions en ce qui concerne le partage des responsabilités. Ces positions sont bien connues, même si elles ne sont pas partagées, comme on s'en doute, par les fournisseurs.

La recommandation actuelle du Cigref aux entreprises est :

Sécurité des personnes et des biens et continuité de l'activité.

1. de privilégier clairement le passage opérationnel à l'an 2000 en mettant en priorité : la sécurité des personnes, puis la sécurité des biens et la continuité de l'activité de l'entreprise, donc de ne pas dissiper d'énergie dans les contentieux prématurés et hasardeux ;

2. de conserver soigneusement trace de tous les éléments permettant de reconstituer ultérieurement l'historique détaillé pour pouvoir examiner posément le problème du partage des responsabilités si cela s'avère nécessaire ;

3. de rassembler tous les éléments permettant de montrer, de façon aussi détaillée que possible, que les meilleurs efforts ont été faits par les entreprises utilisatrices afin de prendre toutes les précautions raisonnablement possibles face à la situation particulière que crée le passage à l'an 2000.

8. *LA CONTRIBUTION DU CIGREF À L'INFORMATION DE TOUTES LES ENTREPRISES*

Depuis plusieurs mois, le Cigref a ouvert sa base de compatibilité An 2000 à toutes les entreprises et personnes ayant besoin de s'informer sur la conformité des matériels et logiciels face à l'an 2000 (www.cigref2000.com).

Cinq membres du Cigref ont accepté de mettre en ligne sur un serveur accessible *via* internet, leur base de conformité An 2000 :

- EDF-Gaz de France ;
- La Poste ;
- France Télécom ;
- Thomson-CSF ;
- Axa.

Ces informations se présentent sous deux formes :

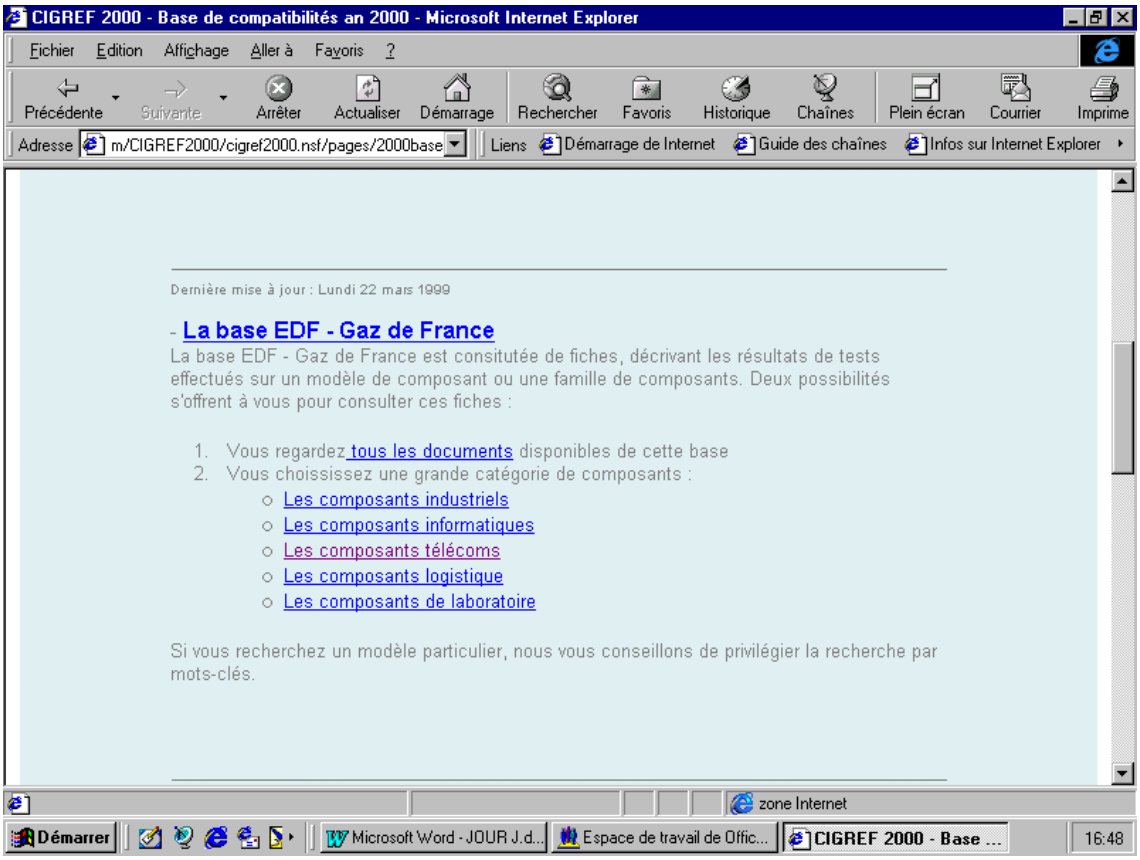
- des fiches techniques ;
- des documents méthodologiques.

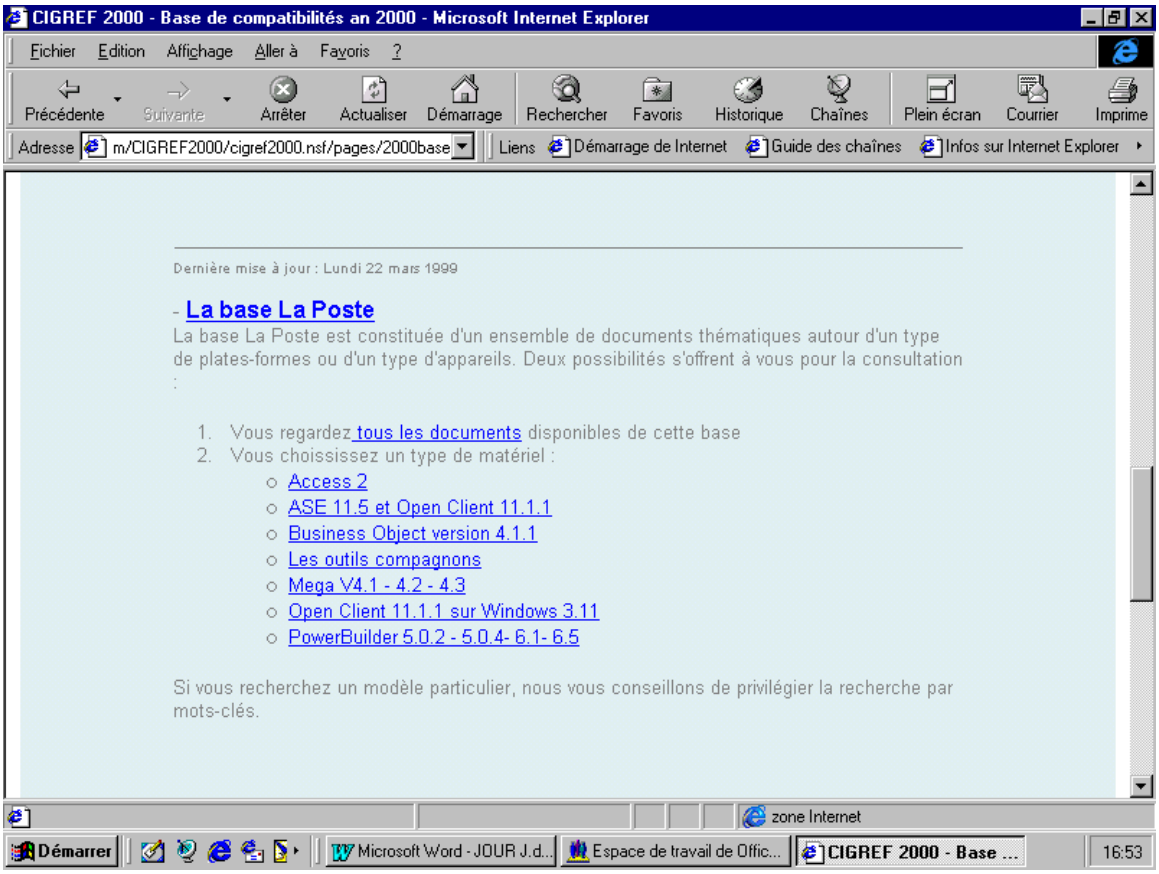
La recherche peut se faire de deux façons :

- par mots clés ;
- par la source.

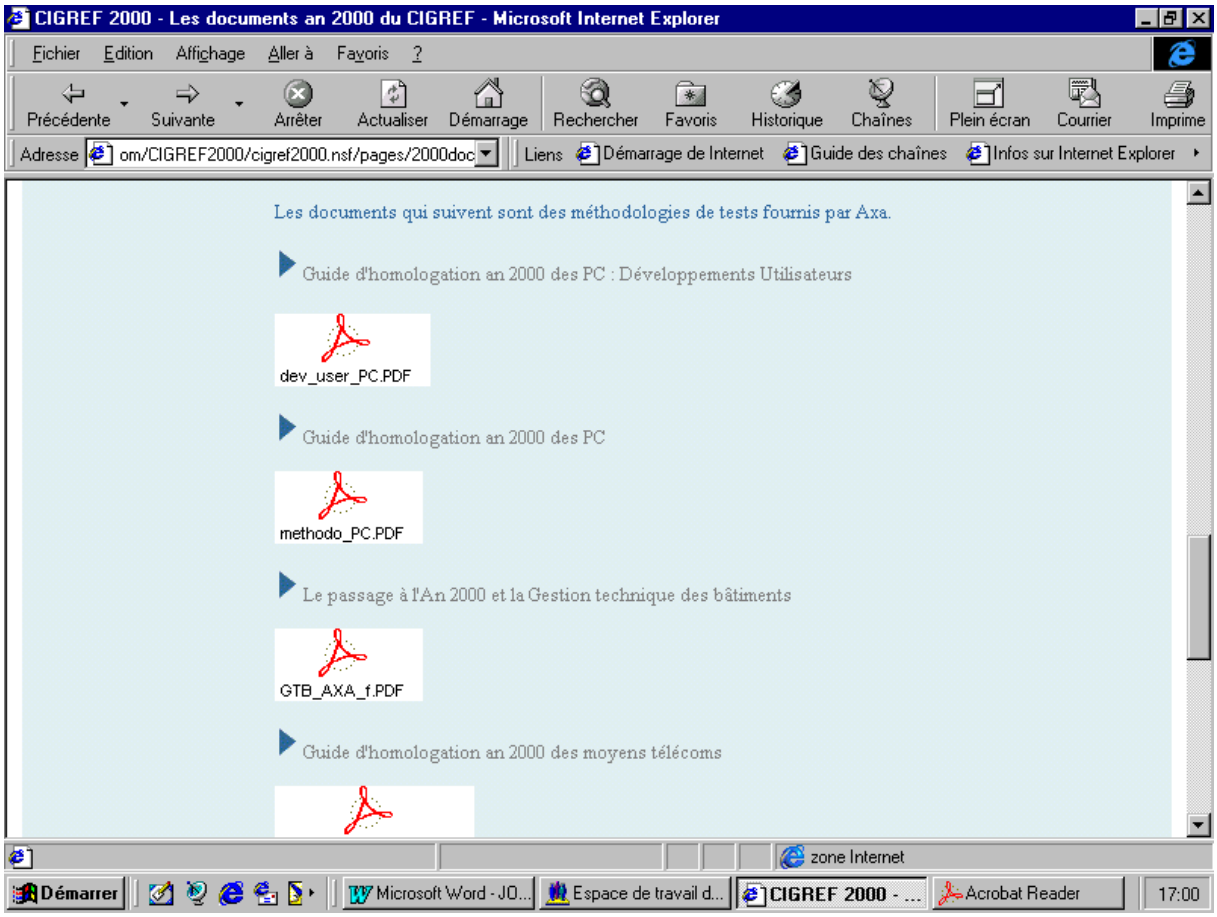
La consultation de cette base ne doit pas exclure la consultation de celles des éditeurs et constructeurs qui vont certainement évoluer d'ici la fin de l'année.

Exemple d'informations accessibles :




CIGREF 2000 - Base de compatibilités an 2000 - Microsoft Internet Explorer
Fichier Edition Affichage Aller à Favoris ?
Précédente Suivante Arrêter Actualiser Démarrage Rechercher Favoris Historique Chaînes Plein écran Courrier Imprime
Adresse m/CIGREF2000/cigref2000.nsf/pages/2000base
Liens Démarrage de Internet Guide des chaînes Infos sur Internet Explorer
Dernière mise à jour : Lundi 22 mars 1999
- La base La Poste
La base La Poste est constituée d'un ensemble de documents thématiques autour d'un type de plates-formes ou d'un type d'appareils. Deux possibilités s'offrent à vous pour la consultation :
1. Vous regardez tous les documents disponibles de cette base
2. Vous choisissez un type de matériel :
Access 2
ASE 11.5 et Open Client 11.1.1
Business Object version 4.1.1
Les outils compagnons
Mega V4.1 - 4.2 - 4.3
Open Client 11.1.1 sur Windows 3.11
PowerBuilder 5.0.2 - 5.0.4- 6.1- 6.5
Si vous recherchez un modèle particulier, nous vous conseillons de privilégier la recherche par mots-clés.
zone Internet
Démarrer
Microsoft Word - JOUR J.d...
Espace de travail de Offic...
CIGREF 2000 - Base ...
16:53


CIGREF 2000 - Base de compatibilités an 2000 - Microsoft Internet Explorer
Fichier Edition Affichage Aller à Favoris ?
Précédente Suivante Arrêter Actualiser Démarrage Rechercher Favoris Historique Chaînes Plein écran Courrier Imprime
Adresse m/CIGREF2000/cigref2000.nsf/pages/2000base
Liens Démarrage de Internet Guide des chaînes Infos sur Internet Explorer
Dernière mise à jour : Jeudi 1er avril 1999
- La base Thomson-Csf
La base Thomson-Csf est consitutée de fiches, décrivant les résultats de tests effectués sur un modèle de composant ou une famille de composants.
Vous ne pouvez consulter cette base qu'en consultant tous les documents disponibles de cette base, ils sont triés par fournisseur.
Si vous recherchez un modèle particulier, nous vous conseillons de privilégier la recherche par mots-clés.
Dernière mise à jour : Lundi 3 mai 1999
- La base France Télécom
La base France Télécom est consitutée de fiches, décrivant les résultats de tests effectués sur un modèle de composant ou une famille de composants.
Ces résultats sont présentés sous deux formes : des textes présentant un ensemble de résultats et des fiches de résultats individuels.
Vous ne pouvez consulter cette base qu'en consultant tous les documents disponibles de cette base.
Si vous recherchez un modèle particulier, nous vous conseillons de privilégier la recherche par
zone Internet
Démarrer
Microsoft Word - JOUR J.d...
Espace de travail de Offic...
CIGREF 2000 - Base ...
16:56


CIGREF 2000 - Les documents an 2000 du CIGREF - Microsoft Internet Explorer
Fichier Edition Affichage Aller à Favoris ?
Précédente Suivante Arrêter Actualiser Démarrage Rechercher Favoris Historique Chaînes Plein écran Courrier Imprime
Adresse om/CIGREF2000/cigref2000.nsf/pages/2000doc
Liens Démarrage de Internet Guide des chaînes Infos sur Internet Explorer
Les documents qui suivent sont des méthodologies de tests fournis par Axa.
Guide d'homologation an 2000 des PC : Développements Utilisateurs
dev_user_PC.PDF
Guide d'homologation an 2000 des PC
methodo_PC.PDF
Le passage à l'An 2000 et la Gestion technique des bâtiments
GTB_AXA_f.PDF
Guide d'homologation an 2000 des moyens télécoms
zone Internet
Démarrer
Microsoft Word - JO...
Espace de travail d...
CIGREF 2000 - ...
Acrobat Reader
17:00

9. ÉTAT D'AVANCEMENT DE LA FRANCE DANS SA PRÉPARATION AU PASSAGE À L'AN 2000

Les grandes entreprises françaises tiennent leur planning. Les tests d'intégration ont atteint fin juin le niveau d'avancement prévu, les mois de juillet et août ont été consacrés aux corrections des derniers incidents.

Les quatre derniers mois vont être consacrés :

- à maintenir des exploitations stables ;
- à l'organisation du passage lui-même ;
- à la mise en place des plans de continuité détaillés.

Jusqu'au dernier moment les équipes resteront attentives à toute possibilité d'incident et seront prêtes à agir.

L'observatoire de Global 2000 qui suit attentivement la mise en conformité des pays suivant 7 critères :

- services financiers ;
- systèmes de transferts bancaires ;
- opérateurs de télécommunications ;
- systèmes de transports ;
- fournisseurs d'énergie ;
- fournisseur d'eau ;
- administration ;

a classé la France au meilleur niveau de préparation pour aborder le passage à l'an 2000.

Les dispositions sont prises pour faire face aux incidents résiduels qui apparaîtront après la remise en exploitation.

10. CONCLUSION

L'état de préparation des grandes entreprises est tout à fait satisfaisant. Celles-ci restent vigilantes jusqu'au dernier moment. Un bogue sournois et caché est toujours possible.

Ce qu'il fallait faire a été fait.

Les DSI et leurs équipes projets ont manifestement fait tout ce qui était réalisable et il serait étonnant que l'on puisse leur reprocher soit des investissements trop importants, sous prétexte que le passage s'est bien déroulé *in fine*, soit des investissements trop faibles, sous prétexte que des incidents se sont produits à tort.

Ce qui est sûr, c'est que le budget du projet An 2000 ne sera pas clos le 31 décembre à minuit.

Il reste trois grandes inconnues : l'instabilité des états de compatibilité chez les éditeurs et constructeurs, les incidents aléatoires avec leur gravité et leur nombre, les incidents qui peuvent être générés par des tiers mal préparés.

Les mises à jour tardives seront génératrices de situations bloquantes.

Les éditeurs et constructeurs doivent comprendre que les entreprises qui gèrent des parcs de plusieurs milliers de terminaux ne pourront pas, malgré toute leur bonne volonté, déployer des mises à jour au-delà de fin septembre.

Pour ce qui est des incidents aléatoires, les dispositions sont déjà prévues et les équipes sont prêtes à agir.

Pour les tiers, il faut se souvenir :

- que toute entreprise qu'elle soit grande, moyenne ou petite dépend d'autres entreprises ;
- qu'un processus quel qu'il soit a pour valeur la valeur de son élément le plus faible.

Le manque de préparation de certains pourrait réduire fortement ou totalement les efforts faits par les autres.

Il appartient donc à chacun d'agir comme il se doit et de faire tout son possible pour être compatible An 2000. S'il n'est pas en mesure de le faire ou s'il n'a pas eu le temps alors il doit, sans hésitation, suspendre toute transmission automatique de données vers ses partenaires au moins pendant le mois de janvier et prendre avec eux toutes les dispositions nécessaires pour détecter et limiter les incidents au moment de leur reprise.

Chacun pour tous !

ANNEXE 1 : Questionnaire

Liste des questions posées à certains fournisseurs pour connaître l'assistance mise en place dans le cadre particulier du passage à l'An 2000.

1. À partir de quelle date et jusqu'à quelle date le dispositif sera-t-il opérationnel ?

2. Quelles que soient les limites du service que vous avez défini, quels seront les horaires du service d'appels téléphoniques pour la période du 27/12/19999 au 09/01/2000 ?

3. Quelle disponibilité du service est particulièrement prévue pour les dates du 31/12/1999 et du 03/01/2000 ?

4. Avez-vous un dispositif réservé aux grands comptes comme les membres du Cigref ?

5. Tous vos clients auront-ils droit à ce service ou seulement ceux qui sont sous contrat ?

6. Par rapport à la question précédente, si la condition est d'être sous contrat de maintenance, est ce que cela s'applique à tous les types de contrat ? Sinon, lesquels ?

7. Y aura-t-il un n° d'appel spécifique ?

8. Par rapport à la question précédente, s'il y a un n° spécifique, comment le ferez-vous connaître ?

9. Le n° spécifique sera-t-il connu de tous vos clients ou seulement de ceux disposant d'un contrat ?

10. Le n° d'appel sera-t-il gratuit ?

11. Si ce n° est déjà connu, quel est-il ?

12. Combien de communications simultanées pourrez-vous absorber ?

13. Avez-vous prévu de communiquer à vos clients des n° de téléphones mobiles pour faciliter l'accès à vos spécialistes ?

14. Envisagez-vous soit des extensions de contrats soit des contrats de maintenance particuliers limités à la durée de votre dispositif ?

15. Avez-vous hiérarchisé vos clients dans l'urgence des interventions ? Autrement dit, avez-vous établi des priorités entre clients ? si oui, sur quels critères (type de contrats, taille de la configuration, importance stratégique de l'activité, etc. ?

16. Disposez-vous de toutes les informations récentes (matériels et logiciels) concernant les installations de vos clients ?

17. Avez-vous un système de débordement d'appels vers d'autres centres, y compris hors de France, et lesquels ?

18. Vos clients pourront-ils s'exprimer uniquement en français ou faudra-t-il qu'ils pratiquent aussi la langue anglaise ?

19. Quel est le pourcentage d'accroissement de vos forces vives durant cette période ?

20. Quel est le délai de réponse sur lequel vous vous engagez en terme de prise d'appel ?

21. Quelle est la procédure d'escalade en terme de *timing* et de degré de compétence ?

22. La prise d'appel sera-t-elle directement opérationnelle ou ne sera-t-elle qu'une chambre d'enregistrement nécessitant le rappel par un technicien ?

23. Par rapport à la question précédente, quel est votre engagement dans le délai de rappel ?

24. Quels sont les moyens de communication que vous avez prévus pour maintenir le contact avec vos clients : téléphone fixe et mobile, fax, télex, Internet, LS, VSAT... ?

25. Avez-vous (vous = *hot line*) prévu une solution sûre voire « rustique » pour vous atteindre rapidement : fax, messagerie, téléphone personnel fixe et mobile, adresse... ?

26. Quelles sont les éléments que vous exigerez lors d'un appel : n° de contrat, nom d'un responsable ?

27. Quels seront vos moyens pour suivre un appel tant qu'il reste ouvert ?

28. Avez-vous décidé que tant qu'un appel reste ouvert, le ou les intervenants ne doivent en aucun cas raccrocher sauf sur accord mutuel client-fournisseur ?

29. En cas de raccroché accidentel, le client abandonné sera-t-il repris en priorité et avec le même interlocuteur ?

30. Disposez-vous de matériels ou logiciels de secours et en quel endroit : à votre siège, sur site, revendeurs... ?

31. Par rapport à la question précédente quels sont les moyens mis en place pour assurer leur transport vers les sites : coursiers, transport express, télétransmission… ?

32. Disposez-vous de relais régionaux et quelle sera leur organisation pendant cette période ?

33. Pouvez-vous transmettre la liste de ces relais et leurs coordonnées : adresse, téléphone, fax, mail ?

34. Vos clients auront-ils la possibilité de les joindre (les relais) directement ou les appels seront-ils centralisés ?

35. Avez-vous prévu une base de connaissance mise à jour au fil de l'eau (internationale) consultable directement et donnant la liste des problèmes rencontrés et le statut des solutions ?

36. À partir de quand avez-vous prévu de faire du *push* sur vos serveurs pour faciliter la détection des mises à jour ? septembre 1999 ?

37. Avez-vous connaissance des points sensibles et à risque chez vos clients et avez-vous prévu une présence sur site ou à proximité ?

38. Quelles sont vos préconisations quant au moment du passage, pour les logiciels et pour les matériels : arrêt logique*, power off*… ?

39. Sur quel site web peut-on trouver vos préconisations ?

ANNEXE 2 : Extrait du code du travail

Cet article du code du travail pourrait être appliqué lors d'incidents aléatoires pouvant survenir au-delà du 1er janvier 2000 et nécessitant de travailler le dimanche.

Article L. 221-12

En cas de travaux urgents dont l'exécution immédiate est nécessaire pour organiser des mesures de sauvetage, pour prévenir des accidents imminents ou réparer des accidents survenus au matériel, aux installations ou aux bâtiments de l'établissement, le repos hebdomadaire peut être suspendu pour le personnel nécessaire à l'exécution des travaux urgents.

Cette faculté de suspension s'applique non seulement aux salariés de l'entreprise où les travaux urgents sont nécessaires, mais aussi à ceux d'une autre entreprise faisant les réparations pour le compte de la première. Dans cette seconde entreprise chaque salarié doit jouir d'un repos compensateur d'une durée égale au repos supprimé. Il en est de même pour les salariés de la première entreprise préposés habituellement au service d'entretien et de réparation.

ANNEXE 3 : Équipements concernés par le bogue

Informatique enfouie

Rappel de quelques équipements pouvant être touchés par le bogue (liste non exhaustive) :

- Stations électrique
- Stations de pompage d'eau
- Systèmes de raffinage et de stockage
- Simulateurs
- Automates industriels
- Systèmes de contrôle et de tests pour la maintenance
- Avions, trains, bateaux…
- Système de contrôle du trafic aérien
- Systèmes de signalisation (feux de circulation, balises, phares, …)
- Radars
- Distributeurs automatiques de tickets
- Systèmes d'accès et de paiement des parkings
- Systèmes de secours électriques et groupe électrogène
- Surveillance incendie
- Climatisations et ventilations
- Ascenseurs, monte-charge
- Système de surveillance vidéo
- Serrures automatiques
- Centraux téléphoniques
- Télécopieurs
- Systèmes d'enregistrement de messages
- Téléphones mobiles
- Systèmes de carte de crédit
- Terminaux points de ventes
- Défibrillateurs cardiaques
- Contrôleurs de pacemaker
- Systèmes d'information pour les malades
- Systèmes de surveillance médicale
- Etc.

ANNEXE 4 : Check-list pour un PC

Exemple de ***check-list*** pour une station à base de micro-ordinateur

Avant de faire appel à la hot line

AVANT le passage :

- sauvegarder ses fichiers sur les disques du réseau ? qui eux seront sauvegardés par les équipes réseau ;
- sauvegarder sur disquette ses fichiers sensibles et vérifier la qualité de la sauvegarde ;
- faire une copie d'écran (touche « impr. écran ») de son bureau sous Windows ;
- relever la liste de ses progiciels (traitement de texte, tableur, logiciel de présentation, gestionnaire de base de données, outils graphiques, utilitaires, etc.
- imprimer la liste des ses fichiers avec leur date et leur taille ;
- réaliser les adaptations recommandées par la DSI…

APRÈS le passage :

- mise sous tension
  - ➢ en cas de problème :
    - vérifier tous les branchements électriques, inter-équipements et réseau,
  - ➢ électrique :
    - en cas de doute sur l'alimentation électrique tester la ou les prises par remplacement, par exemple avec une lampe de bureau dont on est sûr,
  - ➢ Inter-équipements :
    - écran sur l'unité centrale,
    - clavier sur unité centrale,
    - souris sur unité centrale,
    - imprimante si elle est locale,
    - alimentation de l'unité centrale,
    - alimentation de l'écran,
    - alimentation de l'imprimante si elle est locale ;
  - ➢ réseau :
    - connexion du câble entre l'unité centrale et la prise du réseau local,
    - qualité du câble en le permutant avec un autre câble sûr ;

- les dates :

  - se référer aux recommandations faites par la DSI.

En dernier recours, vérifier auprès d'une autre personne ayant le même profil de station et située à proximité si sa station fonctionne correctement.

Si le problème persiste, alors faire appel à la *hot line*.

ANNEXE 5 : Recommandation de l'AFECEI

Le 2 juillet 1999

RECOMMANDATION DE L'AFECEI RELATIVE À LA JOURNÉE DU 31 DÉCEMBRE 1999

1. De l'ensemble des travaux menés, tant au plan européen que national, sur la préparation au passage à l'an 2000 de la communauté bancaire et financière, il ressort que :

- Le Conseil des Gouverneurs de la Banque Centrale Européenne (BCE) a décidé de fermer le 31 décembre 1999 l'ensemble des systèmes nationaux de règlement brut en temps réel (TBF pour la France) et donc leur interconnexion dans TARGET ;

- Les autres systèmes interbancaires de paiement et de règlement seront fermés le 31 décembre 1999, à savoir :

  - PNS (Paris Net Settlement)
  - SIT (Système interbancaire de télécompensation)
  - CHCP (Chambre de compensation de Paris))
  - CERCO (Centrale d'échanges et de règlement des chambres de compensation)
  - Chambres de compensation de province et CREIC (Centres régionaux d'échange d'images-chèques) ;

- Les systèmes de négociation, de compensation et de règlement livraison (Relit et RGV) des marchés gérés par le groupe Paris Bourse SA et Sicovam SA seront également fermés ;

- Selon la lettre du président du Comité français d'organisation et de normalisation bancaires en date du 27 mai 1999, le 31 décembre 1999 ne sera pas un jour ouvré, pour l'application de tous les textes dans lesquels des dates d'exécution des opérations, des dates de règlement ou des délais sont fonction des jours ouvrés ;

- Le Système interbancaire d'autorisation pour les opérations par cartes (RCB : Réseau cartes bancaires) restera ouvert sans interruption, assurant ainsi la continuité du service de retraits d'argent aux distributeurs de billets, et de paiements par cartes par l'intermédiaire des terminaux de paiement du commerce ;

2. Compte tenu de l'ensemble de ces positions, prises pour permettre de mener à bien toutes les activités de fin de journée et de fin d'année , et d'achever toutes les procédures de sauvegarde des données avant minuit,

l'AFECEI recommande à l'ensemble de ses adhérents :

- de fermer les guichets bancaires au public le 31 décembre 1999 et, plus généralement, d'éviter de conclure des opérations se dénouant le 31 décembre 1999, de façon à exécuter, en toute sécurité, les traitements internes liés aux opérations normales et à assurer les sauvegardes indispensables avant le basculement à l'an 2000 ;

- de traiter, sur un plan comptable, la journée du 31 décembre 1999 comme sont traitées habituellement les journées du samedi.

* * *

ANNEXE 6 : Sites internet

Sites Internet

Adresses	Type
www.software.ibm.com/year2000	Technique en français
www.bull.com/year2000	Technique
www.cigref2000.com	Base de compatibilité et aspects juridiques
www.iee.org.uk/2000risk	Informatique enfouie
www.themis-rd.fr	Général
www.clusif.asso.fr	Général
www.cxp.fr	Fiches techniques
www.ccf2000.fr	Général
www.an2000.gouv.fr	Centre national d'informations An 2000
www.premier-ministre.gouv.fr/ DOSSIERS/AN2000/SOMMAIRE.HTM	Site du Premier ministre
europa.eu.int/comm/dg24	Commission européenne
www.gartner.com	Gartner Group
www.computerworld.com	Général
www.metagroup.com	Général
www.y2k.gov/text/contingency.html	Plan de continuité aux USA
www.whistlepig.com/wpinternet/y2kfaq.htm	FAQ plan de continuité
www.whistlepig.com/wpinternet/y2klinks.htm	Liste de liens An 2000
www.cnet.com/Content/Reports/Special/Y2K/Main/	Général
www.zdnet.com/enterprise/zdy2k	Général
www.infoliant.com	Payant, observatoire sur l'état de conformité An 2000 de plusieurs milliers de produits
www.pcprofile.com	Général
www.pcy2000.com	Regroupe plusieurs constructeurs de PC

Pour une liste plus complète, on pourra se reporter aux rapports *Opération An 2000, 1re et 2e parties* du Cigref ou au site web www.cigref2000.com.