COMMISSION BANCAIRE

LIVRE BLANC

SUR LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

DANS LES ÉTABLISSEMENTS DE CRÉDIT

Mars 1996

REMERCIEMENTS

Le Secrétariat général de la Commission bancaire remercie le Forum des Compétences et ses membres[1], représentants des principaux établissements de crédit de la Place, pour l'aide précieuse qu'ils ont bien voulu lui apporter dans l'approfondissement de sa réflexion sur la sécurité de l'information dans le monde bancaire -et qui trouve ici sa traduction dans ce "Livre blanc"-, ainsi que tous les établissements de crédit qui ont répondu au questionnaire sur le "risque informatique" lancé par le S.G.C.B. en 1992[2].

1 La liste des participants figure en annexe XII.

2 Les analyses et résultats ont fait l'objet d'un "Livre bleu" envoyé uniquement aux participants choisis pour répondre à ce questionnaire. Ils ont fait, toutefois, l'objet de présentations résumées dans plusieurs enceintes et de publications -notamment dans la revue BANQUE n° 547 d'avril 1994-.

PRÉAMBULE

En 1991, le Secrétariat général de la Commission bancaire a mené une réflexion sur la prise en compte du "risque systémique dans la surveillance prudentielle des établissements de crédit" qui comportait quatre volets et dont les principaux résultats ont été publiés dans le Rapport annuel de la Commission bancaire.

L'un de ces volets avait trait aux risques informatiques dans le monde bancaire. A cette occasion, une enquête comportant un questionnaire sur 4 thèmes (détermination du "risque maximal tolérable", évaluation du niveau de sécurité, poids des contraintes budgétaires et couverture des risques par les assurances, appréciation de la qualité de l'informatique de l'établissement) a été faite en 1992 auprès d'un échantillon représentatif d'établissements de crédit.

Les résultats complets ont été rétrocédés aux banques interrogées et ont fait l'objet de synthèses dans des publications ou lors de communications à destination de la Profession bancaire.

Il a paru utile de poursuivre ce travail par la publication d'un "Livre blanc sur la sécurité des systèmes d'information dans les établissements de crédit" à destination de leurs dirigeants et de leurs spécialistes. La préparation de cet ouvrage a reçu le soutien technique des principaux établissements de la Place au travers du Forum des Compétences[3].

La Commission bancaire considère que la sûreté des systèmes d'information fait partie intégrante de la sécurité des établissements de crédit dont elle a la responsabilité. Ces derniers ont un devoir de sécurité vis-à-vis de leurs clients, d'eux-mêmes et de l'ensemble du système bancaire.

Toutefois, afin de ne pas alourdir le poids des textes réglementaires en précisant, à cet égard, le contenu des règlements du Comité de la Réglementation bancaire n° 90-08 -sur le contrôle interne- et 91-04[4] -sur l'organisation de l'information comptable-, la Commission bancaire a préféré procéder à l'écriture d'un Livre blanc à visée pédagogique sous forme de conseils, de recommandations et d'exposé des meilleures pratiques.

Parallèlement à ce qui, dans le monde anglo-saxon, est connu sous le nom de "best practice paper", un effort de sensibilisation des Directions générales a été entrepris grâce à l'envoi par le Secrétaire général de la Commission bancaire d'une lettre portant sur ces thèmes et invitant à la réflexion tous les dirigeants bancaires[5]. Elle indiquait que la Commission bancaire était très attachée à ce que le niveau de sécurité des systèmes informatiques fut périodiquement mesuré et que, le cas échéant, les actions nécessaires à son amélioration fussent entreprises. Elle estimait, également, que la définition des objectifs généraux de sécurité de l'établissement et leur contrôle, *in fine*, incombaient à la Direction générale de chaque établissement. Elle formulait, enfin, quelques questions fondamentales auxquelles il paraissait souhaitable d'apporter une réponse et annonçait la publication de recommandations sous forme d'un Livre blanc.

Celui-ci aborde, dans une première partie, les risques liés aux systèmes d'information des établissements de crédit et les conséquences qu'un dysfonctionnement éventuel pourrait engendrer avant d'aborder, dans une deuxième partie, les outils de mesure du risque. Une

3 Auquel la Banque de France (et donc le Secrétariat général de la Commission bancaire -SGCB-) appartient également.

4 Rappelés en annexe II.

5 Cette lettre figure en annexe I.

troisième partie traite des parades possibles. Enfin, une quatrième partie formule des recommandations.

Volontairement synthétique, ce texte renvoie à des annexes où sont analysés les principaux risques sous forme de fiches classées, par commodité, par ordre alphabétique et structurées de façon identique entre "définition", "risques", "parades" (ou "mesures à prendre") et "critères de qualité" ou recommandations à observer pour atteindre un bon niveau de sécurité. Le style de ces fiches est volontairement cursif pour ne pas alourdir le Livre blanc.

D'autres annexes donnent notamment :

- un mini-questionnaire et une table de comparaison permettant à la banque, respectivement d'évaluer directement son niveau de sécurité et de se situer par rapport à ses confrères,

- un récapitulatif des risques, des facteurs de sécurité et des méthodes d'analyse du risque,

- un exemple de prise en compte de la sécurité dans les applications,

- un exemple de charte de sécurité,

- des renseignements pratiques.

ET POUR COMMENCER
(un mini questionnaire destiné aux responsables)

Tout dirigeant d'établissement, conscient des problèmes posés par la sécurité de son système d'information, devrait être en mesure de répondre précisément aux cinq questions suivantes :

❶ Avez-vous défini et formalisé par écrit les objectifs de sécurité informatique pour votre établissement ? Les avez-vous communiqués à vos collaborateurs ?

❷ Avez-vous attribué à un collaborateur direct la fonction de responsable de la sécurité du système d'information (RSSI) de votre établissement ?

❸ Avez-vous déterminé vos vulnérabilités informatiques et évalué les pertes financières (directes ou indirectes) qu'elles pourraient occasionner ?

❹ Connaissez-vous votre "risque maximal tolérable" (RMT), calculé comme une proportion de vos fonds propres que vous "acceptez de perdre" à la suite d'un sinistre touchant votre système d'information ? Autrement dit : quelle est la limite maximale de perte que vous avez fixée pour ne pas remettre en cause la pérennité de votre établissement ?

❺ En cas d'indisponibilité durable de votre système informatique, par exemple aujourd'hui, savez-vous dans quel délai vos services pourraient reprendre une activité normale ?

Si vous ne savez pas actuellement répondre à l'une de ces questions, il vous est suggéré de vous faire transmettre cette information par votre RSSI (ou par le responsable sécurité de votre établissement) et d'en faire une analyse critique. Pour vos collaborateurs, le présent ouvrage peut servir de guide sur les actions à entreprendre et les moyens à mettre en œuvre pour y parvenir. Mais la lecture de ce document peut rester fructueuse pour tous les RSSI car il est le fruit d'une mise en commun de l'expérience de plusieurs de leurs collègues.

N.B. : Une lettre du Secrétaire général de la Commission bancaire a été envoyée à tous les Présidents des établissements de crédit pour attirer leur attention sur les risques que présentent les systèmes d'information ; elle contient ces cinq questions (cf. ANNEXE I).

I - CONSTATS

Plus que pour les autres industries, la menace informatique constitue un danger réel pour les établissements de crédit.

Or, les banques ont un devoir de sécurité vis-à-vis d'elles-mêmes, de leurs clients et du système bancaire.

Les enquêtes réalisées, notamment par le S.G.C.B., indiquent que le niveau de sécurité des systèmes informatiques des établissements de crédit est encore perfectible.

1. Une menace spécifique pour les banques

L'informatique joue un rôle stratégique dans les banques, en raison des répercussions pour l'établissement dans lequel une difficulté apparaîtrait, mais aussi pour ses clients si les problèmes rencontrés sont suffisamment importants pour que des données disparaissent ou, plus grave, que les règlements de toute nature et notamment le remboursement des dépôts soient compromis.

Les risques induits par les défaillances informatiques sont plus élevés dans les établissements de crédit que pour d'autres secteurs de l'économie parce qu'ils peuvent également entraîner des conséquences fâcheuses pour les autres établissements qui sont en relation avec lui, et même, à la limite, avoir des répercussions pour la Place et pour l'économie nationale si l'incident était de nature à provoquer un "risque systémique".

Pour les établissements de crédit, l'informatique est devenue un "outil de production" principal et "incontournable" : les valeurs monétaires, dématérialisées, sont contenues, stockées, transportées, valorisées grâce à elle.

L'impact des problèmes que peut rencontrer une banque, lorsque la sécurité de son système d'information n'est plus assurée, est important et rapide. Les mouvements financiers ayant été multipliés et complexifiés par l'usage des outils informatiques et télématiques, l'effet de masse et de technicité des opérations empêche, comme par le passé, de reconstituer facilement celles-ci à partir de bordereaux papiers ou de "preuves physiques".

De plus, l'usage de plus en plus intense des systèmes informatiques augmente les dangers d'une divulgation d'informations confidentielles : non seulement on peut prélever, plus facilement et sous une forme pouvant être traitée par un autre ordinateur, une quantité beaucoup plus importante de données, mais un accès non autorisé peut se produire sans laisser de trace apparente et les risques encourus demeurer ainsi cachés pendant un certain temps, ce qui accroît leur magnitude.

> Si une entreprise industrielle perd son informatique, il lui restera, en stock, sa production, qu'elle pourra toujours vendre en attendant de rebâtir un nouveau système informatique : celui-ci étant moins intégré au mode de production, une reprise plus ou moins totale de l'activité de l'entreprise pourra intervenir.

> En revanche, la banque possède la particularité d'avoir l'argent en "input" et en "output". Si elle perd toute son informatique, comme sa matière première est "l'argent x information[6]", -ce qui est immatériel-, elle aura perdu et son outil de production principal, et sa mémoire. Ce sont l'information, la valorisation et le transfert d'une forme financière à une autre qui construisent sa valeur ajoutée.

En outre, une banque travaille avec l'argent des autres agents économiques et financiers. Ses difficultés, nécessairement connues si elles sont graves, risquent très vite d'amener les autres établissements de crédit à lui couper ses lignes de refinancement, ou ses clients à retirer ou à ne pas renouveler leurs dépôts, ce qui entraînerait une crise de liquidité rapide.

Comme les masses financières en jeu peuvent être très importantes et que les systèmes bancaires sont très interdépendants, une difficulté technique rencontrée par une banque risque de se répercuter rapidement sur ses contreparties, confrères ou clientèle, voire, dans les cas extrêmes, sur l'ensemble du système financier.

Assurer la sécurité des systèmes d'information, de traitement, de conservation et de transferts des flux financiers est donc impératif dans les économies interdépendantes où les "chocs" sont susceptibles d'avoir très rapidement des conséquences importantes et de constituer l'un des vecteurs possibles de transmission du risque, pouvant, à la limite, créer un risque systémique.

De ce fait, la sécurité de l'information[7] est devenue une exigence essentielle.

2. Une menace financière réelle

Quelles que soient les causes (pannes ou accidents, erreurs ou malveillances), l'informatique peut jouer, si la défaillance est importante, soit un rôle de déclenchement d'une crise, soit celui de propagateur. Des cas comme celui de l'impact des "trading programs" dans la crise boursière américaine puis mondiale de 1987 ont fait l'objet de trop nombreuses analyses pour qu'il soit nécessaire d'y revenir ici, mais ils indiquent, clairement, que les conséquences ne sont pas théoriques mais très concrètes.

Les risques encourus sont ceux :

- de non-transfert, entraînant un "cash liquidity risk" où la banque, pour des raisons diverses liées à son informatique, n'est plus capable, à tout moment, de remplir à court terme ses obligations vis-à-vis de ses clients ou de ses confrères ;

- de pertes d'informations, dues à la destruction totale ou partielle de ses fichiers stratégiques ou de sa "mémoire", ou la divulgation d'informations confidentielles (fichiers clients, positions stratégiques, ...) ;

- enfin, de fraudes, conduisant à des pertes de valeurs (coûts économiques des détournements).

A ces coûts directs, outre le remplacement des matériels et logiciels perdus et les pertes financières afférentes, viennent, en général, s'ajouter des coûts indirects (frais supplémentaires, temps "perdu" de réinstallation du système d'information et de reconstitution des données, pertes d'exploitation ou de patrimoine, responsabilité civile éventuelle, risque de réputation...).

---

6 L'informatique n'accompagne plus un processus de production qui pourrait éventuellement, en cas de panne, avoir sans elle un mode de fonctionnement dégradé : elle constitue à elle seule ce processus.

7 La notion "d'information sécurity" ou INFOSEC recouvre les deux domaines complémentaires que constituent la sécurité des systèmes de traitement de l'information ("computer security" ou COMPUSEC) d'une part, et la sécurité des systèmes de transmission de l'information ("communication security" ou COMSEC), d'autre part.

Le CLUSIF[8] et l'APSAD[9] évaluent, hors monétique mais pour tous les secteurs de l'économie à 10,8 milliards de francs (soit une hausse de 6 % en un an), l'ensemble des pertes dues à des sinistres impliquant l'informatique en 1993 : 58 % imputables à la malveillance, 25 % à des accidents et 17 % à des erreurs, ce que retrace le tableau suivant :

Estimation des pertes dues à des sinistres informatiques en France (1) en 1993 (2) en millions de francs

Conséquences / Types de risques	Directes		Indirectes				
	C1 Matériel	C2 Non matériel	C3 Frais supplémentaires et pertes d'exploitation	C4 Pertes de patrimoine	C5 Responsabilité civile	C6 Divers	TOTAL
Accidents							
A1 - Physiques (incendie, explosion, dégât des eaux, pollution...)	370	20	900		100		1 390
A2 - Pannes		70	830		60		960
A3 - Force majeure (événements naturels)	50		90				140
A4 - Perte de services essentiels (télécoms, électricité, eau...)		15	200		20		235
A5 - Autres							
Erreurs							
E1 - Erreurs d'utilisation	10	60	570	50	210		900
E2 - Erreurs de conception et de réalisation	10	10	750	60	140		970
Malveillance							
M1 - Vol (physique)	120	20					140
M2 - Fraude (non physique)			50	1 490	90		1 630
M3 - Sabotage (physique)	0						0
M4 - Attaque logique (non physique)		575	350	120	80		1 125
M5 - Divulgation		10		720	90		820
M6 - Autres			120 (3)			2 380 (4)	2 500
TOTAL	**560**	**780**	**3 860**	**2 440**	**790**	**2 380**	**10 810**

(1) Ensemble des systèmes informatiques, bureautiques, télécommunications, matériel informatique et télécommunication annexe (serveurs, modems, processeurs, etc. hors téléphone ou fax), périphériques divers et spécialisés (incluant la robotique mais hors monétique et cartes à puces, calculettes, etc.).
(2) Hors gouvernemental et administrations. Ces estimations qui correspondent à des ordres de grandeur établis à partir de la fraction des cas connus et des tendances sont plus ou moins précises selon les lignes et colonnes ; globalement la précision est elle-même estimée à ± 30 %.
(3) Risques humains (départs de personnel, pénurie de personnel, grève, etc.).
(4) Copie illicite de progiciels : 1 250
Utilisation non autorisée de ressources informatiques : 1 130 (0,5 % budget informatique de la nation).

Source CLUSIF (février 1994)

Selon diverses sources, bien qu'il n'existe pas de statistiques officielles dans ce domaine où la discrétion est de rigueur, les pertes des établissements de crédit se chiffreraient, en France, entre 1 et 3,5 milliards de francs. L'enquête menée en 91/92 par le S.G.C.B., a révélé que 6 % des établissements interrogés avaient connu des incidents informatiques ayant entraîné des préjudices au cours des trois années précédentes.

8 Club de la Sécurité Informatique Français.

9 Assemblée plénière des sociétés d'assurance dommage.

3. Quelques exemples des menaces dues aux systèmes d'information

Les quelques exemples réels suivants, empruntés à l'APSAD, montrent, tout à la fois, le caractère concret et la nature multiforme des menaces pesant sur les systèmes d'information.

● Modification de la chaîne "immobilisations" entraînant une surévaluation des amortissements de matériels de traitement de texte, rachetés ensuite à une valeur symbolique par le gestionnaire du parc, puis revendus avec profit. La fraude a duré deux ans pour un montant de 1 MF.

● Modification du programme de "participation du personnel au profit de l'entreprise" en minorant les provisions déductibles et en reversant la différence sur les comptes de trois cadres. La fraude a été découverte plusieurs mois après la clôture du bilan, pour un montant de 1,5 MF.

● Copie d'un fichier d'aide à la décision de crédit pour industriels et commerçants dans une banque. Le fraudeur a recensé les sociétés en difficulté et les a menacées de divulguer l'information à leurs principaux fournisseurs et clients, contre des rançons s'élevant au total à 2,5 MF.

● A la suite d'un arrêt programmé pour changement de matériel, les agences d'un établissement devaient se connecter sur un centre de secours pendant trois jours. Les programmes correspondaient à un mode légèrement dégradé par suite de différences de configuration. Par souci d'économie, on avait décidé de traiter les opérations sur valeurs mobilières de placement en batch, en utilisant d'anciens programmes. Il s'est avéré, lors de l'exploitation réelle, certaines incompatibilités conduisant à des endommagements logiques de fichiers. La perte totale en frais de restauration et en pertes d'intérêts a été évaluée à 3,2 MF.

● Une bombe logique dans les tables des taux de change d'une banque, posée par un groupe interne à l'entreprise, a été activée deux mois après sa pose, estime-t-on, à la suite d'un conflit de personnes. Il a fallu trois jours pour recharger et "patcher" les sauvegardes (qui n'étaient -volontairement- pas à jour). La perte totale est évaluée à 4 MF.

● Un certain nombre d'erreurs de conception de la translation d'un ancien système vers un nouveau, notamment au niveau du mode d'accès conversationnel à une base de données, se sont traduites par un retard (0,4 MF), des impossibilités fonctionnelles qu'il a fallu reprendre (0,3 MF), des fonctions très alourdies impliquant plus de personnel pendant six mois (0,7 MF), ainsi que des temps de réponse dégradés pendant deux ans dont le coût est estimé à 4 MF.

● Faux incidents d'exploitation ayant entraîné la destruction de la principale base de données. Le rechargement a pris huit heures. La saisie complémentaire qui a été nécessaire à cause d'un écrasement volontaire d'une partie du journal "after" a retardé une partie des opérations pendant deux jours. La perte totale est estimée à 4,2 MF.

● Une banque qui proposait à ses clients P.M.E. un logiciel d'optimisation de trésorerie sur micro ou sur vidéotex, leur offrait dans un premier temps la possibilité de l'essayer dans les agences sur des matériels en libre-service. Un détournement a été réalisé par un tiers par suite de l'oubli d'effacer certains des fichiers installés sur un des micros d'un client. La perte de notoriété et l'atteinte en responsabilité civile sont estimées à au moins 5 MF.

● Menace de chantage au virus. Les responsables n'ont pas pris la menace au sérieux mais ont entrepris de vérifier le système. Par mesure de sécurité, ils ont changé les mots de passe. C'est à ce moment que les pirates, à l'écoute sur le réseau, ont détecté les mots de passe système et en

ont profité pour implanter un virus actif. Celui-ci, déclenché ultérieurement, à la suite du non-paiement, a coûté environ 7 MF à l'entreprise.

● Un cadre ayant autrefois travaillé au service informatique entre sur écran une série d'écritures dont le compte d'origine est "Réserves" et le compte d'aboutissement est un numéro de compte personnel dans une banque étrangère. Les opérations sur le compte "Réserves" sont rejetées en anomalies dans un fichier d'attente afin d'être ultérieurement recyclées. Le fraudeur utilise alors une chaîne de recyclage "batch", normalement employée en mode dégradé dans le cadre du plan de secours. Cette chaîne, ancienne, n'est pas à jour et les écritures passent. Ce n'est que le lendemain, lors du contrôle quotidien que l'anomalie est identifiée. Les mouvements de fonds ont déjà été réalisés pour 7,5 MF.

● Un utilitaire, qui se lance comme une commande TSO (Time-Sharing Option : mode conversationnel sur MVS), possède certaines commandes particulières permettant l'inspection et la modification de certains champs. Ces commandes sont protégées par un mot de passe lisible sur le "load module". Un ingénieur système utilisant alors la simple commande List s'est donné toutes les autorisations nécessaires pour réaliser un détournement de 8,5 MF.

● Une banque proposait à ses clients P.M.E. la possibilité de traiter leurs bandes virements sur son centre d'informatique. Une bande a été détournée et les informations publiées (salaires des dirigeants en pleine période électorale alors que certains étaient candidats). La perte de notoriété et l'atteinte en responsabilité civile sont estimées au moins à 10 MF.

● Reprise de provisions pour dépréciation de titres sur des courtiers fictifs : passation illicite des écritures associée à une modification de la table des valeurs qui sert de référence de contrôle aux écritures sur provisions. La fraude a été réalisée pour un montant de 11 MF.

● Passage illicite et temporaire de fausses écritures de caution qui ont généré des bons de cautions (signés par le responsable du service après vérification comptable). Ces bons ont permis de réaliser très rapidement des emprunts avec lesquels le fraudeur a disparu. La perte est estimée à 14 MF.

● Suite à un faux incident d'exploitation, rechargement à partir d'une ancienne version du système d'exploitation de l'ordinateur établissant le lien avec la chambre de compensation au siège social d'une grande banque américaine. Le fonctionnement normal n'est rétabli que très tard dans la nuit et le déficit comptable incompensable enregistré en fin de journée est énorme ce jour-là. Cette situation, théoriquement illicite, est rétablie le lendemain par un prêt consenti par la banque centrale, dont les intérêts se montent à 14 MF.

● Intrusion d'un pirate dans le système par le service vidéotex/client. Sa complicité avec un chef de projet informatique lui a permis de violer la table des codes d'accès et de simuler une ouverture de crédit international pour trois virements : 4,5 MF, 8 MF et 9 MF.

● Transactions illicites introduites à partir d'un micro-ordinateur branché sur un réseau de virements électroniques : l'opérateur était un tiers en collusion avec l'informaticien chargé du réseau et connaissant les moyens de déchiffrer facilement les mots de passe et les instructions codées. Il y a eu modification des montants et des comptes de destination. Le montant de la fraude serait de l'ordre de 25 MF.

Sur ces seuls exemples, le total des pertes s'élève à 138,2 MF avec un préjudice moyen de 8,1 MF.

II - LES OUTILS DE MESURE DU RISQUE

Le risque pesant sur les systèmes d'information des établissements de crédit est donc une réalité. Encore faut-il le mesurer.

Avant de formaliser une méthode de mesure du risque, il sera donné un exemple concret, celui de l'enquête menée par le Secrétariat général de la Commission bancaire (SGCB).

1. Un exemple : l'enquête menée par le SGCB

Cette enquête, dont l'analyse suit, confirmait que si la sécurité moyenne des établissements de crédit est relativement satisfaisante et meilleure que celle d'autres branches de l'industrie, - puisque la note moyenne s'élève à environ 13 sur 20 sur l'ensemble des questionnaires- cette situation pouvait et devait être améliorée. Elle justifiait que l'effort de sensibilisation déjà commencé soit poursuivi.

a. Une enquête pour servir de base de référence

En 1992, le Secrétariat général de la Commission bancaire a procédé à une enquête sur le risque informatique auprès d'un échantillon représentatif d'établissements de crédit. Les résultats complets ont été rétrocédés aux banques interrogées. Ils ont également été à nouveau partiellement présentés dans des publications ou lors de communications. Ces résultats comprennent des tableaux pouvant servir de "base de référence" aux établissements souhaitant procéder à une évaluation comparative de leur informatique (cf. annexe III).

L'enquête s'appuyait sur un questionnaire composé de quatre parties : évaluation du risque maximal tolérable, mesure de la sécurité technique, détermination des coûts et du niveau de couverture par les assurances, analyse de la qualité de l'informatique. Ces quatre parties couvrent un champ plus vaste que celui retenu habituellement dans une analyse traditionnelle du risque informatique car seule une analyse globale du risque est pertinente. L'informatique d'une banque peut être relativement sûre mais trop coûteuse, amenuisant la marge de manœuvre dont elle dispose et lui faisant courir un risque économique parfois trop lourd. Mais il ne suffit pas qu'une informatique soit techniquement sûre et peu coûteuse ; elle doit, aussi, être efficace et répondre aux attentes de ses utilisateurs et "clients", faute de quoi elle constituerait, encore, un risque économique.

b. Un impératif : sensibiliser au plus haut niveau

L'appréhension par la direction générale d'un établissement du "risque maximal tolérable", RMT[10], doit lui permettre de répondre à la question : "Quel est le montant maximal du risque (conséquences financières d'un sinistre informatique) que l'entreprise peut supporter sans mettre en cause la continuité de ses opérations ?".

10 On trouvera également page 25 et surtout en ANNEXE III, partie 3.1., des considérations plus précises sur le RMT.

La nécessaire analyse du risque maximal tolérable

En première analyse, le RMT est la valeur limite, en millions de francs, imposée par la direction générale, de la part α des fonds propres nets désirés (car la banque peut avoir un objectif supérieur au minimum de 8 % en termes de ratio de solvabilité) et de celle, β, de la capacité bénéficiaire prévisionnelle nette de l'année que la banque "accepte" de perdre (part des bénéfices pouvant absorber un sinistre), plus, éventuellement, le montant des garanties (ne sont retenues que celles dont on est sûr, ce qui explique que le facteur γ est inférieur ou égal à 1) accordées par les assurances en cas de sinistres informatiques.

$RMT = \alpha$ FP + β Bénéf. + γ Garanties avec $\alpha, \beta, \gamma \leq 1$

L'analyse peut être compliquée par le fait que l'établissement peut ou non, souhaite ou non, lever des fonds propres auprès de ses actionnaires ou du marché.

Volontairement très ouverte, la question, qui ne permettait pas aux banques de répondre facilement, avait pour objet de vérifier que chaque direction générale avait déjà étudié ce problème et pouvait y apporter une réponse.

Les résultats recueillis sont contrastés. Avec toute la prudence nécessaire, l'impression qui semble se dégager est qu'un effort de sensibilisation au plus haut niveau est indispensable pour conduire à une prise de conscience de la nécessité d'une analyse globale et d'une action cohérente en matière de sécurité informatique. C'est ce qui a justifié la rédaction de ce livre blanc.

La direction générale d'un établissement ne peut percevoir la nécessité d'un investissement à long terme dans ce domaine que si les enjeux lui sont présentés dans un langage compréhensible et si elle peut donc, correctement et préalablement, faire face à ses responsabilités. Le discours doit être clair, débarrassé de tous les "jargons" employés par les informaticiens (ils ne sont pas les seuls...). C'est uniquement après cette prise de conscience qu'une analyse basée sur un arbitrage entre le coût du risque et le coût de la sécurité à mettre en œuvre pour contrer ce risque est, non seulement, possible mais aussi nécessaire.

La réponse à cette question, enfin, est indispensable pour classer les projets visant à améliorer la sécurité. Encore faut-il cerner les points faibles. C'est l'objet du paragraphe suivant.

c. Soixante-cinq questions pour cerner la sécurité

Les techniques et "logiciels" permettant de "mesurer" le niveau de sécurité sont disponibles sur le marché : en particulier la méthode Marion (Méthode d'analyse informatique en organisation par niveaux) du Clusif, qui est publique, et la méthode Melisa.

L'enquête, réalisée par le Secrétariat général de la Commission bancaire, s'appuyait sur un mini-questionnaire reprenant les questions de poids important parmi les six cents figurant dans les recueils Marion et comportant, en outre, cinq questions supplémentaires d'ordre général hors recueil, soit un total de soixante-cinq.

Le tableau général des indicateurs révélés par l'enquête et la rosace Marion qui lui est associée peuvent servir aux établissements pour situer leur niveau de sécurité (cf. tableau 1). Ceux-ci peuvent par ailleurs, s'ils l'estiment utile, faire appel aux groupes de réflexion (Clusif, Forum des compétences...) ou aux sociétés de services connues pour leur spécialisation en matière de sécurité.

Les notes Marion vont de 0 à 4[11].

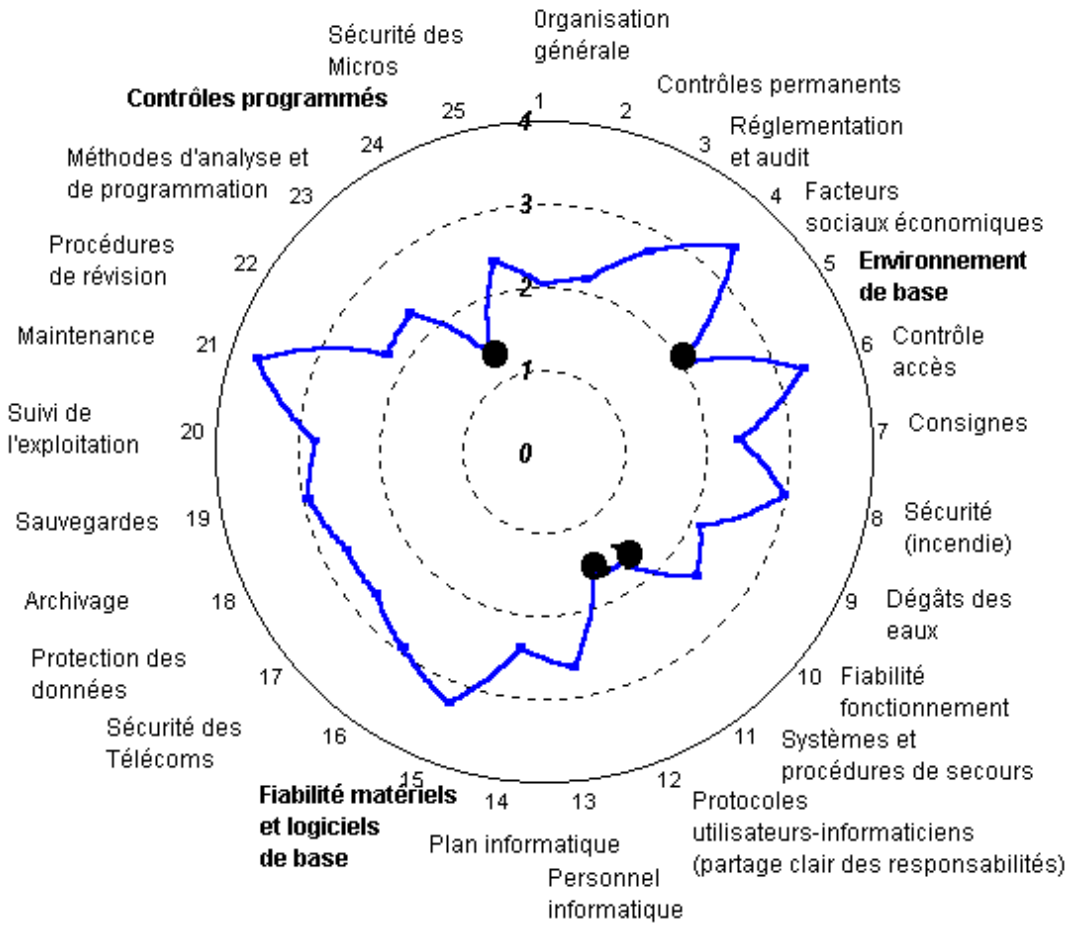
Un résultat inférieur à 2 est "mauvais" et doit être rapidement étudié et amélioré ; l'objectif à atteindre est au minimum 3.

Le graphique polaire de la "rosace Marion" montre clairement les points faibles qui ont pu être décelés lors de l'enquête : contrôles programmés, protocoles utilisateurs/informaticiens, systèmes et procédures de secours, environnement de base, ainsi que les points forts : maintenance, contrôle des accès...

11 Avec l'échelle suivante : 0 = sans objet, 1 = mauvais, 2 = médiocre, 3 = assez bon, 4 = bon, avec les conventions suivantes :
- ne répondre bon (cote 4) que si toutes les conditions posées dans la question sont totalement satisfaites en même temps ;
- Si, par hasard, la question est sans objet, pour ne pas introduire de biais, il convient de reprendre la note moyenne donnée dans le tableau de référence (Annexe III).

Tableau 1

Rosace Marion et valeurs révélées par l'enquête du Secrétariat général de la Commission bancaire
(1991-1992)



Noms des facteurs		Valeurs trouvées
1	Organisation générale	2,03
2	Contrôles permanents	2,15
3	Réglementation et audit	2,75
4	Facteurs socio-économiques	3,39
5	**Environnement de base**	**1,97**(1)
6	Contrôle des accès	3,32
7	Consignes	2,38
8	Sécurité incendie	2,96
9	Dégâts des eaux	2,10
10	Amélioration fiabilité fonctionnement	2,39

Noms des facteurs		Valeurs trouvées
11	**Systèmes et procédures de secours**	**1,65**(1)
12	**Protocoles utilisateurs/ informaticiens**	**1,61**(1)
13	Personnel informatique	2,62
14	Plan informatique	2,37
15	Fiabilité des matériels et logiciels de base	3,24
16	Sécurité des télécommunications	2,92
17	Protection des données	2,67

Noms des facteurs		Valeurs trouvées
18	Archivage	2,67
19	Sauvegardes	2,92
20	Suivi de l'exploitation	2,79
21	Maintenance	3,67
22	Procédures de révision	2,26
23	Méthodes d'analyse programmation	2,34
24	**Contrôles programmés**	**1,35** (1)
25	Micro-informatique (*)	2,38
	Moyenne	**2,52**

(1) Zone de danger.
(*) Les deux questions regroupées dans ce facteur 25 n'appartiennent pas au catalogue Marion standard. Pour tous les autres facteurs, les 58 questions sont celles de poids important repondérées en fonction du poids total de chaque facteur Marion.
Ainsi, pour le facteur (code Marion 101) relatif à l'organisation générale, la pondération est la suivante : [(Q1 X6) + (Q2 X 6) + (Q3 X 5) + (Q4 X 6) + (Q5 X 4) + (Q6 X 2) + (Q7 X 2)] / 31, où Q1 à 7 sont les sept questions de poids le plus important retenues dans l'ensemble des questions Marion de code 101 (le dossier Marion donne le détail des facteurs) [voir annexe III].

En tenant compte de ce que, depuis deux ans, le niveau de sécurité moyen a dû vraisemblablement augmenter et se situer autour de 2,6 - 2,7, cette base de référence permet à un établissement de crédit de se comparer à l'échantillon.

d. Évaluer les contraintes budgétaires

La troisième partie du questionnaire avait trait à l'appréciation des contraintes budgétaires et au niveau de couverture par les assurances des risques informatiques.

• Les tableaux 2 et 3 donnent la structure des budgets informatiques et quelques ratios significatifs observés en 1990 (les chiffres en francs courants sont donc plus élevés aujourd'hui).

Tableau 2
Budgets informatiques
(pourcentage des différents postes)

Frais de personnel	24,9 %
Matériels	39,2 %
Logiciels	9,4 %
Locaux	3,6 %
Télécommunications	7,4 %
Micro-informatique	1,9 %
Travaux à façon	11,0 %
Divers	2,6 %

N.B. : il faut être très prudent sur l'utilisation de ces chiffres qui ne retracent qu'une moyenne.

Tableau 3
Ratios des frais informatiques

Coûts informatiques (en kF)

par agent	71
par informaticien	1 336

Frais informatiques (en %)

sur PNB	11,5 (*)
sur frais généraux	15,4

(*) L'enquête a été menée sur cinq catégories de banques, dont des banques filiales de grands groupes et des banques étrangères dont l'informatique relève souvent en partie de la maison mère et qui pèsent sur cette moyenne ; les chiffres domestiques les plus fréquents se situent entre 12 et 14 %. Les chiffres sont naturellement pondérés par l'importance des budgets ; donc par la taille des établissements.

• Concernant les assurances, le questionnaire, tel qu'il était conçu, ne permettait pas de savoir avec certitude si les risques informatiques étaient ou non correctement couverts par les assurances : le domaine est complexe et l'absence d'homogénéité des produits proposés aux banques rend les comparaisons difficiles. D'autant que les assurances ont une propension naturelle à fixer des limites aux couvertures et à imposer des seuils de franchise.

Bien qu'il faille, donc, rester prudent, il n'est toutefois pas certain que les assurances contractées constituent toujours une garantie suffisante contre les risques informatiques, ce qui tient sans doute au fait que les personnes chargées des contrats d'assurance dans les banques font peu ou pas appel aux spécialistes informatiques, la couverture des risques informatiques n'étant qu'un sous-ensemble du domaine plus vaste de l'assurance (immobilier, personnel...)[12].

Par ailleurs, l'absence de recours à des polices d'assurance sur le modèle anglo-saxon du "Tout, sauf..." permet plus difficilement d'acquérir la certitude qu'en cas d'incident la couverture des risques informatiques est effective.

e. Apprécier la satisfaction des utilisateurs et le niveau d'efficacité/qualité de l'informatique

Dans la quatrième partie du questionnaire, -auto-appréciation par la banque et ses utilisateurs de l'efficacité et de la qualité de son informatique-, les questions concernaient plusieurs domaines : positionnement de l'informatique et du plan informatique, taux d'informatisation, niveau d'intégration et de centralisation, niveau de standardisation des systèmes informatiques, types de solutions informatiques retenues, cibles stratégiques et choix technologiques, recours à l'assistance extérieure, préoccupations des dirigeants, performances de l'informatique, appréciations portées par les utilisateurs sur leur système d'information et sur les hommes qui le développent et le maintiennent. Le sentiment qui se dégage des réponses obtenues est, en moyenne, assez bon.

12 Voir recommandations données dans la "fiche-conseil" n° 6 (Assurances) en ANNEXE IV.

Le besoin d'une meilleure prise en compte de la sécurité dans les applications informatiques et d'un usage plus important des méthodes de planification et de développement peut, toutefois, être noté, facteurs contribuant tous deux à diminuer les risques.

De plus, si les informaticiens professionnels ne placent pas la sécurité au premier rang de leurs préoccupations, leurs dirigeants affirment en revanche que la sécurité de leur système d'information est encore plus primordiale que la satisfaction de la clientèle. C'est un facteur rassurant ; toutefois, si l'intention est avérée, les résultats du premier questionnaire sur le RMT indiquent que les outils techniques de mesure et de fixation des risques devraient être affinés.

Signe d'une certaine satisfaction, les utilisateurs ont, en moyenne, accordé la note de 13,2 sur 20 à leur informatique, avec presque 14 sur 20 à la sécurité.

A noter cependant, pour certains établissements, plusieurs notes très basses sur des secteurs sensibles : fiabilité des informations de pilotage, couverture des besoins...

Le tableau 4 donne les résultats globaux pour l'ensemble des établissements analysés et pour les quatre sous-populations interrogées : les contrôleurs de gestion, l'inspection, les comptables et les commerciaux.

Tableau 4
Notes de satisfaction données par les responsables fonctionnels selon six critères
(Moyenne générale sur 20)

Satisfaction des utilisateurs	13,2
Fiabilité des informations de pilotage	13,3
Couverture des besoins	12,8
Rapport qualité/prix des actions	12,3
Sécurité du système d'information	13,8
Evolutivité du système d'information	12,7

f. Au total, une sécurité informatique globalement assez satisfaisante mais encore perfectible

Globalement, avec une moyenne de 13 sur 20 sur l'ensemble des quatre questionnaires, la situation des établissements de crédit de l'échantillon a pu être jugée assez satisfaisante.

Néanmoins, cette moyenne cache des disparités importantes : si plus des trois-quarts des établissements sondés n'appellent que des remarques de détail, un peu moins du quart présentait une ou plusieurs faiblesses significatives ; l'exercice les aura incités à les combler. Mais ceci indique que, globalement, des efforts restent à faire ; ce qui justifie ce Livre blanc.

Tous les établissements de crédit disposant d'une informatique propre devraient au minimum avoir fait ou réaliser au plus vite ce type d'analyse. Bien que d'un niveau assez "basique", le mini-questionnaire présenté en annexe ne réclame qu'un investissement humain bien moins important que les méthodes plus élaborées du marché. Il fournit, néanmoins, rapidement une vue d'ensemble relativement correcte des points forts et des points faibles et, surtout, offre une base de comparaison entre banques. Il est donc impératif, au minimum, qu'il soit utilisé. Toutefois, il reste indispensable de mener une analyse complète avec l'une des méthodes disponibles sur le marché pour avoir une vision plus fine des forces et faiblesses du système d'information.

2. Une méthode formalisée de mesure du risque : quelques conseils

Il est impossible, dans ce court ouvrage, de traiter de tous les aspects de la sécurité, tant ils sont multiformes.

Toutefois, l'articulation des étapes suivantes doit être connue et observée.

Mesurer les risques, c'est d'abord :

- connaître ces risques,
- pouvoir classer ses informations en fonction des quatre critères ou facteurs de sécurité D.I.C.P. (Disponibilité, Intégrité, Confidentialité, Preuve),
- évaluer son risque maximal tolérable, car lui seul permettra d'effectuer le tri entre ce qui est acceptable et ce qui est intolérable et par conséquent d'induire une démarche volontariste constructive,
- classer ses informations entre "stratégiques" et "non stratégiques" en s'aidant d'une échelle d'évaluation de l'impact des risques.

On en déduira la méthode et l'organisation à adapter pour répondre à ces besoins.

a. Connaître les risques[13]

Le système d'information[14] est soumis, à travers l'environnement sécurisé, à des menaces d'origine :

- naturelle ou accidentelle[15],
- humaine, volontaire ou involontaire.

Il en résulte un état de vulnérabilité qui affecte les composants du système d'information et de son environnement.

Pour parer aux menaces, les responsables de la gestion du système d'information mettent en place des mesures de sécurité qui diminuent la vulnérabilité.

Le risque informatique peut être défini comme la probabilité qu'une menace se concrétise, à la suite d'un sinistre portant atteinte à l'un des composants du système d'information ou de son environnement, avec un impact que l'on mesure, soit quantitativement par le montant des pertes, soit de façon qualitative.

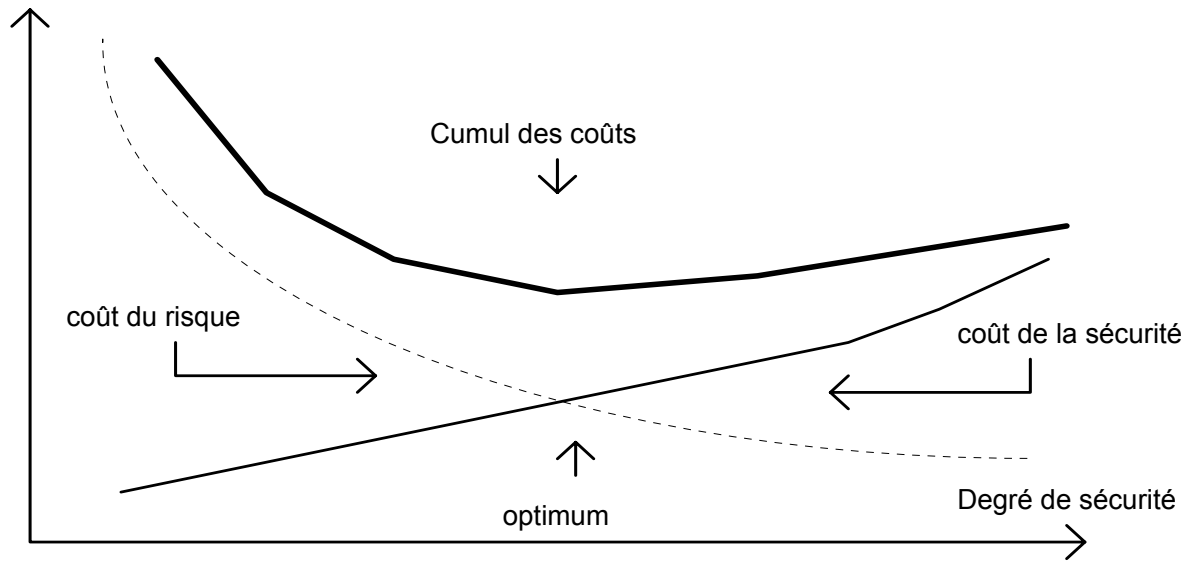
L'objectif de la politique de sécurité du système d'information vise à garantir quatre facteurs de sécurité : la disponibilité, l'intégrité, la confidentialité et la possibilité de contrôle et de preuve. Ces facteurs, qui ont fait l'objet d'une définition du CFONB (voir page 23 "Les facteurs de sécurité"), sont parfois appelés "facteurs DICP".

La gestion de la sécurité du système d'information consiste à choisir les mesures permettant d'abaisser le niveau de risque à un coût acceptable, tout en respectant, au niveau de l'Entreprise, la cohérence des moyens mis en œuvre.

13 On trouvera en ANNEXE V un exemple de méthode d'analyse des risques.

14 Par "système d'information" on entend l'ensemble [organisation (hommes, structures, données), procédures (consignes...) et système technologique].

15 Une variante tient aux dérèglements et aux effets "d'emballement" (cf. théorie du chaos).



La bonne sécurité passe par un optimum entre le coût
du risque et le coût de la sécurité (protection + prévention).

Les mesures de prévention agissent sur la probabilité des atteintes ; les mesures de protection, sur leur impact.

b. Classer ses informations en fonction des quatre facteurs de sécurité

LES FACTEURS DE SÉCURITÉ

La sécurité des systèmes d'information repose sur quatre facteurs définis de la façon suivante par le CFONB :

- "Disponibilité (D) :
  Aptitude des systèmes à remplir une fonction dans des conditions prédéfinies d'horaires, de délais, de performances."

- "Intégrité (I) :
  Propriété qui assure que des informations sont identiques en deux points, dans le temps et dans l'espace."

- "Confidentialité (C) :
  Propriété qui assure la tenue secrète des informations avec accès aux seules entités autorisées."

- "Contrôle et preuve (P) :
  Faculté de vérifier le bon déroulement d'une fonction.
  Non répudiation : impossibilité pour une entité de nier avoir reçu ou émis un message."

Ces définitions recouvrent les exigences suivantes :

Disponibilité (D)
Garantir la continuité du service.
Assurer les objectifs de performances (temps de réponse).
Respecter les dates et heures limites des traitements.

Intégrité (I)
Garantir : l'exhaustivité,
l'exactitude,
la validité
de l'information.
Eviter la modification, par erreur, de l'information.

Confidentialité (C)
Réserver l'accès aux données d'un système par les seuls utilisateurs habilités (authentification), en fonction de la classification des données et du niveau d'habilitation des utilisateurs.
Garantir le secret des données échangées par deux correspondants, sous forme de message ou de fichiers.

Possibilité de contrôle et de preuve (P)
Garantir la possibilité de reconstituer un traitement à tous les niveaux (logique de programmation, déroulement du traitement, forme des résultats) à des fins de contrôle ou de preuve[16].

16 Voir règlements du CRB 90-08 sur le contrôle interne et 91-04 sur la "piste d'audit" (annexe II).

ILLUSTRATION DES FACTEURS DE SÉCURITÉ

	FLUX	TRAITEMENTS	DONNEES
DISPONIBILITÉ	**Garantie de la continuité des échanges d'informations** Disposer, chaque fois que le besoin existe, des possibilités de réception ou de transfert, aussi bien à partir du réseau informatique que sur d'autres supports. (Cf. contrat de service). [voir fiche 27]	**Garantie de la continuité de service des traitements.** Disposer des ressources en matériels et logiciels nécessaires à l'ensemble des services, des agences et à la clientèle extérieure. (Cf. contrat de service).	**Garantie de la disponibilité prévue pour l'accès aux données (délais et horaires).** Disposer de l'accès aux données, chaque fois que le besoin existe, dans les conditions de performances définies au contrat de service, entre l'utilisateur et l'exploitant.
INTÉGRITÉ	**Garantie de fiabilité et d'exhaustivité des échanges d'informations.** Faire en sorte que les données soient reçues comme elles ont été émises et avoir les moyens de le vérifier.	**Assurance de conformité de l'algorithme des traitements automatisés ou non par rapport aux spécifications.** Obtenir des résultats complets et fiables quel que soit le processus.	**Garantie d'exactitude et d'exhaustivité des données vis-à-vis d'erreurs de manipulation ou d'usages non autorisés.** Disposer de données dont l'exactitude, la fraîcheur et l'exhaustivité sont reconnues.
CONFIDENTIALITÉ	**Protection des échanges d'informations dont la divulgation ou l'accès par des tiers non autorisés porterait préjudice.** Protéger au mieux les échanges effectués par l'intermédiaire du réseau ou tout autre mode de transport de l'information. Authentifier les utilisateurs habilités.	**Protection des algorithmes décrivant les règles de gestion et les résultats dont la divulgation à un tiers non autorisé porterait préjudice.** Protéger le savoir-faire et les modalités de fonctionnement.	**Protection des données dont l'accès ou l'usage par des tiers non autorisés porterait préjudice.** Donner l'accès aux seules personnes habilitées par des procédures organisationnelles et informatiques.
POSSIBILITÉ DE CONTRÔLE ET DE PREUVE	**Garantie de ne pouvoir nier avoir émis ou reçu un flux et possibilité de reconstituer le flux.** Pouvoir apporter la preuve de la réception du message (logs, authentifiants, accusés de réception...) et pouvoir relancer le message.	**Garantie de pouvoir à tout moment reconstituer le déroulement d'un traitement et de ne pouvoir nier la réception des résultats.** Avoir la possibilité de vérifier pas à pas le déroulement du traitement et prouver la remise des résultats.	**Garantie de pouvoir à tout moment reconstituer la donnée et de ne pouvoir nier l'accès à la donnée.** Assurer la possibilité de reconstituer une donnée et de retrouver la trace de son utilisation.

c. Évaluer le risque maximal tolérable (RMT)

Tout ne peut pas être fait tout de suite et à n'importe quel prix pour éviter toute forme de risque. Un calcul économique coût/avantage s'impose donc. Mais il doit être fait dans la clarté et les arbitrages doivent être rendus, en connaissance de cause, par la Direction générale.

Pour éviter des dilemmes de type indiqué par l'équation suivante :

Équation 1

"ε" ↙ Probabilité d'apparition du risque (faible ou "epsilon")	x	"∞" ↘ Conséquences financières du risque, une fois réalisé (importantes ou "infinies")	= Risque

(que, tant les mathématiques que l'esprit humain ont du mal à appréhender, 0 x T étant, en général, indéterminé !), il convient d'affiner l'analyse par l'imposition raisonnée d'un "majorant" qui ne peut être que le Risque Maximal Tolérable ou RMT. Celui-ci est défini comme la part des fonds propres que la banque, en fonction de sa stratégie[17], "accepte" de perdre en cas de catastrophe, auquel on peut ajouter la part des résultats opérationnels ("cash-flow") qui pourrait également absorber ce sinistre et les garanties, notamment les remboursements possibles "garantis" par la police d'assurance couvrant ces risques[18].

soit

$$RMT = \alpha\ FP + \beta\ Bénéfice + \gamma\ Garanties$$

où α est la part des fonds propres, par exemple 20 %, fixée comme limite de perte maximale en cas de sinistre informatique total ; β serait la fraction du résultat brut d'exploitation annuel pouvant servir à éponger une catastrophe ; γ est la proportion estimée (taux de couverture probabilisé), compte tenu des garanties (assurances...) prises, pouvant servir de compensation monétaire (ou technique) en cas d'accident survenant au système d'information.

On verra par la suite que la détermination de ce RMT par la Direction générale est indispensable non seulement parce que c'est elle et elle seule qui doit fixer les arbitrages, mais aussi parce qu'il sert de "majorant" aux équations de risques définies ci-après.

En tout état de cause, il est clair que, globalement, même si rien n'est fait, l'espérance mathématique du coût des risques doit, quand même, être inférieure ou égale à la barre maximale représentée par le RMT.

Équation 2

P ↙ Probabilité d'apparition des risques	x	V ↘ Valorisation financière des conséquences directes et indirectes de ces risques	≤ RMT

17 notamment, ses moyens, son assise financière, son aversion pour le risque...

18 Il s'agit d'une limite de pertes, comme les banques s'en fixent dans d'autres domaines.

Cette équation 2 peut, bien sûr, aussi se décliner par type i[19] de risque auquel on peut associer une part 6i du RMT et qui peut ne pas être strictement proportionnelle à la part

$$Pi \times Vi \,/ \sum_{i=1}^{m} Pi\ Vi$$

pour peu que la contrainte globale représentée par l'équation 2 soit satisfaite.

Soit l'équation 3 :

$$Pi \times Vi \leq \lambda i\ RMT$$

d. Classer ses informations entre "stratégiques" et "non stratégiques"

Dans l'analyse ci-dessus on a fait l'hypothèse que les risques s'appliquaient à des informations de qualité identique. Il est évident qu'il n'en est rien : les informations peuvent et doivent être classées[20] -par la Direction générale, in fine- entre "stratégiques" et "non stratégiques" au minimum. Mais une classification plus fine peut être faite en s'aidant d'une échelle d'évaluation de l'impact des risques. Bien entendu, cette échelle est donnée à titre indicatif puisque c'est à chaque Direction générale, en fonction de ses contraintes et de ses choix, d'afficher ses arbitrages.

19 Cette déclinaison par type de risque permet une évaluation fine par chaque spécialiste dans son domaine. La globalisation, nécessaire, sera faite par le responsable de la sécurité du système d'information.

20 Ceci doit se faire à partir d'une "architecture globale" du système d'information où sont répertoriés tous les systèmes et sous-systèmes de données (bases informatiques + environnement et liens).

L'ÉCHELLE D'ÉVALUATION DE L'IMPACT DES RISQUES

Les risques sont évalués selon une échelle à cinq niveaux définis en fonction des conséquences des incidents qui altéreraient le fonctionnement et le déroulement normaux de l'activité. Seuls les risques de niveau égal ou supérieur à 2 sont pris en considération dans la recherche des contre-mesures. Les risques de niveau 1, dits "risques résiduels", sont assumés par le responsable du sous-système d'information.

Stratégique : 4

- Tout événement susceptible d'entraîner l'arrêt immédiat (ou rapide) d'une activité de l'établissement, ou d'entraîner des sanctions judiciaires au plus haut niveau de responsabilité de l'établissement.

Critique : 3

- Tout événement pouvant entraîner des pertes financières inacceptables (ex : 30 % du RMT) ou importantes au regard des enjeux économiques de l'entreprise.
- Tout événement susceptible d'entraîner une perte importante de clientèle.
- Tout événement susceptible d'être considéré comme une infraction majeure à la législation.
- Tout événement pouvant entraîner une nuisance organisationnelle jugée importante sur l'ensemble de l'entreprise.
- Tout événement susceptible de nuire aux décisions et orientations de l'établissement (tableaux de bords erronés).

Sensible : 2

- Tout événement susceptible d'occasionner des pertes financières significatives.
- Tout événement susceptible de nuire de manière significative à l'image de marque et à l'aspect commercial.
- Tout événement susceptible d'être considéré comme une infraction mineure à la législation.
- Tout événement pouvant entraîner une nuisance organisationnelle jugée significative par l'utilisateur.

Faible : 1

- Tout événement susceptible d'occasionner des pertes financières faibles au regard des enjeux.
- Tout événement pouvant générer une nuisance organisationnelle faible, interne au domaine considéré et peu gênante pour l'utilisateur.

Nul : 0

- Niveau d'évaluation présent dans l'échelle d'évaluation des risques MARION mais jugée non significative.

Une évaluation plus précise, et quantifiée, des niveaux 3, 2 et 1 n'est pas toujours immédiatement possible ; elle dépend de l'entreprise et s'appuiera au fur et à mesure du temps passé sur l'expérience acquise et les comparaisons entre applications.

On trouvera quelques conseils pratiques dans la fiche conseil n° 26 : "propriétaires et classification des informations" (on remarquera que la classification retenue n'y est pas absolument la même que celle ci-avant mais c'est à dessein que cette dernière est donnée comme représentative d'une évaluation à forte aversion contre le risque, alors que celle de la fiche 26 correspond à une évaluation plus habituelle. Ceci illustre bien ce qui a déjà été indiqué (cette évaluation dépend des choix de la Direction générale).

e. La mesure des faiblesses peut être réalisée selon l'une (ou plusieurs) des méthodes connues (MARION[21], MELISA, CRAMM...).

Il est conseillé, pour les établissements qui souhaiteraient se positionner, de remplir eux-mêmes le questionnaire "mini-MARION" figurant en annexe III et qui est celui réalisé et utilisé par le SGCB lors de son enquête de 1992[22].

Les faiblesses découvertes grâce à ce mini-questionnaire (niveau de facteur MARION inférieur à 2) pourront faire l'objet d'un plan de remise à niveau.

Si l'objectif à atteindre est ≥ 3, il serait bon que les établissements se fixent un objectif global $\geq 2{,}7$ sans qu'aucun facteur soit inférieur à 2.

Toutefois, ce n'est pas seulement le niveau de sécurité qu'il convient d'examiner, mais, également, son évolution dans le temps. C'est pourquoi, selon une fréquence à déterminer, cet examen sera à refaire périodiquement (minimum = 3 ans).

f. Les faiblesses mesurées, la classification des données opérées, l'analyse des risques réalisée, comment arbitrer entre les priorités ?

Il faut passer de l'équation 2 ($P \times V \leq RMT$) à l'équation 3 plus opérationnelle et faire un bilan coût/avantage des parades face aux risques. On peut en effet, pour chaque risque, écrire[23] :

21 MARION est plus orientée vers la mesure et MELISA vers la solution des problèmes (mise en place des parades avec leurs coûts associés). Le fait que MARION soit une méthode publique (APSAD/CLUSIF), donc gratuite, et de ce fait fort répandue, l'a désignée comme candidate à l'enquête du SGCB.

22 Ce mini-questionnaire ne saurait dispenser d'effectuer un vrai "chantier" MARION, MELISA ou autre qui, seul, permettra d'avoir un diagnostic complet.

23 La garantie donnée par un contrat d'assurance dont la probabilité d'exécution est certaine se retranchera de V et s'ajoutera à C (pour les primes). On peut compléter ce schéma en distinguant les mesures de prévention des mesures de protection.
Les 3 paramètres P, V et C sont grosso modo connus des spécialistes (cf. CLUSIF, APSAD, Forum des compétences, SSII spécialisées, constructeurs, confrères...).
Il est clair que Ci doit être inférieur à Pi x Vi.

Équation 3

Bi	=	Pi	x	Vi	-	Ci
Bilan de l'opération i		Probabilité d'apparition du risque		Valorisation financière des conséquences financières		Coûts des éléments de sécurité à mettre en œuvre pour contrer ce risque

<------->
Echelle de gravité traduite en coûts actualisés

<--->
Bilan actualisé coût/avantage lié aux opérations de sécurité mises en place pour contrer ce risque

Ce bilan risque par risque permet de hiérarchiser les actions à mener (pour un coût de solution standard ou moyen CiBAR). Toutefois, pour être complet, on doit, lui aussi, le "probabiliser" en fonction de son efficacité pour tenir compte du fait qu'il existe une probabilité non nulle pour que, une fois l'opération de sécurité mise en œuvre, la couverture ne soit pas totale. Ce risque résiduel probabilisé après couverture doit faire l'objet des mêmes opérations que celles réalisées pour le premier membre de l'équation 3 (Pi x Vi), c'est-à-dire qu'il faut tenir compte des conséquences financières de ces risques résiduels et, éventuellement, de la solution supplémentaire à mettre en œuvre pour les réduire...

C'est la somme probabilisée de ces risques résiduels qui, une fois valorisée, doit être inférieure au risque maximum tolérable (RMT) déjà défini.

Si ce n'est pas le cas -i.e. si la somme des risques résiduels n'est pas inférieure au RMT- une autre solution de sécurité, plus efficace mais sans doute plus onéreuse[24], devrait faire l'objet d'une évaluation selon l'équation 3.

Il est possible de procéder par itération jusqu'à ce que la part du risque résiduel ayant diminué, la somme de ces risques soit compatible avec le RMT fixé.

C'est ce que décrit l'équation 4.

Équation 4

R =	$\sum_{i=1}^{n=\text{risques}}$	Risques résiduels probabilisés et valorisés compte tenu de l'efficacité probable des solutions	≤ RMT

[24] C'est-à-dire CiBAR ` Ci. La couverture du risque peut jouer sur V (par exemple assurance) mais surtout sur P (par exemple installation d'onduleur contre les micro-coupures électriques). Mais, s'il y a bien un lien (une corrélation positive) entre le coût de la solution et l'efficacité de la couverture, et donc le risque résiduel, en probabilité, ce lien n'est ni absolu, ni linéaire, ni même garanti. De ce fait, autant il est relativement aisé d'appliquer intuitivement cette méthode sur des cas concrets, autant il est délicat de donner une expression analytique complète à l'équation 4.

RETOUR SUR LES ÉQUATIONS DE RISQUE

• L'analyse

Les équations 3 et 4, ont été extrêmement simplifiées pour des raisons pédagogiques.

Il faut, maintenant, un peu les compliquer pour les rendre opérationnelles, et ceci en introduisant le temps ; et distinguer la perte ex-ante -si aucune parade n'était mise en œuvre- de la perte possible ex-post après leur installation. Cette mesure a toutefois une incidence sur la probabilité d'apparition du risque (après) et/ou des conséquences : on peut faire un investissement de prévention (ceci diminue la probabilité Pi) ou un investissement de protection (ceci diminue la valorisation financière Vi). De plus, il faut un certain temps pour mettre en place la parade de coût Ci. Il faut donc distinguer les probabilités ex-ante Pi et celles ex-post P'i.

Les équations 3 et 4 peuvent alors se récrire :

Équation 5 $$Bi = Pi\ Vi - Ci + P'i\ V'i$$

1. bilan partiel avant mesure prise bi = Pi Vi
2. bilan partiel après mesure prise b'i = P'i V'i - Ci

ou avec prise en compte du temps :

Équation 6 $$Bi = Pi^{t}\ Vi^{t} - (P'i^{t+1}\ V'i^{t+1}) - (Ci^{t\ à\ t+1})$$

Bilan de l'opération i	ancienne perte	perte possible (après prise des mesures en t+1)	dépenses (coûts des mesures s'étalant de t à t+1)

ou Équation 7 $$Bi = \Delta\ Pi\ Vi - Ci$$

Bilan	gain (perte évitée) diminution possible du risque	coût de la parade mise en œuvre

D'autres contraintes existent :

- P'i V'i < RMT i.e. : pas de risque demeurant supérieur au RMT
- Bi > 0 i.e. : la parade doit être rentable (le bilan actualisé doit demeurer positif)

et Équation 8 $$\Sigma\ P'i\ V'i\ 9\ (RMT - \Sigma\ Ci)$$

car le coût des mesures pourrait avoir un impact sur le RMT (on supposera, par la suite, que cet effet du deuxième ordre est à négliger).

Enfin, il convient, après coup, que la somme des risques résiduels (probabilité x valorisation) demeure inférieure ou égale au RMT.

Équation 9 | $\Sigma P'j V'j \leq RMT$

Il faut noter qu'il n'y a pas de lien absolu, rigoureux, entre la dépense et l'efficacité de la parade. Dès lors, des erreurs de choix peuvent exister entre plusieurs solutions dont les écarts des couples (Pi Vi - P'i V'i) / Ci ne sont pas proportionnels. Le lien existe cependant si on décide d'ajouter des mesures pour un même risque, mais la question est alors de savoir où s'arrêter.

Un exemple simple permet d'expliciter cela :

Contre le risque de vol d'un PC, on a le choix entre les solutions suivantes :

1. disposer d'une clef sur le PC
2. fermer le bureau où est le PC à clef
3. blinder tous les accès du bureau (porte...)
4. mettre un gardien devant la porte
5. assurer le contrôle d'accès (électronique + vigiles) de l'ensemble du périmètre
6. déménager et mettre le bureau et le PC sur une île déserte...

Malheureusement, la gradation des mesures et de leur coût n'assure pas, complètement, contre une absence de proportionnalité de l'efficacité.

Ainsi : on a le choix entre la mesure 1 (de faible coût) et, par exemple, 4 (de fort coût) sans qu'il y ait une garantie absolue que 4 soit plus efficace que 1.

Certes, analytiquement, tout ceci est pris en compte dans la modification des probabilités et des valeurs de P'i V'i ; mais la difficulté concrète est d'évaluer comment une mesure, de coût Ci, face à un risque probabilisé Pi Vi va changer effectivement la valeur du risque probabilisé après installation (P'i V'i).

• Algorithme opérationnel proposé

Concrètement, ces difficultés peuvent trouver une solution. Il est proposé la démarche suivante :

1. Eliminez tous vos risques importants (ceux qui, ex-ante, sont supérieurs au RMT) sans mener l'analyse en termes de bilan actualisé.
2. Procédez à une analyse fine sur les risques résiduels (ceux dont Σ Pi Vi < RMT). Faites un tri par ordre décroissant de Σ Pi Vi puis de Bi des mesures à prendre en fonction des "équations" de bilan actualisé. La mesure des W Pi Vi sera réalisée par jugement d'expert (s'appuyer sur l'APSAD, le CLUSIF, le Forum des Compétences, vos confrères, une société de service spécialisée...).
3. Commencez par les opérations Bi de rang supérieur.
4. Tenez compte du temps (arbitrage, étalement, planning, prévision) et des possibilités.

III - LES PARADES POSSIBLES

Les deux chapitres précédents ont indiqué que les risques pesant sur les systèmes d'information des établissements de crédit représentent une menace réelle, mais que des méthodes connues existent pour déterminer ces risques et tenter de les mesurer.

Face à eux, une fois valorisés et hiérarchisés, comment faut-il organiser les parades pour qu'elles soient efficaces ?

Trois niveaux de réponse sont possibles :

1. Niveau 1 : réduire les faiblesses découvertes,
2. Niveau 2 : passer d'une réponse "au coup par coup" à une réponse organisée,
3. Niveau 3 : surveiller en permanence les risques présents et ajuster les parades. Agir en prévision des risques nouveaux.

1. Niveau 1 : réduire les faiblesses découvertes lors des analyses menées

La méthodologie décrite au chapitre précédent -ou une variante plus sophistiquée- permet, si elle est soigneusement appliquée, d'éliminer, sinon les sources du risque, du moins de maîtriser avec une bonne probabilité les conséquences fâcheuses d'un sinistre.

2. Niveau 2 : passer à une réponse organisée

a. Désigner un RSSI, responsable de la sécurité du système d'information

En effet, toutes les techniques et mesures qui sont évoquées précédemment, doivent s'inscrire dans la durée. Il convient pour cela d'élaborer une politique de la sécurité qui doit trouver sa traduction première dans un schéma directeur de la sécurité des systèmes d'information ou SDSSI[25].

Bien entendu, ce schéma doit être traduit en propositions et actions concrètes et constituer le "plan sécurité" de l'établissement.

Une organisation doit être mise en place si l'on veut assurer efficacité et pérennité. Il importe, en particulier, qu'un responsable de la sécurité des systèmes d'information (RSSI) soit désigné et que son rattachement hiérarchique soit suffisant pour assurer son rôle inter-services. Disposant de la confiance de sa Direction générale, suffisamment technicien mais disposant de la hauteur de vue qu'un trajet dans différentes directions opérationnelles lui aura permis d'acquérir, il lui appartiendra d'impulser et de coordonner les actions dont certaines seront entreprises par d'autres Directions que la sienne. Il n'est pas conseillé de le rattacher à l'OI puisque son rôle est celui d'un décideur qui effectue surtout un contrôle de deuxième niveau[26] ; mais étant contrôleur il doit pouvoir être maître d'œuvre au besoin et "payeur" des actions sécuritaires qu'il entreprend, c'est-à-dire qu'il doit disposer d'un budget.

---

25 Le SDSSI est la mise en application des recommandations figurant dans ce livre blanc (analyse des risques, évaluation du niveau de sécurité, mesures correctives pour les points faibles, organisation de la sécurité...). Il est suggéré de faire un planning sur 3 ans, en réalisant les mesures à prendre en fonction de l'ordre décroissant de leur "bilan-sécurité".

26 Une autre raison tient au désir -naturel-, des informaticiens à rendre l'informatique "conviviale". Trop de convivialité peut aller à l'encontre de la sécurité. De plus, les techniciens de l'informatique sont parfois trop confiants dans la capacité des logiciels à couvrir tous les besoins de sécurité et, d'une manière générale, dans la technique. Ainsi, l'informaticien aura tendance à minimiser l'occurence d'un incident (avec, à la limite, le risque d'en nier l'existence) et à moins se soucier des conséquences d'un incident, au cas où il se produirait. C'est, en effet, le couple (P,V) qu'il faut analyser et surveiller.

Toutefois, son rôle est, d'abord, celui d'un "maître d'ouvrage" qui impose des normes, exige des travaux que le plus souvent il ne réalise pas lui-même mais qu'il réceptionne et contrôle (= "recette"). Ce n'est que s'il y a carence de l'informatique interne, qu'il devient momentanément "maître d'œuvre", réalisateur de ce qu'il souhaite.

Il participera à, ou imposera, l'intégration de la sécurité dans la méthode de développement et l'AGL[27] retenu par l'établissement (cf. annexes V et VI) ainsi qu'à la mise en place de codes de déontologie pour les informaticiens ou à celle de la charte de sécurité (cf. annexes VII et VIII).

Il impulsera, enfin, les actions de sensibilisation, d'information et de formation des personnes aux règles, consignes et état d'esprit sécuritaires.

La sécurité est, en effet, surtout une question d'état d'esprit, de culture d'entreprise et de comportement : l'essentiel de ses actions consistera donc à mettre en place une organisation adéquate, possédant correspondants et relais à tous les niveaux nécessaires, disposant de moyens de sensibilisation, de formation et de documentation.

b. Les cinq conditions de sa réussite

Toutefois, pour que cette politique de la sécurité puisse être efficace, cinq points apparaissent fondamentaux.

- un engagement suivi de la Direction générale, qui doit définir le risque maximal tolérable, la liste des données stratégiques et les grandes options : coûts/avantages, problèmes de personnels.
  De plus, une fois l'analyse des menaces et des parades réalisée, les "équations" du risque doivent être examinées par les dirigeants[28].
  L'appui de la Direction est également indispensable au RSSI dont le rôle, parfois ingrat, l'oblige à des "remobilisations" et des "piqûres de rappel" à l'état d'esprit sécuritaire qui peuvent à la longue lasser ses collègues. Parmi les facteurs de sécurité, il faut donc placer très haut le soutien sans faille de la Direction.
- l'analyse de la situation (cf. supra) ;
- la définition du schéma directeur de la sécurité des systèmes d'information (SDSSI) qui présente à l'arbitrage de la Direction générale le plan d'action (mesures à prendre, organisation à définir), les budgets, les plannings, la politique de protection et de gestion des risques et le contrôle ;
- la sensibilisation permanente de tout le personnel pour rechercher l'adhésion autour du schéma sécuritaire : les moyens techniques ne sont rien sans l'organisation humaine et les hommes qui la font vivre ;
- la cohérence et le bon sens. Il n'existe pas, en effet, de parade absolue et éternelle. Le bon sens conduit à adapter la nature et l'importance des moyens aux risques et aux enjeux. La cohérence, parce qu'il est inutile de raffiner la sécurité sur un sous-ensemble s'il existe de grosses faiblesses dans d'autres sous-ensembles : le niveau de solidité de la chaîne est celui de son maillon le plus faible[29].

---

27 Atelier de génie logiciel.

28 On rappelle que cette équation -qui exprime la différence entre la valorisation du risque et le coût des éléments de sécurité à mettre en oeuvre pour contrer ce risque- a une valeur plus générale ; elle s'applique autant à l'analyse des risques bancaires, notamment de marché, qu'au domaine informatique (cf. page 43 le schéma sur la "constellation" du risque bancaire).

29 On rappellera le cas récent de cette institution britannique dont l'accès au système -théoriquement inviolable- avait aisément été forcé par des stagiaires ayant noté les mots de passe laissés en clair par les agents sur des auto-collants mis sur leurs écrans !

Prévue à temps, c'est-à-dire au début de toute application, la mise en œuvre de la sécurité peut ne représenter qu'un coût assez modique[30]. Souvent, mais pas toujours, les lacunes dans la sécurité peuvent être en partie comblées par des matériels et des logiciels pas trop onéreux ou par des modifications administratives et par une action d'explication et de sensibilisation du personnel, pour peu que la Direction générale donne une impulsion suffisante[31]. Bref, il ne s'agit pas nécessairement de dépenser plus mais de dépenser mieux.

Enfin, l'analyse préventive des risques doit devenir un réflexe. Aucune mesure sécuritaire ne pouvant garantir une infaillibilité totale et durable, le "réflexe sécurité" doit jouer par principe et être modulé en fonction des risques et des coûts. Toute catégorie d'opérations nouvelles, toute application nouvelle doit faire l'objet d'une étude du risque dans toutes ses composantes ; et donc, la composante système d'information/informatique. Ceci rendra plus actuel le développement de la fonction risk manager en y ajoutant une composante : le "gestionnaire des risques non strictement bancaires" ou RSSI dans les établissements de crédit.

3. Niveau 3 : agir en prévision des risques nouveaux

L'environnement, la technologie, les risques et les fraudeurs ne restent pas sans changer. Il convient donc, en permanence, non seulement de surveiller les risques présents et d'ajuster les parades, mais aussi d'agir en prévision des risques nouveaux. L'analyse globale des risques doit être renouvelée périodiquement, par exemple, tous les trois ans ou, mieux, devenir une action permanente impulsée et coordonnée par le RSSI. En effet, les innovations technologiques ou d'organisation imposent de revoir les analyses de risque déjà effectuées.

A titre d'exemple, le lecteur pourra se reporter aux fiches-conseil de l'ANNEXE IV qui, sans couvrir tous les risques, en répertorient l'essentiel. Ces fiches qui, pour la commodité, ont été classées par ordre alphabétique, peuvent être regroupées en trois parties : celle relative aux risques "traditionnels" (mais toujours dangereux), celle traitant des risques liés aux "nouvelles technologies" (interconnexions des réseaux, "downsizing", réseaux locaux, architecture client/serveur, EDI, GED...), celles, enfin, exposant les risques tenant à "l'externalisation" (infogérance ou "outsourcing", "facility management" ou FM, télémaintenance...).

---

30 La sécurité coûte d'autant plus cher qu'elle est rapportée ; son intégration sous forme d'analyse de risques, dès la conception des projets, doit en faire une composante banale de la production, au même titre que la qualité.

31 On trouvera en ANNEXE VI un exemple de prise en compte de la sécurité dans les applications. Ceci suppose, bien sûr, que les "chefs de projet" soient sensibilisés et/ou formés à l'analyse du risque dans les applications qu'ils développent, ou que les spécialistes de la sécurité (RSSI) surveillent la mise en œuvre des recommandations sécuritaires.

IV - RECOMMANDATIONS

Cet ouvrage vise à être un "guide des meilleures pratiques", c'est-à-dire un idéal vers lequel il est souhaitable que tous les établissements de crédit situés en France tendent à se rappprocher. Tous les conseils méritent attention (et les chapitres précédents et les annexes qui suivent en présentent de nombreux aspects), mais s'il fallait résumer le "noyau dur" de ces recommandations, voici deux fiches présentant l'indispensable : l'une à destination des techniciens (RSSI ou à défaut responsable sécurité ou informaticiens), l'autre à destination des dirigeants.

RECOMMANDATIONS POUR LES **RSSI**
Responsables sécurité
INFORMATICIENS

1. Mesurez et classez vos risques.
   - Les méthodes sont connues ou faciles à trouver (cf. annexes III et IX)
   - Contrairement à une opinion répandue, dans la banque, le risque réel n'est pas tant 1. La disponibilité, 2. La confidentialité, car, en général, les mesures adéquates sont déjà -sauf exception- prises, mais 1. Intégrité, 2. Confidentialité, 3. Disponibilité, 4. Preuve.
     C'est sur ces deux premiers aspects qu'il convient maintenant de faire porter l'effort.

2. Bien sûr, éliminez au plus vite vos points faibles.
   - Tout facteur MARION ayant une cote inférieure à 2 devrait être désigné à l'attention des responsables et les mesures appropriées pour résoudre ces points faibles prises.
   - Comparez vos résultats à la matrice de référence donnée en annexe III.

3. Mais surtout, procédez à une étude formalisée (auditable) de VOTRE risque.
   - Examinez les causes du risque.
   - Imaginez les scénarios catastrophes et chiffrez les (coûts, probabilité...).
   - Etablissez pour vos dirigeants le plan d'action (parades, coûts/avantages...).

4. Intégrez la sécurité dès le début des applications (INCAS, MESSIE).

5. Avant tout, comme pour vos risques bancaires, de façon générale pour tous les sujets, procédez à une "division des risques".

   - pas de mono fournisseur, constructeur, machine...
   - informations stratégiques, versus non stratégiques (à faire)
   - établissez impérativement un plan de sauvegarde ("back-up", "mirroring"...) au moins pour les données stratégiques.

6. Il n'y a pas de sécurité sans tableau de bord de la sécurité (suivi ; détection avancée -"early warning").
   - choisissez vos indicateurs (opèrez une distinction entre les actions relevant de la "sécurité ordinaire" et la prévention des fraudes, car la démarche à mener est différente)
   - et surveillez-les (voir indicateurs de qualité des 36 fiches-conseil de l'annexe IV)

7. S'il convient d'évoluer, méfiez-vous des "modes" même si elles recouvrent aussi des "vagues de fond". Notamment :
   - client/serveur (surtout sur système ouvert)
   - systèmes ouverts (pas encore assez sécurisés)
   - "outsourcing" total
   - réseaux extérieurs (pas d'interbanking avec Internet !)
   - réseaux locaux
   - downsizing
   - solutions "exotiques"
   - informatiques des salles de marché en dehors du schéma de sécurité général ou en dehors de tout contrôle (pas de professionnalisme informatique, solutions sécurité trop "légères" -notamment "back-up" et liaisons back-office et comptabilité générale-, logiciels importants trop dépendants d'un seul fournisseur parfois fragile (boîtes noires, maintenance non assurée à terme...)).
   - EDI
   - portables
   - etc.

Se méfier n'est pas rejeter mais analyser avec soin et monter les parades adéquates.

Sauf si cela est jugé primordial et que les moyens adéquats sont là, la stratégie optimale n'est pas, en général, d'être "pionnier/leader", mais d'être "suiveur-agile". Cette dernière solution, tout en permettant la flexibilité nécessaire par rapport au progrès, permet d'évaluer avec un peu de recul les coûts, les risques et les avantages des nouvelles techniques.

8. Il faut, enfin, convaincre, sensibiliser, informer, surveiller...

RECOMMANDATIONS POUR LES DIRIGEANTS

Niveau ❶ Faites procéder à une analyse des vulnérabilités de l'établissement, et faites vous en communiquer le rapport. Ceci implique de :

a. mesurer, par une des méthodes disponibles sur le marché, le niveau de sécurité atteint, le comparer et en suivre l'évolution.

A défaut, utiliser le mini-questionnaire MARION figurant en ANNEXE III et se positionner.

b. éliminer les faiblesses et les vulnérabilités découvertes (niveau < 2).

c. évaluer le risque maximal tolérable, RMT, ou montant maximal du risque - conséquences financières d'un sinistre informatique- que l'établissement peut supporter sans remettre en cause la continuité de ses opérations [la définition du RMT figure dans le corps de ce Livre blanc].

d. choisir, parmi les informations (fichiers, bases...) de l'entreprise, celles qui sont jugées stratégiques et qui doivent absolument faire l'objet d'une haute protection (plan de secours).

e. orienter les mesures à prendre (arbitrages) b ne pas dépenser plus mais dépenser mieux.

Niveau ❷ Essayez, dès que possible, de passer de l'artisanat à l'industrie. Ceci suppose que vous donniez vos instructions pour faire :

a. mettre en place une organisation. Notamment désigner un responsable de la sécurité des systèmes d'information -RSSI- avec un haut niveau de rattachement hiérarchique. Mais aussi faire en sorte que la sécurité informatique soit intégrée, dès le départ, dans toutes les applications informatiques [voir annexe VI].

b. élaborer une politique de la sécurité traduite dans un schéma directeur de la sécurité des systèmes d'information ou SDSSI [voir infra]. Définir une charte de la sécurité de l'information.

c. la traduire en PLAN SECURITE et la mettre en œuvre dans des délais adaptés. Comme pour toute activité importante, demander un "tableau de bord" de suivi pour les responsables.

d. sensibiliser, éduquer, former les personnels et développer une culture de l'entreprise intégrant bien la notion de risque. Le facteur humain reste déterminant. Rien ne peut se faire sans une adhésion du personnel (voir ANNEXE VII).

Niveau â Agissez en prévision des risques nouveaux.
L'analyse globale des risques doit être renouvelée, mieux : devenir une action permanente

Mais tout ceci ne peut se réaliser **sans une forte implication de la Direction Générale**[32] pour qui la sécurité doit être l'un des objectifs.

[32] C'est-à-dire qui doit "patronner" cette démarche et le faire savoir clairement ; et le démontrer par un suivi actif et continu : dans ce domaine, les "opérations-gadget" ou "coup de poing" ne servent qu'à gaspiller du temps et de l'argent.

POUR FINIR
UNE "CHECK-LIST" SUR
LES POINTS DE SÉCURITÉ LES PLUS IMPORTANTS

• Organisation de la sécurité : responsabilités

La nomination d'un Responsable de la Sécurité du Système d'Information est la première mesure qui permet à un établissement de crédit d'affirmer l'importance accordée aux objectifs de sécurité.

Est-ce fait ?	oui	non
	☐	☐

• Méthode et outils de développement

Les méthodes de conception et de réalisation d'applications informatiques doivent intégrer une analyse de risque débouchant sur une prise de conscience des causes de risques et l'élaboration des mesures de sécurité appropriées.

Est-ce fait ?	oui	non
	☐	☐

• Moyens et procédures de secours

Le Plan de secours met en œuvre des moyens et des procédures qui permettront à l'établissement de reprendre et de poursuivre son activité à la suite d'un sinistre affectant son outil informatique. Le caractère indispensable d'un tel Plan est démontré dès que sont analysés les impacts d'un arrêt partiel ou total des traitements informatiques.

Est-ce fait ?	oui	non
	☐	☐

• Sauvegardes procédures et conservation

L'un des objectifs majeur du Plan de secours réside dans la production régulière et la conservation des sauvegardes ; en effet, de leur cohérence, de leur exhaustivité et de leur aptitude à limiter la perte d'information dépendra la poursuite de l'activité de l'établissement de crédit.

Est-ce fait ?	oui	non
	☐	☐

• Contrôle d'accès logique

Les contrôles d'accès logiques s'avèrent indispensables pour restreindre et contrôler les possibilités opératoires quasi illimitées offertes par l'utilisation de l'outil informatique.

Est-ce fait ?	oui	non
	☐	☐

• Audits et contrôles

La permanence des missions d'audit et de contrôle est un élément déterminant de leur efficacité qui vise à détecter, le plus tôt possible, des dérives par rapport aux règles internes et externes.

Est-ce fait ?	oui	non
	☐	☐

***

Une seule réponse négative devrait vous inciter à revoir au plus vite cette question.

CONCLUSION

Le risque pesant sur les systèmes d'information est l'une des composantes du risque global de la banque.

Dans la "constellation des risques" auxquels un établissement de crédit doit faire face, ce n'est pas en général celui qui inquiète le plus les autorités de contrôle ; mais, parce qu'il a une "volatilité" extrême et parce qu'il est croissant[33], ce risque informatique[34] doit être mesuré, surveillé, contrôlé, géré et réduit au mieux.

Ceci est faisable : convenablement organisée, la prise en compte dans les projets de la sécurité, comme celle de la qualité, n'est pas si coûteuse ; en revanche, faute de le faire, les conséquences financières directes (pertes) ou indirectes (image de marque, service à la clientèle...) peuvent être importantes.

La Commission bancaire se doit d'attirer l'attention des responsables bancaires sur la nécessité de maîtriser correctement ce risque, le parallèle pouvant être fait avec le risque nucléaire -une probabilité d'accident "faible", mais des conséquences "infinies"- dont chacun conviendra qu'il serait insensé qu'une action efficace et rigoureuse pour le prévenir ne soit pas entreprise.

C'est la raison pour laquelle à la suite d'une enquête réalisée auprès d'un échantillon d'établissements de crédit sur le risque informatique, enquête dont la publication a montré certes les forces (un niveau de sécurité supérieur aux autres industries marchandes), mais aussi les faiblesses, il a paru utile à la Commission bancaire de poursuivre cet effort de sensibilisation en publiant ce Livre blanc.

Cet ouvrage est un guide des pratiques conseillées ("a best practice paper") et se veut pragmatique et opérationnel. Plutôt que de procéder par voie réglementaire -dans un domaine où la mouvance des techniques rend la chose peu efficace sauf à se cantonner à quelques schémas simples-, il a paru plus judicieux et plus efficace, avec l'aide de la Profession, de réunir conseils et méthodes et de les synthétiser en recommandations[35].

Ce Livre blanc indique que, plus que pour les autres industries, la menace informatique constitue, pour les banques, un danger réel et spécifique. Or, les banques ont un devoir de sécurité vis-à-vis d'elles-mêmes, de leurs clients et du système bancaire. Les enquêtes réalisées, notamment par la Commission bancaire, et dont un résumé figure dans les pages précédentes, montrent que le niveau de sécurité des établissements de crédit est encore perfectible.

Pour améliorer ce niveau de sécurité, il faut disposer d'outils de mesure du risque -qui sont ici exposés- de façon à établir des parades et à formuler des recommandations d'actions.

---

33 Toujours plus présente, l'informatique présente des faiblesses dans deux domaines en expansion : l'explosion des télétransmissions et des tranferts -que la mondialisation et les produits de marché provoquent-, le développement des salles de marché reposant sur des techniques informatiques nouvelles et parfois fragiles (montants financiers très élevés et outils "sophistiqués").

34 S'il convient, en toute rigueur, de parler de risques du système d'information, la place prise par l'informatique dans le processus de production bancaire est maintenant tel, que la surveillance de l'informatique au sens large (y compris télécommunications, réseaux, fax, téléphone, gestion électronique des documents...) en est la composante essentielle.

35 Ceci explique le niveau de langue retenu ici, plus proche du "style journalistique" qu'administratif.

Il est fortement suggéré aux établissements de crédit de s'en inspirer. Les contrôles sur place menés par la Commission bancaire tendront, de plus en plus, à s'orienter, entre autres, vers cet aspect du risque déjà répertorié par les règlements 90-08 et 91-04 et par la Directive sur les services d'investissement qui dispose que les établissements de crédit doivent "avoir des mécanismes de contrôle et de sécurité dans le domaine informatique".

La sécurité des systèmes d'information doit donc devenir, -si elle ne l'est déjà- l'un des objectifs de chaque Direction générale.

Si l'absence de sécurité est un risque, sa présence peut être une arme commerciale, non seulement en réduisant ou en supprimant les pertes dues aux risques mal maîtrisés mais aussi, parce que, tôt ou tard, sous la pression des clients, des contreparties, des techniques (EDI...), des agences de notation, un "rating du niveau de sécurité informatique" finira par s'imposer. Les établissements qui s'y seront préparés bénéficieront d'un avantage concurrentiel incontestable.

C'est pourquoi il est utile qu'à côté d'une fonction de gestionnaire de tous les risques bancaires, il existe une fonction de responsable de la sécurité des systèmes d'information, gestionnaire des risques non strictement bancaires.

LA CONSTELLATION DU RISQUE BANCAIRE

Le schéma, ci-après, indique que la banque doit faire face à trois grandes catégories de risques :

1. Les risques "politiques"
2. Les risques bancaires
3. Les risques techniques

1. Les risques "politiques" comprennent (liste non exhaustive) :

a. le risque de management :
- équipe dirigeante mal informée, défaillante ou divisée
- actionnaires divisés ou faibles
- mauvaise organisation et surveillance ou contrôle interne insuffisants (mauvais suivi).

b. le risque de stratégie :
- mauvaise orientation générale, défauts d'arbitrage
- mauvais choix de partenaires
- déséquilibres entre les moyens, les finalités, la rentabilité et les risques
- stratégie incohérente
- mauvaise communication (interne, externe) et image de marque.

c. le risque "éthique" ou de non respect implicite ou volontaire de règles :
- réglementaires
- fiscales
- déontologiques

d. le risque extérieur : mauvaise appréhension des risques politiques, sociaux, humains, internationaux, systémiques ; mauvaises réactions et parades.

Ces risques, l'expérience le prouve, sont ceux qui ont le plus d'impact sur la survie d'un établissement de crédit. Ils inter-réagissent, bien sûr, sur les risques suivants.

2. Les risques bancaires. On peut y distinguer :

a. les risques économiques :
- erreurs de prévisions (inflexions sur les marchés mal évaluées, évolutions des taux mal prévues, prises de positions inconsidérées, ...)
- erreurs de calcul de rentabilité (contrôle de gestion défaillant, provisionnement incertain...).

b. les risques de contrepartie :
- de signatures, de crédit ou de défaillance (interbancaire, clientèle)
- sectoriels ou géographiques (risque-pays) : mauvaise division des risques
- de produits/supports (ex. : pension livrée versus réméré).

c. les risques financiers ou de marché :
- liquidité/transformation
- solvabilité/rentabilité
- taux d'intérêt
- change, devises
- titres (à revenus variables ; à revenus fixes)
- règlement/livraison (risque Herstatt)

- transferts.

d. les risques non strictement bancaires ou para bancaires sur les autres activités (services, ingénierie financière...).

3. Les risques techniques. Parmi eux :

a. les risques opérationnels :
   - risques techniques (divers)
   - risques technologiques (mauvais choix)
   - risques juridiques (ex. : mauvais montages, pas de garanties, erreurs d'analyse...)
   - risques organisationnels (procédures) et humains
   - risques administratifs (gestion, mauvais traitements, pertes de documents...).

b. les risques environnementaux (naturels, sociaux)

c. les risques sur les systèmes d'information (D, I, C, P)
Incapacité à faire face aux besoins internes et externes :
- catastrophes, destruction
- défaillances, pannes
- fraudes, détournements, pertes
- traitements erronés
- mauvaise organisation, productivité basse, coûts
- réactivité

Ce sont ces risques dont traite ce Livre blanc.

d. divers (autres sécurités physiques, transports, risques sur les biens et les personnes...)

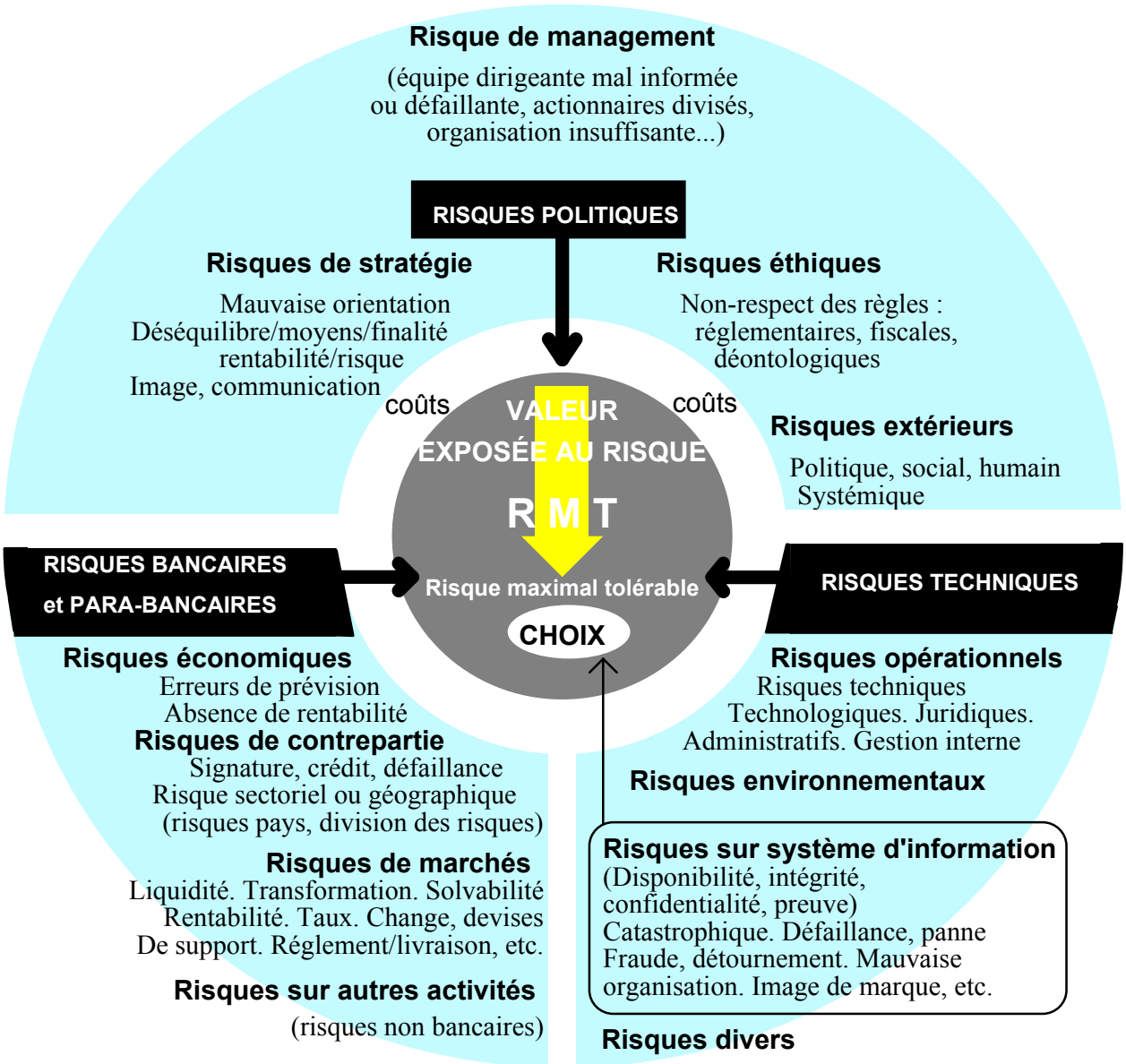
*
* *

Le risque portant sur les systèmes d'information (RSI) n'est **que l'un** des risques auxquels les établissements sont confrontés ; mais c'est **l'un** des risques. Il doit donc être correctement surveillé et géré par les agents désignés et contrôlés par les dirigeants responsables ; ces derniers , in fine, assument les grands arbitrages et la responsabilité face à leurs actionnaires et aux autorités de tutelle et ne peuvent se désintéresser de ce "domaine technique".

Comme tous les autres risques, le risque (RSI) peut faire l'objet d'une même analyse globale en termes de "valeur exposée au risque" ("value at risk"). Tous les risques, une fois évalués, doivent se voir imposer des limites exprimées en termes RMTs (risques maximals tolérables)*, et donc -en fonction des coûts, des contraintes et de la stratégie- faire l'objet de choix (arbitrages, plannings, décisions).

* dont le total doit être inférieur ou égal au risque maximal tolérable affecté par la Direction générale au risque RSI

LA CONSTELLATION DU RISQUE BANCAIRE



LISTE DES ANNEXES

ANNEXE I : Lettre envoyée par le Secrétaire général de la Commission bancaire aux Présidents des Etablissements de crédit

ANNEXE II : Textes réglementaires

ANNEXE III : Questionnaire simplifié (mini-Marion) ; matrice de pondération et tableaux de résultats

ANNEXE IV : Fiches-conseils ; 36 fiches-conseils, par types de risques, classées par ordre alphabétique

ANNEXE V : Les risques, les facteurs de sécurité et les méthodes d'analyse du risque (un exemple)

ANNEXE VI : La prise en compte de la sécurité dans les applications

ANNEXE VII : Exemple de charte de la sécurité de l'information

ANNEXE VIII : Le RSSI : responsable de la sécurité des systèmes d'information ; sa fonction

ANNEXE IX : Méthodes utilisables par le RSSI

ANNEXE X : Nouveau questionnaire

ANNEXE XI : Renseignements pratiques
- éléments bibliographiques
- adresses utiles
- glossaire

ANNEXE XII : Liste des participants au groupe de travail sur le Livre blanc

ANNEXE I

Lettre envoyée par le

Secrétaire général de la Commission bancaire

aux Présidents des Établissements de Crédit

COMMISSION BANCAIRE

LE SECRETAIRE GENERAL

PARIS, LE

73, RUE DE RICHELIEU (2e)

M

Monsieur le Président,

Les modalités de fonctionnement des systèmes d'information des établissements de crédit peuvent avoir des conséquences importantes tant pour leur situation propre que pour le système bancaire dans son ensemble. C'est la raison pour laquelle la Commission bancaire est très attachée à ce que le niveau de sécurité des systèmes informatiques soit périodiquement mesuré et que, le cas échéant, les actions nécessaires à son amélioration soient entreprises.

Les règlements du Comité de la réglementation bancaire n° 90-08 et 91-04 relatifs, respectivement, au contrôle interne ainsi qu'à l'organisation du système comptable et au dispositif du traitement de l'information donnent les grands principes qui doivent présider à la bonne organisation et à la sûreté des systèmes d'information.

Dans cet esprit, la Commission bancaire a procédé à une enquête sur la sécurité informatique dont les résultats complets ont été, d'ailleurs, déjà communiqués aux participants et dont la synthèse a été publiée dans plusieurs revues.

A partir des résultats de cette enquête, la réflexion a été poursuivie en liaison avec la profession et a abouti à la publication par la Commission bancaire d'un "livre blanc" sur la sécurité des systèmes d'information. L'objet de ce document est de présenter l'analyse des principaux risques et les parades possibles ainsi que de formuler des recommandations à destination des établissements de crédit.

L'attention est ainsi appelée sur les principaux problèmes posés par la sécurité des systèmes d'information des établissements de crédit, cette démarche étant d'autant plus utile que la Commission bancaire a parfois l'occasion de constater des insuffisances en ce domaine, préjudiciables au bon fonctionnement des établissements en cause, comme de l'ensemble de la place.

Vous trouverez ci-joint, en annexe, une synthèse du contenu de ce Livre blanc ainsi que son sommaire.

Je vous prie de bien vouloir agréer, Monsieur le Président, l'assurance de ma considération distinguée.

J.-L. BUTSCH

ANNEXE

SYNTHESE DU CONTENU DU LIVRE BLANC SUR LA SECURITE DES SYSTEMES D'INFORMATION

~~~~~~

Les systèmes d'information, et notamment leur support informatique, peuvent constituer une menace financière réelle pour les établissements de crédit.

C'est pourquoi, à la suite d'une enquête menée il y a deux ans auprès d'un échantillon représentatif -et dont les résultats ont été portés à la connaissance de la Profession-, la Commission bancaire a souhaité diffuser un "Livre blanc sur la sécurité des systèmes d'information". Réalisé avec l'aide de la Profession, ce document se veut un guide des meilleures pratiques ou selon la terminologie anglo-saxonne : "a best practice paper".

Le Livre blanc est articulé autour de quatre chapitres : les constats, la mesure du risque, les parades et les recommandations possibles. Onze annexes, dont certaines très détaillées comme les trente-six fiches conseils par type de risque, viennent compléter l'ouvrage qui comporte en tout 230 pages.

Les principaux enseignements que l'on peut en tirer sont les suivants.

La Commission bancaire estime que la définition des objectifs généraux de sécurité incombe à la Direction générale de chaque établissement de crédit. Pour assumer pleinement sa responsabilité, la Direction générale doit connaître avec suffisamment d'exactitude le degré de sûreté de son système d'information, définir le niveau de sécurité qu'elle juge souhaitable par rapport aux exigences des métiers de l'établissement, déterminer les grandes lignes d'une politique de renforcement ou de maintien de la sécurité et se faire rendre compte des résultats des plans d'action qui ont été jugés nécessaires par elle pour les rendre appropriés au degré choisi de sûreté du système d'information de l'établissement. La Direction générale doit également s'assurer que le niveau de sécurité qu'elle a ainsi retenu lui permette d'atteindre ses objectifs malgré la survenance de sinistres ou de dysfonctionnements graves et prolongés. Elle doit avoir, enfin, désigné une ou plusieurs personnes pour mettre en œuvre les modalités pratiques destinées à maintenir ou améliorer la sûreté de son système d'information.

D'une façon plus précise, les questions fondamentales auxquelles il me paraîtrait souhaitable d'apporter une réponse sont les suivantes :

- les objectifs de sécurité informatique de l'établissement sont-ils définis, formalisés et communiqués à tous les collaborateurs concernés ?

- un collaborateur direct a-t-il été désigné pour assumer la fonction de "responsable de la sécurité du système d'information" (RSSI) de la Maison ?

- les points éventuels de vulnérabilité informatique ont-ils été déterminés et les pertes directes ou indirectes qu'ils pourraient occasionner sont-elles mesurées ?

- le "risque maximal tolérable" (RMT), -défini comme la proportion des fonds propres fixée comme limite à ne pas dépasser pour ne pas remettre en cause la pérennité de l'établissement face à un sinistre informatique majeur- est-il connu ?

- dans quel délai d'autres mécanismes de circulation de l'information vous permettraient-ils de reprendre une activité normale, en cas d'indisponibilité durable du système informatique ?

L'objet de ce Livre blanc est de tenter d'aider tous les établissements à apporter des réponses concrètes à ces questions.
~~~~~~

ANNEXE II

Textes réglementaires

- Règlement du CRB n° 90-08
- Règlement du CRB n° 91-04
- Directive sur les Services d'Investissement (extraits)

RÈGLEMENT N° 90-08 DU 25 JUILLET 1990
relatif au contrôle interne

Article 1er. - Les établissements de crédit et les maisons de titres, ci-après désignés les établissements assujettis, doivent se doter d'un système de contrôle interne dans les conditions prévues par le présent règlement.

Le système de contrôle interne a notamment pour objet de :

a) vérifier que les opérations réalisées par l'établissement, ainsi que l'organisation et les procédures internes sont conformes aux dispositions législatives et réglementaires en vigueur, aux normes et usages professionnels et déontologiques et aux orientations de l'organe exécutif ;

b) vérifier que les limites fixées en matière de risques, notamment de contrepartie, de change, de taux d'intérêt ainsi que d'autres risques de marché, sont strictement respectées ;

c) veiller à la qualité de l'information comptable et financière, en particulier aux conditions d'enregistrement, de conservation et de disponibilité de cette information.

Pour l'application du présent règlement, on entend par :

a) organe exécutif : l'ensemble des personnes qui, conformément à l'article 17 de la loi du 24 janvier 1984 susvisée, assurent la détermination effective de l'orientation de l'activité de l'établissement ;

b) organe délibérant :

- le conseil d'administration, le conseil de surveillance ou les gérants pour les sociétés régies par la loi du 24 juillet 1966 susvisée ;

- le conseil d'administration pour les caisses de crédit agricole régies par le Livre V du Code rural, pour les banques populaires et les sociétés de caution mutuelle régies par la loi du 13 mars 1917 susvisée et pour les caisses de crédit mutuel régies par la loi du 10 septembre 1947 susvisée ;

- le conseil d'orientation et de surveillance pour les caisses d'épargne ;

- le conseil d'administration ou le conseil de surveillance pour les établissements publics ;

- le conseil d'administration, le conseil de surveillance ou l'organisme collégial qui a notamment la charge de surveiller, pour le compte des apporteurs de capitaux, la gestion et la situation de l'établissement dans le cas des établissements ayant une autre forme juridique.

Article 2. - L'information comptable et financière visée au c) du 2ème alinéa de l'article 1er ci-dessus, dont le contenu varie selon le destinataire, comprend :

- celle qui est destinée à l'organe exécutif et à l'organe délibérant ;
- celle qui est transmise aux autorités de tutelle et de contrôle ;
- celle qui figure dans les documents destinés à être publiés.

En ce qui concerne l'information comprise dans les comptes publiés, le système de contrôle interne doit garantir l'existence d'un ensemble de procédures, appelé piste d'audit, qui permet :

a) de reconstituer dans un ordre chronologique les opérations ;

b) de justifier toute information par une pièce d'origine à partir de laquelle il doit être possible de remonter par un cheminement ininterrompu au document de synthèse et réciproquement ;

c) d'expliquer l'évolution des soldes d'un arrêté à l'autre par la conservation des mouvements ayant affecté les postes comptables.

Les informations comptables qui figurent dans les situations destinées à la Commission bancaire, ainsi que celles qui sont nécessaires au calcul des normes de gestion établies en application de l'article 33-6° de la loi du 24 janvier 1984 susvisée, doivent respecter, au moins, les deux premiers aspects a) et b) de la piste d'audit. Dans ce cas, les éléments constitutifs de la piste d'audit relatifs à l'arrêté périodique le plus récent et au dernier calcul de chacune des normes de gestion sont conservés.

Article 3. - Les établissements assujettis élaborent et tiennent à jour un document qui précise les objectifs du contrôle interne et les moyens destinés à assurer cette fonction. L'organisation de la fonction de contrôle interne peut associer à celui-ci des personnes autres que les employés de l'établissement, notamment des membres de l'organe délibérant au sens de l'article 1er ci-dessus. En outre les établissements assujettis désignent un responsable chargé d'évaluer la cohérence et l'efficacité du système de contrôle interne.

Au moins une fois par an, les établissements assujettis élaborent un rapport sur les conditions dans lesquelles le contrôle interne est assuré. Ce rapport est communiqué aux commissaires aux comptes et, sur sa demande, à la Commission bancaire.

Au moins une fois par an, l'organe délibérant procède à l'examen de l'activité et des résultats du contrôle interne sur la base des informations qui lui sont transmises à cet effet par l'organe exécutif.

Lorsque la taille de l'établissement ne justifie pas de confier à une personne spécialement désignée l'exercice de la fonction de contrôle interne, l'organe exécutif peut assurer lui-même cette fonction.

Article 4. - Lorsqu'un établissement appartient à un groupe au sens de l'article 2 du règlement n° 85-12 modifié susvisé, l'exercice de la fonction de contrôle interne de cet établissement peut être assuré par un autre établissement du même groupe après accord des organes sociaux compétents des deux établissements concernés. Dans ce cas, le rapport visé au 2ème alinéa de l'article 3 ci-dessus est communiqué à ces deux établissements ainsi qu'à l'entreprise mère du groupe.

Lorsqu'un établissement est affilié à un organe central, la fonction de contrôle interne de cet établissement est organisée en accord avec l'organe central. Le rapport visé au 2ème alinéa de l'article 3 ci-dessus est également communiqué à l'organe central.

Article 5. - Le présent règlement entre en vigueur le 1er janvier 1991.

RÈGLEMENT N° 91-04 DU 16 JANVIER 1991
concernant l'organisation du système comptable et du dispositif de traitement de l'information des établissements de crédit et des maisons de titres

Article 1er. - Les établissements de crédit et les maisons de titres ci-après dénommés établissements assujettis organisent leur système comptable et leur dispositif de traitement de l'information conformément aux dispositions du présent règlement.

Article 2. - Les établissements assujettis doivent respecter les dispositions des articles 1 à 6 du décret n° 83-1020 susvisé, en tenant compte des précisions ci-après :

a) Les soldes des comptes qui figurent dans le plan de comptes prescrit à l'article 4 du décret précité se raccordent, par voie directe ou par regroupement, aux postes et sous-postes du bilan et du compte de résultat ainsi qu'aux informations contenues dans l'annexe ; par exception, le solde d'un compte peut être raccordé par éclatement, à condition de pouvoir en justifier, de respecter les règles de sécurité et de contrôle adéquates et de décrire la méthode utilisée dans le document prescrit à l'article 1 du décret précité ;

b) Chaque montant figurant dans les situations, dans les tableaux annexes, dans les déclarations relatives aux normes de gestion et dans les autres documents remis à la Commission bancaire doit être contrôlable, notamment à partir du détail des éléments qui composent ce montant.

Article 3. - Le contrôle des systèmes d'information s'étend à la documentation relative aux analyses, à la programmation et à l'exécution des traitements.

Article 4. - Les établissements assujettis sont tenus de conserver, jusqu'à la date de l'arrêté suivant, l'ensemble des fichiers nécessaires à la justification des documents du dernier arrêté remis à la Commission bancaire.

Article 5. - Les éléments détenus par l'établissement pour le compte de tiers, mais ne figurant pas dans les comptes individuels annuels, doivent faire l'objet d'une comptabilité ou d'un suivi matière retraçant les existants, les entrées et les sorties.

Une distinction est faite entre les éléments détenus pour le compte des organismes de placement collectif en valeurs mobilières (OPCVM) et pour celui de la clientèle ; parmi ces derniers, une répartition est effectuée, si elle significative, entre les éléments détenus à titre de simple dépositaire et ceux qui garantissent, soit un crédit accordé, soit un engagement pris, à des fins spécifiques ou en vertu d'une convention générale et permanente, en faveur du déposant.

Article 6. - Le présent règlement est applicable aux exercices ouverts postérieurement au 31 décembre 1992.

EXTRAITS DE LA DIRECTIVE SUR LES SERVICES D'INVESTISSEMENT
N° 93/22/CEE du Conseil du 10 mai 1993

Article 10. :

"[...] Ces règles obligent notamment [...] :

- à avoir une bonne organisation administrative et comptable, des mécanismes de contrôle et de sécurité dans le domaine informatique[36], ainsi que des procédures de contrôle interne adéquates [...]".

En application des dispositions de la Directive européenne relative aux services d'investissement, la transposition de ces principes -qui concernent les mécanismes de contrôle de sécurité dans le domaine informatique- pourrait être prochainement l'occasion de les préciser.

36 souligné par nous

ANNEXE III

3.1. Questionnaire simplifié (mini-Marion) d'analyse du niveau de sécurité informatique

3.2. Matrice de pondération

3.3. Principaux résultats trouvés lors de l'enquête menée par le S.G.C.B. en 1991/1992

3.1. QUESTIONNAIRE SIMPLIFIÉ

QUESTIONNAIRE 1
Évaluation des enjeux

(à servir par la Direction Générale et/ou le Secrétariat Général)

RISQUE MAXIMAL TOLÉRABLE (RMT)

Quel est le montant maximal (en kF) du risque[37] créé par un sinistre d'origine informatique pouvant être supporté par votre entreprise sans mettre en cause la continuité de ses opérations ?

MONTANT :_____KF

37 Voir définition du RMT pages 16 et 25 et pages ci-après (61 et 62).

LE RISQUE MAXIMAL TOLÉRABLE (RMT)[38]

C'est aux dirigeants responsables d'assumer la responsabilité du choix de cette limite importante qu'est le RMT.

Toutefois, si la détermination fine du montant du RMT peut s'avérer délicate, on peut dans un premier temps n'en procéder qu'à une approximation fruste. En effet, tant pour les dirigeants que pour la Commission bancaire, le fait de se poser la question -c'est-à-dire de procéder à cette démarche de fixation d'une limite- est plus importante que le résultat lui-même. Ceci ne veut, bien sûr, pas signifier que le niveau du RMT retenu soit indifférent mais qu'on peut trouver des approximations simples.

Si, donc, définir le RMT est "politiquement" et "techniquement" important, son calcul approché n'est pas compliqué. D'ailleurs, cette analyse en termes de RMT peut, -plus, devrait-être utilisée pour tous les risques de la banque (cf. "la constellation" du risque bancaire page 43). Les activités de marché ont popularisé ce concept sous le nom de limite maximale de la valeur exposée au risque ou "VALUE AT RISK".

1. Pourquoi la détermination du RMT est-elle importante ?

   a. Pour sensibiliser la Direction générale, l'obliger à s'impliquer, la contraindre à arbitrer. Cette notion de valeur au risque à laquelle elle est maintenant familiarisée, permet dans un langage compréhensible pour elle, de "mesurer" les coûts/avantages des actions de sécurité à mener (et du risque à ne pas les mener).

   Ce qui permet une démarche rationnelle.

   b. Techniquement, en effet, le RMT sera le "juge de paix" des bilans actualisés trouvés en utilisant les équations de risque. Dans un monde incertain, celui du risque, seule la fixation de limites permet des arbitrages.

2. Comment définir son RMT ? (RMTi = partie du RMT global de la banque réservé à l'informatique)

La relation suivante permet de le faire :

RMTi = , Fonds Propres + - Bénéfice + . Assurances

C'est le rôle des fonds propres de combler les pertes ; ce stock des richesses détenues en propre par la banque peut s'accroître d'une partie des bénéfices de l'année (ou du Résultat courant avant impôt RCAI). La marge de manœuvre peut enfin augmenter soit de la certitude que l'on a que des ressources extérieures seront disponibles (subventions, actionnaires, fonds de garantie...) soit surtout de la probabilité d'être remboursé par son assurance en cas de sinistre.

38 Ou, plus précisément, RMTi : partie du RMT attribuée au risque des systèmes d'information.

Les parts α, β, γ qui permettent de calculer le RMTi et qui sont toutes inférieures à 1, doivent être évaluées :

- La part α des fonds propres[39] dépend de la proportion qui sera allouée au risque du système d'information (RSI) parmi l'ensemble des risques et de l'aversion au risque témoignée par la Direction générale ; aussi , pourrait-elle se situer entre 5 % et 50 %. Toutes les catastrophes ne se produisant pas au même moment[40], on peut accorder au RSI environ 20 %.

- La part β pourrait aller de 30 à 50 % du RCAI (ou, si la banque est plus conservatrice, du Bénéfice net). Le chiffre - = 30 % est proposé.

- Enfin, la part γ dépend de la probabilité globale d'être remboursé ce qui dépend avant tout :

    - du degré de couverture effectif par les assurances qu'on a prises,

    - de la probabilité de remboursement par les assurances (notamment en fonction des limites, des franchises...)[41].

Une estimation type tourne autour de 50 à 90 %. Le chiffre de γ = 80 % est suggéré.

Soit, au total, la relation suivante :

$$RMTi = 0,2\ FP + 0,3\ BENEF. + 0,8\ ASSURANCE$$

qui si elle est encore trouvée trop compliquée, peut se simplifier en :

$$RMTi = FP / 4$$

Mais encore une fois, si ces relations sommaires permettent d'esquiver la question, une partie de la démarche aura perdu de son intérêt. Il est particulièrement instructif pour une Direction générale de réfléchir à l'articulation des limites pour les différents risques au sein du RMT afin d'en assurer la cohérence en fonction de sa stratégie.

---

39 Au sens du ratio de solvabilité de la Commission bancaire (RSE ; modèle 4008).

40 Il est possible que la somme des parts attribuées aux multiples risques dépasse le RMT si l'on sait évaluer ce dépassement par une démarche probabiliste de type "bayésien" : probabilité de B si A n'arrive pas. Cette sur-utilisation des fonds propres ou "overbooking" (qui peut tenir compte des corrélations existant entre les probabilités d'apparition des différents risques à un instant donné et sur la période d'observation retenue pour estimer les probabilités moyennes) doit demeurer prudente.

41 Ceci plaide en faveur d'assurances du type "TOUT SAUF".

QUESTIONNAIRE 2
Évaluation du Niveau de Sécurité

(à servir par la Direction de l'Informatique)

Cette partie de l'enquête s'appuie sur une formulation réduite d'un questionnaire d'audit mis au point par l'A.P.S.A.D. (Assemblée Plénière des Sociétés d'Assurance Dommages) et le CLUSIF (Club de la Sécurité Informatique Français) dans le cadre de la Méthodologie d'Analyse des Risques Informatiques et d'Optimisation par Niveau (MARION).

Ce questionnaire inspiré de MARION Etape 3, mais fortement réduit ici, est destiné à évaluer la sécurité de 27 facteurs caractéristiques regroupés sous 6 chapitres :

❶ Appréciation Générale de la sécurité de l'entreprise,

❷ Facteurs sociaux-économiques,

❸ Principes généraux de la sécurité informatique,

❹ Sécurité du matériel et du logiciel de base,

❺ Sécurité de l'exploitation informatique,

❻ Sécurité des études et des réalisations informatiques.

Chaque question est caractérisée par un numéro, un libellé et une réponse. On portera dans les cases **Réponses** une cotation sur 4 points (la cote 0 ne repère que l'absence d'objet) :

0	***Néant***	**3**	***Assez Bon***
1	***Mauvais***	**4**	***Bon***
2	***Médiocre***		

Lorsqu'une question est sans objet pour motif technique, noter 0 et l'indiquer dans le cartouche **Observations**.

Pour faciliter le rapprochement avec le questionnaire MARION, la référence d'origine est indiquée entre parenthèses.

QUESTIONNAIRE SÉCURITÉ INFORMATIQUE

① Appréciation Générale de la Sécurité de l'Entreprise

Préambule[42]

QUESTION A

Votre établissement est-il sensible aux risques (et aux conséquences) liées à l'informatique ?

Réponse OUI ☐ NON ☐

Observations :

QUESTION B

Pour vous, l'Informatique est-elle un facteur stratégique de pérennité et de développement de votre activité ?

Réponse OUI ☐ NON ☐

Observations :

QUESTION C

Connaissez-vous des méthodes d'appréciation et d'évaluation des risques liés à l'informatique (MARION, AROME, MELISA, CRAMM) ?

Réponse OUI ☐ NON ☐

Observations :

QUESTION D

Au cours des 3 dernières années, votre établissement a-t-il subi un préjudice, conséquence d'un dommage informatique (accident matériel ou applicatif, erreurs ou malveillance) ?

Réponse OUI ☐ NON ☐

Observations :

42 Questions non référencées dans le questionnaire MARION

á <u>Organisation générale</u>

QUESTION 1 **(MARION 1-06)**

Existe-t-il un Comité Permanent chargé des problèmes liés à la sécurité, composé de représentants de la Direction Générale, de la Direction de l'Organisation et de l'Informatique, de représentants des fonctions utilisateurs, audit interne, juridique et assurances se réunissant au moins 4 fois par an ?

Réponse : (1 à 4) ☐

<u>Observations :</u>

QUESTION 2 **(MARION 1-09)**

Y-a-t-il eu une étude sur la vulnérabilité de l'entreprise face à différents risques physiques ou non physiques incluant le risque informatique au cours des 3 dernières années, donnant lieu à un rapport écrit ?

Réponse : (1 à 4) ☐

<u>Observations :</u>

QUESTION 3 **(MARION 1-10)**

Cette étude a-t-elle entraîné la mise en place d'un Plan de Sauvegarde de l'entreprise (mesures conservatoires incluant celles financières) ?

Réponse : (1 à 4) ☐

<u>Observations :</u>

QUESTION 4 **(MARION 1-12)**

La fonction "Sécurité informatique" dispose-t-elle d'un poste spécifique sur l'organigramme avec un rattachement hiérarchique élevé assorti d'une définition de poste précisant les responsabilités et l'affectation d'un budget spécifique ?

Réponse : (1 à 4) ☐

<u>Observations :</u>

QUESTION 5 **(MARION 1-11)**

Y-a-t-il un responsable de la Sécurité Générale (bâtiments, environnement, accès) ?

Réponse : (1 à 4) ☐

Observations :

QUESTION 6 **(MARION 1-14)**

Le choix des garanties des polices d'assurances en matière informatique est-il le résultat d'une étude spécifique conduite en commun avec la Direction de l'Informatique ?

Réponse : (1 à 4) ☐

Observations :

QUESTION 7 **(MARION 1-19)**

Le(s) Système(s) Informatique(s) est-il couvert par un contrat incluant :

- les dommages matériels,
- la reconstitution des médias,
- d'autres contrats liés au précédent (Globale Informatique, Spécifique détournement, Multirisques professionnelles) ?

Réponse : (1 à 4) ☐

Observations :

② **Les Contrôles permanents**

QUESTION 8 **(MARION 2-27)**

Existe-t-il un "propriétaire des informations" par fonction, responsable de l'évaluation, de la classification des biens, de la définition et la révision périodique des règles, et des procédures et autorisations d'utilisation des informations ?

Réponse : (1 à 4) ☐

Observations :

QUESTION 9 **(MARION 2-28)**

Y-a-t-il une étude particulière, lors de la conception des applications, sur le choix des contrôles automatisés et utilisateurs en amont et en aval de l'informatique ?

Réponse : (1 à 4) ☐

Observations :

QUESTION 10 **(MARION 2-29)**

Cette étude prend-elle en compte les critères d'analyse et de réduction des risques issus d'informations ou de traitements classés comme stratégiques ?

Réponse : (1 à 4) ☐

Observations :

QUESTION 11 **(MARION 2-33)**

Y-a-t-il une analyse des comptes comptables sensibles au moins 2 fois par an, les résultats étant consignés dans un rapport ?

Réponse : (1 à 4) ☐

Observations :

③ La réglementation et l'audit

QUESTION 12 **(MARION 3-36)**

Existe-t-il un règlement écrit précisant les responsabilités des personnes et la procédure de signature selon le type de document traité ?

Réponse : (1 à 4) ☐

Observations :

QUESTION 13 **(MARION 3-40)**

A-t-on pris en compte la possibilité de destruction d'informations stratégiques sur support informatique et en a-t-on déduit des procédures systématiques de rétention des documents de base qui pourraient servir à leur reconstitution ?

Réponse : (1 à 4) ☐

Observations :

QUESTION 14 **(MARION 3-44)**

S'il existe un service d'Audit interne, a-t-il des compétences pour exercer le contrôle de la fonction informatique ?

Réponse : (1 à 4) ☐

Observations :

④ Facteurs sociaux économiques

QUESTION 15 **(MARION 4-57)**

A-t-on le sentiment que le climat social est correct et qu'il n'y a pas à redouter d'action malveillante ?

Réponse : (1 à 4) ☐

Observations :

QUESTION 16 **(MARION 4-56)**

Le Turn-over moyen des personnels des services informatiques, sur les 3 dernières années, est-il compris entre 5 et 15% ?

Réponse : (1 à 4) ☐

Observations :

⑤ Principes généraux de la sécurité informatique

- **L'environnement de base**

QUESTION 17 **(MARION 5-59)**

Y a-t-il eu des études contrôlées périodiquement par des organismes spécialisés, sur les dangers présentés par des facteurs externes, sur le bâtiment renfermant des locaux informatiques avec un suivi des recommandations prescrites ?

Réponse : (1 à 4) ☐

Observations :

QUESTION 18 **(MARION 6-98)**

Existe-t-il un système (automatique ou gardiennage) de contrôle d'accès systématique aux bâtiments renfermant les locaux informatiques ?

Réponse : (1 à 4) ☐

Observations :

QUESTION 19 **(MARION 6-106)**

Y a-t-il un système automatique de contrôle d'accès systématique aux salles des ordinateurs ?

Réponse : (1 à 4) ☐

Observations :

- **Les consignes**

QUESTION 20 **(MARION 8-141)**

Y a-t-il des consignes de sécurité physique spécifiques aux risques liés à l'informatique (incendie, dégâts des eaux, etc) différenciées par type de local et par type de risque, et correctement affichées ?

Réponse : (1 à 4) ☐

Observations :

- **La protection incendie**

QUESTION 21 **(MARION 9-145)**

Pour le bâtiment renfermant des locaux informatiques et administratifs, y a-t-il eu une étude spécifique du risque incendie prenant en compte les aspects protection et prévention avec un suivi des recommandations prescrites ?

Réponse : (1 à 4) ☐

Observations :

- **Les dégâts des eaux**

QUESTION 22 **(MARION 10-188)**

Y a-t-il eu des études contrôlées périodiquement (suivies d'effets) par un organisme spécialisé sur les dangers présentés par l'eau sur les salles des ordinateurs et les matériels d'environnement ?

Réponse : (1 à 4) ☐

Observations :

- **L'amélioration de la fiabilité de fonctionnement**

QUESTION 23 **(MARION 11-203)**

Y a-t-il une redondance réelle locale des unités centrales des ordinateurs et des organes stratégiques (contrôleurs) et repose-t-elle sur un plan de basculement écrit ?

Réponse : (1 à 4) ☐

Observations :

QUESTION 24 **(MARION 11-209)**

Y a-t-il un système complémentaire (groupe électrogène) et un système de régulation (onduleur) de l'alimentation électrique ?

Réponse : (1 à 4) ☐

Observations :

- **Les systèmes et procédures de secours**

QUESTION 25 **(MARION 12-237)**

Y a-t-il un site de secours (salle blanche, contrat de "back-up", SSII, ...) strictement réservé au site étudié ?

Réponse : (1 à 4) ☐

Observations :

QUESTION 26 **(MARION 12-251)**

La solution de secours est-elle testée au moins 4 fois par an ?

Réponse : (1 à 4) ☐

Observations :

QUESTION 27 **(MARION 12-222)**

Dans le cas d'un sauvetage exhaustif de toutes les applications a-t-on étudié les besoins globaux, la planification de la charge et les contraintes techniques et organisationnelles ?

Réponse : (1 à 4) ☐

Observations :

QUESTION 28 **(MARION 12-220)**

Dans le cas d'un sauvetage partiel ou en mode dégradé, a-t-on étudié le choix des applications à reprendre en fonction de leur degré stratégique ?

Réponse : (1 à 4) ☐

Observations :

- **Les protocoles utilisateurs-informaticiens**

QUESTION 29 **(MARION 13-258)**

Les Comités Informatiques ou Sécurité font-ils obligation qu'il y ait un chapitre sûreté des systèmes d'information dans chaque document (avant-projet, cahier des charges, dossier applicatif) relatif à une étude informatique ?

Réponse : (1 à 4) ☐

Observations :

QUESTION 30 **(MARION 13-261)**

Y a-t-il un protocole de liaison utilisateurs-informaticiens défini par le Comité Informatique précisant le partage des responsabilités dans les domaines suivants:

- les moyens infocentre et leurs limites,
- les micro-ordinateurs libres et leurs limites,
- les micro-ordinateurs connectés à l'ordinateur central ou à des serveurs de données,
- la conception des applications (élaboration du cahier des charges),
- les jeux d'essai et les recettes,
- les demandes de maintenance,
- les soumissions de travaux (en local ou à distance),
- le mode dégradé (plan de secours) ?

Réponse : (1 à 4) ☐

Observations :

- **Le personnel informatique**

QUESTION 31 **(MARION 14-273)**

Le taux de maintenance des études (charge ponctuelle < 1 mois/homme) exprimé en mois/hommes, est-il inférieur à 35% ?

Réponse : (1 à 4) ☐

Observations :

QUESTION 32 **(MARION 14-274)**

La formation du personnel informatique (hors saisie de données), en moyenne sur les 3 dernières années, est-elle supérieure à 5 jours par an et par personne ?

Réponse : (1 à 4) ☐

Observations :

QUESTION 33 **(MARION 14-282)**

Y a-t-il une répartition, un contrôle et un suivi des tâches stratégiques et/ou confidentielles ?

Réponse : (1 à 4) ☐

Observations :

- **Le Plan Informatique**

QUESTION 34 **(MARION 15-292)**

Y a-t-il un Plan Informatique glissant à moyen terme (2 à 5 ans), tenu à jour et approuvé chaque année par le Comité Informatique incluant :

- l'analyse des besoins (données, traitements),
- l'analyse de l'existant,
- l'analyse des contraintes,
- le plan des moyens (logiciel, matériel, personnel),
- le planning et les priorités,
- le plan de sécurité,
- le budget complet ?

Réponse : (1 à 4) ☐

Observations :

- **Fiabilité des matériels et des logiciels de base**

QUESTION 35 **(MARION 16-231)**

Y a-t-il un seul responsable -titulaire de la fonction- de la gestion et de la mise en place des droits d'accès ?

Réponse : (1 à 4) ☐

Observations :

- **Sécurité des Télécommunications et Protection complémentaire des données**

QUESTION 36 **(MARION 17-325)**

Le progiciel de contrôle d'accès prend-il en compte tous les accès locaux et à distance sans exception (y compris le vidéotex) ?

Réponse : (1 à 4) ☐

Observations :

QUESTION 37 **(MARION 17-326)**

Existe-t-il un système d'identification et d'authentification par mot de passe (ou carte) pour chaque utilisateur ?

Réponse : (1 à 4) ☐

Observations :

QUESTION 38 **(MARION 17-342)**

Y a-t-il protection et surveillance du matériel de télécommunications (unités, contrôleurs, modems, têtes de lignes,...) dans des locaux isolés et protégés ?

Réponse : (1 à 4) ☐

Observations :

QUESTION 39 **(MARION 17-359)**

Les virements et opérations financières télématiques, les transferts d'informations stratégiques ou confidentielles sont-ils uniquement supportés par des réseaux professionnels spécifiques (type SWIFT) ?

Réponse : (1 à 4) ☐

Observations :

QUESTION 40 **(MARION 18-367)**

Y a-t-il un administrateur de données responsable :

- de la définition de la sémantique des données,
- de l'élaboration et de la mise à jour du dictionnaire de données,
- de la mise en place, des modifications et de la surveillance de la structure des fichiers et bases de données ?

Réponse : (1 à 4) ☐

Observations :

QUESTION 41 **(MARION 19-377)**

Y a-t-il des procédures écrites concernant l'archivage/désarchivage spécifiques à chaque type de support et tenant compte de la classification des informations ?

Réponse : (1 à 4) ☐

Observations :

- **Sauvegardes**

QUESTION 42 **(MARION 21-410)**

Y a-t-il une procédure de sauvegarde périodique, dite de Très Haute Sécurité, pour les programmes et fichiers stratégiques ?

Réponse : (1 à 4) ☐

Observations :

QUESTION 43 **(MARION 21-404)**

Y a-t-il au moins une sauvegarde systématique (une génération) stockée dans des locaux hautement sécurisés et physiquement distincts des salles machines ?

Réponse : (1 à 4) ☐

Observations :

QUESTION 44 **(MARION 21-414)**

Y a-t-il des procédures de reprise automatique des applications en cas d'interruption accidentelle de l'exploitation (points de reprise, journal image avant, ...) ?

Réponse : (1 à 4) ☐

Observations :

QUESTION 45 **(MARION 21-418)**

Possède-t-on une sauvegarde de la documentation des études et de la documentation d'exploitation dans des locaux externes à l'entreprise et protégés.

Réponse : (1 à 4) ☐

Observations :

- **Suivi de l'exploitation**

QUESTION 46 **(MARION 22-441)**

L'exploitation repose-t-elle sur des procédures cataloguées dont l'accès est limité et contrôlé ?

Réponse : (1 à 4) ☐

Observations :

QUESTION 47 **(MARION 22-401)**

Y a-t-il une procédure de contrôle de tous les rapports d'activité des travaux exécutés ?

Réponse : (1 à 4) ☐

Observations :

QUESTION 48 **(MARION 22-446)**

Y a-t-il une documentation d'exploitation complète et mise à jour pour l'ensemble des applications ?

Réponse : (1 à 4) ☐

Observations :

- **La Maintenance**

QUESTION 49 **(MARION 23-456)**

Y a-t-il des contrats de maintenance incluant des engagements d'intervention pour tous les matériels dont la réparation ou le remplacement ne pourrait se faire dans des délais acceptables ?

Réponse : (1 à 4) ☐

Observations :

- **Les Procédures de révision**

QUESTION 50 **(MARION 24-483)**

Y a-t-il des procédures écrites de révision (protocoles de recettes) appliquées systématiquement, avant la mise en exploitation, pour toute création ou maintenance d'une application ?

Réponse : (1 à 4) ☐

Observations :

- **Les Méthodes d'Analyse-Programmation**

QUESTION 51 **(MARION 25-509)**

Chaque projet fait-il l'objet d'un avant-projet et d'un cahier des charges cosigné par le service informatique et le service utilisateur ?

Réponse : (1 à 4) ☐

Observations :

QUESTION 52 **(MARION 25-513)**

Y a-t-il et applique-t-on une méthodologie d'analyse fonctionnelle, d'analyse organique et de programmation ?

Réponse : (1 à 4) ☐

Observations :

QUESTION 53 **(MARION 25-522)**

Dispose-t-on et utilise-t-on un dictionnaire de données exhaustif ?

Réponse : (1 à 4) ☐

Observations :

- **Les Contrôles Programmés**

QUESTION 54 **(MARION 26-535)**

Y a-t-il eu au moment de l'analyse fonctionnelle des applications stratégiques une étude quantitative des conséquences d'accident, d'erreurs ou d'action volontaire malveillante sur chaque type de données stratégiques (rapport écrit) ?

Réponse : (1 à 4) ☐

Observations :

QUESTION 55 **(MARION 26-537)**

Cette étude (Cf. 54) a-t-elle permis un classement des données en fonction de leur "poids stratégique" ?

Réponse : (1 à 4) ☐

Observations :

QUESTION 56 **(MARION 26-543)**

Disposez-vous pour chaque donnée stratégique de tableaux croisés contrôles-programmes afin de vérifier la cohérence des contrôles dans tous les programmes utilisant cette donnée ?

Réponse : (1 à 4) ☐

Observations :

QUESTION 57 **(MARION 26-549)**

Pour les données stratégiques, y a-t-il des contrôles de vraisemblance ou de cohérence (évolution par rapport à une base historique ou statistique) ?

Réponse : (1 à 4) ☐

Observations :

QUESTION 58 **(MARION 26-556)**

Y a-t-il un audit périodique (interne ou externe) portant au minimum sur la conformité des contrôles programmés (batch et TP) des applications stratégiques ?

Réponse : (1 à 4) ☐

Observations :

- **Micro informatique et réseaux de micros**

QUESTION 59 **(MARION MICRO 1-66)**

Existe-t-il un chapitre micro-informatique dans le Plan Informatique (évolution des matériels, cohérence, compatibilité, connexions aux systèmes centraux, logiciels, budgets, ...) incluant les aspects sécurité ?

Réponse : (1 à 4) ☐

Observations :

QUESTION 60 **(MARION 26-537)**

La Direction Informatique propose-t-elle une information, des moyens centraux de sauvegarde et des outils de détection et de lutte contre le sabotage immatériel sur les micro-ordinateurs (virus) ?

Réponse : (1 à 4) ☐

Observations :

QUESTIONNAIRE 3
Éléments d'appréciation du coût de l'informatique

(à remplir par la Direction Comptable ou la Direction de l'Informatique)

Nom de l'établissement : .....

C.I.B. : .....

Nom de la personne ayant rempli : .....

Qualité/fonction : .....

Téléphone : .....

BUDGET INFORMATIQUE

		Dépenses 1991 (kF)	Dépenses 1993 (kF)	Prévisions 1994
Direction de l'organisation et/ou Direction de l'Informatique		**N - 2**	**N**	**N + 1**
FRAIS GÉNÉRAUX				
Charges diverses de personnel	*C18*			
Formation Professionnelle	*C19*			
Loyers ou amortissements				
des locaux professionnels	*C20*			
des matériels informatiques	*C21*			
des logiciels informatiques	*C22*			
Entretien des locaux et des installations techniques	*C23*			
Entretien des matériels informatiques	*C24*			
Travaux à façon facturés (dépenses)	*C25*			
Travaux à façon à déduire (recettes)	*C26*			
Rémunération des conseils extérieurs	*C27*			
Liaisons informatiques	*C28*			
Fournitures informatiques	*C29*			
FRAIS DIVERS DE GESTION	*C30*			
Fonctions informatiques décentralisées				
INFRASTRUCTURE DE PRODUCTION				
Centre technique informatique	*C31*			
Organisation Administrative	*C32*			
Travaux à façon	*C33*			
ÉQUIPEMENTS LOCAUX				
Processeurs intermédiaires	*C34*			
Terminaux	*C35*			
Traitement des chèques	*C36*			
TÉLÉCOMMUNICATIONS	*C37*			
TESTS & DÉVELOPPEMENTS	*C38*			
DÉCENTRALISATION				
Micro-informatique :				
Investissement annuel	*C39*			
Formation	*C40*			
Maintenance	*C41*			
AUTOMATES (GAB)	*C42*			

ESTIMATION DES DÉPENSES CONSACRÉES À LA SÉCURITÉ INFORMATIQUE

TYPE DE DÉPENSE		MONTANT 1989 (KF)	MONTANT 1990 (KF)	PRÉVISION 1991 (KF)
ORGANISATION, AUDITS (poste de responsable sécurité, audits externes et internes)	C1			
SÉCURITÉ PHYSIQUE (Environnement de base, contrôle des accès, pollution, sécurité incendie et dégâts des eaux)	C2			
PLANS ET MOYENS DE SECOURS (Back-up, salle blanche...)	C3			
SÉCURITÉ DES ACCÈS LOGIQUES (progiciels de contrôle d'accès)	C4			
SÉCURITÉ DES TÉLÉCOMMUNICATIONS (chiffrement, authentification, coût de la redondance des unités de télécommunications)	C5			
SÉCURITÉ D'EXPLOITATION (archivage, procédures de transfert des données, sauvegardes, outils d'automatisation...)	C6			
SÉCURITÉ DES ÉTUDES ET RÉALISATIONS (méthode d'analyse-programmation, audit-trail...)	C7			
ASSURANCES (montant annuel des primes)	C8			
AUTRES (à préciser)	C9			

ÉVALUATION DES «COUVERTURES» ASSURANCE

		MONTANT ASSURÉ (KF)	MONTANT FRANCHISE (KF)	MONTANT PRIME (1990)
POLICE GLOBALE INFORMATIQUE	C10			
GLOBALE DE BANQUE Transports de fonds Coffres Détournements	C11			
EXTENSION AUX RISQUES INFORMATIQUES Pertes de fonds Pertes de biens Détournements Sabotage immatériel	C12			
GARANTIES SPÉCIALES ERI Pertes d'exploitation sur informations (perte d'intégrité) Pertes d'exploitation sur utilisation non autorisée de ressources informatiques	C13			
PERTES D'EXPLOITATION SUR DOMMAGES MATÉRIELS	C14			
MULTIRISQUE INCENDIE	C15			
TOUS RISQUES INFORMATIQUES Dommages matériels Frais supplémentaires d'exploitation Reconstitution des informations	C16			
GARANTIES SPÉCIALES de personnes ; Homme clé informatique de moyens ; Back up de bonne fin de projet Assurance + maintenance	C17			

Cet état doit être servi de façon exclusive et non redondante,
c'est-à-dire en cumulant les risques sur une même police
et en veillant à ne pas porter le même risque plusieurs fois

QUESTIONNAIRE 4
Appréciation de l'efficacité et de la performance de l'informatique

Première partie

(à remplir par la Direction de l'Informatique)

Deuxième partie (les critères d'appréciation)

(à remplir par la Direction Générale et les principaux utilisateurs)

Cette partie de l'enquête s'appuie sur un ensemble de questions permettant de "situer" la prestation informatique de l'établissement en la rapportant soit à des objectifs prédéfinis, soit à des références statistiques.

LA DIRECTION INFORMATIQUE

1. Les effectifs :

Les effectifs développement et exploitation en nombre d'agents :

Secteurs d'activité	*nombre d'agents*
Exploitation (y compris système & réseau)	
Développement	
Divers	

2. Le rattachement hiérarchique :

La Direction de l'Informatique est-elle directement rattachée à :

- ❍ *Direction Générale*
- ❍ *Direction Financière*
- ❍ *Direction Administrative*
- ❍ *Secrétariat Général*
- ❍ *Autre (précisez) :*_____

3. Participation du Responsable informatique au Comité de Direction :

Le responsable informatique participe-t-il au Comité de Direction ? ❍**oui** ❍**non**

LE PLAN INFORMATIQUE

1. Année de réalisation du schéma directeur : **19..**

2. Horizon du schéma directeur : **3ans** **5ans** **> 5ans**

3. <u>Domaines couverts par le schéma directeur</u> :

- ❍ *Matériels centraux,*
- ❍ *Micro informatique,*
- ❍ *Bureautique (traitement de texte, tableur...),*
- ❍ *Télécommunications,*
- ❍ *Stratégie de l'informatique et de l'information*,
- ❍ *Méthode et outils,*
- ❍ *Infocentre,*
- ❍ *Télématique,*
- ❍ *Personnel,*
- ❍ *Budgets,*
- ❍ *Sécurité,*
- ❍ *Informatique de pilotage (tableaux de bord, OAD),*
- ❍ *Systèmes experts, Intelligence artificielle,*
- ❍ *Autres (précisez)* : _____

4. <u>Existe-t-il un Plan Informatique formalisé</u> ? ❍**oui** ❍**non**

5. <u>Le Plan Informatique est-il révisé annuellement</u> ? ❍**oui** ❍**non**

6. <u>Le Plan est-il contrôlé par un Comité Directeur Informatique</u> ? ❍**oui** ❍**non**

7. <u>S'il existe un Comité de pilotage, est-il composé du</u> :

- ❍ *Directeur Informatique,*
- ❍ *Directeur Général,*
- ❍ *Directeur Financier,*
- ❍ *Directeur Commercial,*
- ❍ *Secrétaire Général,*
- ❍ *Représentant(s) d'utilisateurs*.

8. <u>Les méthodes de planification</u> :

Quelle méthode de conception et/ou de suivi de projets utilisez-vous ?

- ❍ *MERISE,*
- ❍ *AXIAL,*
- ❍ *RACINES,*
- ❍ *AUTRE (laquelle)* : _____,
- ❍ *AUCUNE,*
- ❍ *ETUDE EN COURS.*

9. <u>Les méthodes de développement</u> :

Quelle méthode de développement utilisez-vous ?

- ❍ *MERISE,*
- ❍ *AXIAL,*
- ❍ *S.D.M.,*
- ❍ *I.E.M.,*
- ❍ *AUTRE (laquelle)* : _____,
- ❍ *AUCUNE,*
- ❍ *ETUDE EN COURS.*

10. <u>Les outils de développement</u> :

Quels outils de développement utilisez-vous et depuis quand ?

<u>date</u>

- ❍ *Dictionnaire de données,*
- ❍ *L4G,*
- ❍ *Générateur de code,*
- ❍ *Maquettage,*
- ❍ *Atelier de génie logiciel*,
- ❍ *AUTRE (lequel)* : _____,
- ❍ *AUCUN,*
- ❍ *ÉTUDE EN COURS.*

LE SYSTÈME D'INFORMATION

<u>Les fonctions suivantes sont-elles informatisées</u> ?

- ❍ *Gestion clients-comptes-produits,*
- ❍ *Système du réseau d'agences,*
- ❍ *Systèmes de paiement,*
- ❍ *Echanges interbancaires,*
- ❍ *Gestion des Valeurs Mobilières et interventions sur les marchés,*
- ❍ *International,*
- ❍ *Contrôle de Gestion, pilotage*

LE NIVEAU DE CENTRALISATION

<u>Quel est le niveau de centralisation</u> : (exprimé en pourcentage)

- ❍ *Matériels : _____%,*
- ❍ *Données : _____%,*
- ❍ *Equipes de développement : _____%,*

LE NIVEAU DE STANDARDISATION

Quelle est la part des développements spécifiques internes (maison) sur l'ensemble des progiciels applicatifs ?

_____ *%*

LES SOLUTIONS INFORMATIQUES

Quelle est la part des solutions informatiques (hors bureautique) apportées à travers :
***(*Répondre en % du nombre d'utilisateurs)**

- *L'informatique classique* : _____%,
- *La micro-informatique* : _____%,
- *L'infocentre* : _____%,

L'INFORMATIQUE STRATÉGIQUE

1. Les cibles stratégiques :

Quelles sont, par ordre d'importance relative, les cibles définies comme stratégiques de votre informatique (par exemple : avantages concurrentiels par réduction des coûts, croissance et innovation, relations clientèle, maîtrise interne, produits de substitution, nouveaux entrants, ...).

❶ _____

❷ _____

❸ _____

❹ _____

❺ _____

2. Les choix technologiques :

Classez hiérarchiquement, par degré stratégique décroissant, les technologies de l'information : (par ordre décroissant d'importance, 1 = le premier)

- ❍ *Échange de données informatisées (EDI),*
- ❍ *Liaisons PC-Mainframes,*
- ❍ *Outils de simulation,*
- ❍ *Minitel, Vidéotex,*
- ❍ *Messagerie électronique,*
- ❍ *Systèmes experts, Intelligence artificielle.*

L'ASSISTANCE EXTÉRIEURE

Quel est le budget moyen sur les 3 dernières années consacré aux :

- ● *Cabinets de conseil, consultants* :_____ *KF*
- ● *S.S.I.I. (réalisations, ingénierie)* :_____ *KF*

Pourcentage budgétaire des applications données en sous-traitance (FM ou "facility management", infogérance ou "outsourcing") par rapport au total du budget informatique.

_____ %

Les critères d'appréciation des utilisateurs

(cette partie du questionnaire pourra être reproduite et distribuée à des utilisateurs fonctionnellement bien déterminés : Direction générale, Directions opérationnelles, Direction administrative, responsables de la comptabilité, trésorier, etc.)

Donner une note de 0 à 10 (10 = maximum) traduisant votre sentiment de satisfaction vis-à-vis du système informatique que vous utilisez :

- **Le système d'information** :
  - Fiabilité : _____,
  - Ergonomie, convivialité : _____,
  - Adéquation aux besoins : _____,
  - Sécurité : _____,
  - Intégration : _____,

- **Les hommes** :
  - Réactivité de l'équipe informatique : _____,
  - Respect des délais et des budgets : _____,
  - Capacité à imaginer et gérer le changement : _____,
  - Facilité de communication : _____,
  - Compétence : _____,

NOM :
Qualité/Fonction :
☎ **:**

3.2. MATRICE DE PONDÉRATION (À UTILISER POUR CALCULER LES FACTEURS ET LA NOTE GÉNÉRALE) - QUESTIONNAIRE 2

Remarques :

• Les 65 questions du mini-questionnaire regroupent souvent des questions séparées dans le questionnaire MARION complet, (en 600 questions) et qui ont été, ici, condensées.

De ce fait, pour lever toute ambiguïté, notamment en cas de notateurs multiples, il faut se donner une règle de notation.

Par exemple, pour la question 11 : "Y-a-t-il une analyse des comptes comptables sensibles au moins deux fois par an, les résultats étant consignés dans un rapport ?", il faut définir une règle du type :

4 = oui, : 2 fois par an, consigné, tous comptes

3 = oui, : 2 fois par an, mal consigné

2 = oui, 1 fois par an et consigné

1 = oui, parfois fait (moins de ou 1 fois par an) et non consigné ou jamais

0 = sans objet[43]

• La matrice des pondérations sert à calculer les chiffres par facteur (et donc obtenir le niveau global de sécurité et pouvoir tracer la rosace MARION).

Par exemple, sur les sept questions retenues pour le facteur 1 (sur les 17 que comporte ce facteur dans le document MARION complet), il existe une formule de pondération qui est la suivante :

facteur 1 = [(Q1 x 6) + (Q2 x 6) + (Q3 x 5) + (Q4 x 6) + (Q5 x 4) + (Q6 x 2) + (Q7 x 2)]/31

où Q1 à Q7 sont les 7 premières questions posées dans le questionnaire simplifié, les chiffres multiplicatifs (exemple : x 6) étant repris de la dernière colonne de la matrice des pondérations figurant page suivante.

Les sept premières questions retenues sont les questions de poids MARION important (correspondant à un risque constaté par l'APSAD) ; mais comme toutes les questions de poids inférieur n'ont pas été retenues (10 sur 17), de façon à ne pas modifier la répartition MARION d'origine, l'écart à la somme de ce facteur 1 a été réparti sur les pondérations. Autrement dit, la somme des poids du mini-questionnaire reste identique à celle du questionnaire complet.

Sur les autres 26 facteurs restants, la même procédure -avec une formule chaque fois différente de la matrice de pondération- est à appliquer.

L'ensemble, une fois valorisé par les pondérations, permet de calculer la note représentative du niveau de sécurité informatique.

---

43 Du moins en théorie ; car pour cette question, une réponse 0 est exclue. Les questions notées 0 se verront attribuer la note correspondante reprise de la matrice (en dernière colonne) ou du tableau 3 ci-après (représentant la moyenne de l'échantillon ou du groupe) pour ne pas affecter la note totale.

Matrice de pondération

Facteurs		Coeff.	Poids %	Questions	Coeff.
Organisation générale	**101**	3,1	2	1	0,6
				2	0,6
				3	0,5
				4	0,6
				5	0,4
				6	0,2
				7	0,2
Contrôles permanents	**102**	5	3,26	8	2,0
				9	0,9
				10	0,9
				11	1,2
Réglementation et Audit	**103**	1,5	0,98	12	0,7
				13	0,6
				14	0,2
Facteurs socio-économiques	**201**	2	1,3	15	1,0
				16	1,0
Environnement de base	**301**	1	0,65	17	1,0
Contrôle des accès	**302**	4,5	2,93	18	2,5
				19	2,0
Consignes	**304**	1	0,65	20	1,0
Sécurité incendie	**305**	1	0,65	21	1,0
Dégâts des eaux	**306**	1	0,65	22	1,0
Amélioration Fiabilité fonctionnement	**307**	2	1,3	23	1,0
				24	1,0
Systèmes et procédures de secours	**308**	4,2	2,74	25	2,5
				26	0,9
				27	0,3
				28	0,5
Protocoles utilisateurs-informaticiens	**309**	2	1,3	29	1,0
				30	1,0
Personnel informatique	**310**	3,5	2,28	31	1,0
				32	1,0
				33	1,5
Plan informatique	**311**	1	0,65	34	1,0
Fiabilité des matériels et logiciels de base	**401**	1	0,65	35	1,0
Sécurité des télécommunications	**402**	4,3	2,8	36	1,0
				37	1,0
				38	1,3
				39	1,0
Protection des données	**403**	1	0,65	40	1,0
Archivage	**501**	1	0,65	41	1,0
Sauvegardes	**503**	8	5,2	42	3,0
				43	2,8
				44	1,0
				45	1,2

Suivi de l'exploitation	**504**	3	1,96	46	1,0
				47	1,0
				48	1,0
La maintenance	**505**	1	0,65	49	1,0
Les procédures de révision	**601**	1	0,65	50	1,0
Méthodes Analyse-programmation	**602**	4,3	2,80	51	1,0
				52	1,8
				53	1,5
Contrôles programmés	**603**	6,8	4,43	54	2,0
				55	1,0
				56	1,3
				57	1,2
				58	1,3
Micro-informatique	**999**	1	0,65	59	0,5
				60	0,5
			65,2		

(Enquête Risque Informatique du SGCB)

3.3. PRINCIPAUX TABLEAUX RÉSULTANT DE L'ENQUÊTE MENÉE EN 1991/92

Cinq classes d'établissement -qui rassemblent plusieurs groupes homogènes (GHE) tels que définis par le Secrétariat général de la Commission bancaire- avaient été constituées :

Classe 1 : grandes ou moyennes banques à vocation générale (GHE : 100, 200, 510, 720),

Classe 2 : banques locales (GHE : 310, 410, 420, 430),

Classe 3 : établissements spécialisés (GHE : 400, 600),

Classe 4 : banques de marché, de groupe (GHE : 520, 610, 620, 710, 730),

Classe 5 : banques étrangères (GHE : 800).

Ce regroupement avait été imposé par le nombre relativement limité (volontairement) d'établissements retenus (50), qui représentaient, toutefois, plus de 17 % de l'ensemble de l'activité des établissements assujettis.

Tableau 1 : données relatives aux effectifs

	GROUPE 1	GROUPE 2	GROUPE 3	GROUPE 4	GROUPE 5	ENSEMBLE DES BANQUES DE L'ÉCHAN-TILLON
Effectifs (agents)	85 176	4 035	8 656	937	1 938	100 742
Produit net bancaire (MF)	49 631	2 451	5 672	1 803	1 351	60 908
Produit net bancaire / agent (kF)	583	607	665	1 924	697	605
Effectifs informatiques	3 930	233	647	65	177	5 052
Eff. informatiques / total des effectifs (en %)	4,61	5,77	7,47	6,94	9,13	5,01
Effectifs exploitation	1 330	116	239	24	72	1 781
Effectifs exploitation / informatiques (en %)	33,84	49,79	36,94	36,92	40,68	35,25
Effectifs développement	2 286	97	383	34	100	2 900
Eff. développement/eff. informatiques (en %)	58,17	41,63	59,20	52,31	56,50	57,41
Effectifs divers	314	20	25	7	5	371
Eff. divers/effectifs informatiques (en %)	7,99	8,58	3,86	10,77	2,82	7,34

Tableau 2 : données de cadrage (chiffres 1991)

	GROUPE 1	GROUPE 2	GROUPE 3	GROUPE 4	GROUPE 5	ENSEMBLE DES BANQUES DE L'ÉCHAN-TILLON
Produit net bancaire (MF)	49 458	917	5 211	3 850	1 351	60 787
Frais généraux (MF)	36 720	595	4 668	916	1 134	44 033
Effectifs (agents)	83 294	1 258	7 303	1 216	1 938	95 009
Informatique (kF)	**5 865 494**	**65 082**	**558 810**	**100 910**	**192 259**	**6 782 555**
Produit net bancaire / agent (kF)	594	729	714	3 166	697	640
Informatique / agent (kF)	70	52	77	83	99	71
Informatique / produit net bancaire (%)	11,86	7,10	10,72	2,62	14,23	11,16
Informatique / frais généraux (%)	15,97	10,93	11,97	11,02	16,95	15,40

NB : en raison de réponses incomplètes, les données du tableau 2 sont un sous-ensemble de celles des tableaux 1 et 4.

Tableau 3 : notation générale

Le tableau suivant fait apparaître la notation des 25 facteurs MARION pour la totalité de l'échantillon et pour chaque groupe. De plus, la notation communiquée par l'APSAD sur une enquête réalisée en 1989 est apportée à titre indicatif, sachant que la population observée (secteur financier : banques, assurances et prévoyance) et la méthode étaient légèrement différentes.

		APSAD 1989	ENQUÊTE CB moyenne des 5 groupes	GROUPE 1	GROUPE 2	GROUPE 3	GROUPE 4	GROUPE 5
Organisation générale	101	1,73	2,03	2,51	1,84	2,08	1,76	1,94
Contrôles permanents	102	2,51	2,15	2,25	1,78	2,34	2,33	2,07
Réglementation et Audit	103	2,29	2,75	2,93	2,87	2,80	2,68	2,46
Facteurs socio-économiques	201	3,40	3,39	3,24	3,64	3,75	3,42	2,90
Environnement de base	301	1,27	1,97	2,68	0,86	1,67	1,83	2,80
Contrôle des Accès	302	1,91	3,32	3,53	3,49	2,96	3,37	2,56
Consignes	304	2,17	2,38	2,44	2,14	2,00	2,50	2,80
Sécurité Incendie	305	2,58	2,96	3,60	2,57	2,83	3,00	2,80
Dégâts des eaux	306	1,15	2,10	2,76	0,86	2,50	2,17	2,20
Amélioration Fiabilité Fonctionnement	307	2,32	2,39	3,10	2,00	2,67	3,00	1,20
Systèmes et Procédures de secours	308	1,79	1,85	2,12	1,07	1,75	2,27	1,03
Protocoles utilisateurs informaticiens	309	2,21	1,61	2,08	1,14	1,67	1,58	1,60
Personnel informatique	310	2,29	2,62	2,70	2,22	2,52	2,86	2,80
Plan informatique	311	2,40	2,37	2,72	2,14	2,00	3,00	2,00
Fiabilité des matériels et logiciels de base	401	2,61	3,24	3,20	3,71	3,50	3,00	2,80
Sécurité des télécommunications	402	1,76	2,92	2,96	2,92	2,92	3,03	2,77
Protection des données	403	2,00	2,67	2,66	2,43	3,00	2,83	2,40
Archivage	501	1,78	2,67	2,64	2,57	2,83	2,50	2,80
Sauvegardes	503	3,11	2,92	2,72	2,70	3,19	2,96	3,05
Suivi de l'exploitation	504	2,74	2,79	3,19	2,71	2,89	2,94	2,20
La maintenance	505	2,69	3,67	3,76	4,00	3,83	3,33	3,40
Les procédures de révision	601	1,59	2,26	2,40	2,29	2,00	1,83	2,80
Méthodes Analyse-Programmation	602	2,42	2,34	2,69	1,99	2,56	2,45	2,02
Contrôles programmés	603	1,10	1,35	1,18	1,14	1,50	1,44	1,51
Micro-informatique	999	ND	2,36	2,40	2,50	2,00	2,06	2,80
		2,07	2,52	2,74	2,30	2,55	2,57	2,39

Tableau 4 : dépenses informatiques (total des banques de l'échantillon ; données 1991)

	TOTAL	%
Charges diverses personnel.....	1 409 410	20,37
Formation professionnelle	33 210	0,48
Loyers ou amortissements :		
- locaux professionnels	180 497	2,61
- matériels informatiques	954 744	13,80
- logiciels	331 008	4,78
Entretien des locaux et des installations	31 580	0,46
Entretien des matériels informatiques	611 637	8,84
Travaux à façon dépenses	428 413	6,19
Travaux à façon recettes	68 855	0,99
Rémunérations, conseils extérieurs	335 661	4,85
Liaisons informatiques.....	421 083	6,08
Fournitures informatiques.....	95 874	1,38
Frais divers de gestion	84 111	1,22
Fonctions informatiques décentralisées :		
- CTI.....	620 512	8,97
- organisation administrative	52 595	0,76
- travaux à façon	51 110	0,74
- procédures intermédiaires.....	83 133	1,20
- terminaux.....	549 223	7,94
- traitement des chèques.....	24 753	0,36
- Télécom	77 292	1,12
- tests développements	217 590	3,14
Micro informatique :		
- investissements/an	95 109	1,37
- formation	8 735	0,13
- maintenance.....	25 249	0,36
Automates GAB.....	128 881	1,86
TOTAL GÉNÉRAL.....	**6 920 265**	**100,00**

ANNEXE IV

FICHES-CONSEILS

- Chaque fiche-conseil fait l'objet d'un court développement selon 4 points :

  . définition
  . risques
  . parades
  . critères de qualité

- La liste des fiches-conseils est la suivante :

1. Administration et protection des données
2. Architecture client/serveur
3. Archivage, gestion et contrôle des supports
4. Aspects juridiques
5. Aspects socio-économiques
6. Assurances
7. Audit et contrôles
8. Les consignes de sécurité
9. Contrôles d'accès logique
10. Contrôles d'accès physique
11. Contrôles programmés
12. Développements externes
13. Downsizing et réseaux locaux
14. E.D.I.
15. "Exotisme"
16. "Facilities management" - "Out Sourcing" (sous-traitance, externalisation et infogérance)
17. G.E.D. : Gestion électronique des documents
18. Maintenance des matériels et logiciels de base
19. Messageries
20. Méthodes et outils de développement
21. Modifications applicatives
22. Moyens et procédures de secours
23. Organisation de la sécurité ; responsabilités
24. Personnel informatique ; fonctions, éthique
25. Procédures de recette
26. Propriétaires et classification des informations
27. Relations utilisateurs/informaticiens
28. Sauvegardes : procédure et conservation
29. Sécurité des bâtiments, des locaux et de l'environnement
30. Sécurité des micro-ordinateurs
31. Sécurité des télécommunications
32. Sécurité d'accès aux réseaux
33. Sécurité incendie et dégâts des eaux
34. Suivi et contrôle des travaux d'exploitation
35. Système d'exploitation
36. Télémaintenance

Fiche 1 : Administration et protection des données

Définition

L'administration des données consiste à recenser, de façon unique et centralisée, les données de l'entreprise (au moins les données de référence, communes à plusieurs entités) et leurs principales caractéristiques.

Parmi ces caractéristiques doit figurer le niveau de sensibilité, qui permettra de définir le **niveau de protection** à affecter aux données lors de leur utilisation.

N.B. : Il ne faut pas confondre **l'administration des données** (ADD) avec **l'administration des bases de données** (DBA), qui est une fonction de l'exploitation informatique consistant à gérer les espaces de stockage (le contenant) des données (le contenu).

Risques (consécutifs à l'absence d'ADD)

Incohérence, confusion, erreurs, dans l'interprétation de la signification des données.

Difficultés pour maintenir les applications en cohérence.

Pertes de temps à redéfinir sans cesse les noms, les normes, les modèles de données, les contrôles...

Création et maintenance de multiples interfaces (tables de correspondance ...), aussi bien pour les échanges d'informations entre applications internes qu'avec les applications externes (SWIFT, Banque de France, EDI, ...).

Protection insuffisante ou incohérente des données.

Parades

Mettre en place une administration des données, dotée des moyens (structure) et outils (dictionnaire conceptuel) nécessaires.

Le dictionnaire doit gérer au minimum les caractéristiques suivantes, pour chacune des données référencées :

- son nom (conforme aux normes internes),
- sa définition,
- son propriétaire,
- ses critères de sécurité D.I.C., codifiés en niveaux (définis par le propriétaire),
- où et par qui cette donnée est utilisée (base, application, ...),
- ses valeurs possibles, et les contrôles associés,
- ses liens avec d'autres données, et les cohérences à respecter.

Il appartient à l'administration des données :

- de juger si une donnée doit être référencée ou non,
- de valider le modèle conceptuel de données et d'assurer leur cohérence avec les modèles physiques,
- d'assurer la diffusion des données de référence (sous forme de tables, de listes...) auprès de l'ensemble des utilisateurs,
- de définir le niveau de protection adapté pour chaque donnée et d'en assurer la cohérence globale.

Chaque utilisation de données référencées doit faire l'objet d'un **niveau de protection** correspondant à celui de la donnée la plus sensible.

Quelques exemples de protections :

- Disponibilité → duplication, sauvegarde, secours...
- Intégrité → certification, contrôle d'accès, scellement...
- Confidentialité → coffre, habilitation, chiffrement...

Critères de qualité

Assurer l'unicité et l'autonomie de l'administration des données : la structure n'est pas forcément rattachée au service informatique.

Utiliser un dictionnaire conceptuel intégré à un atelier de génie logiciel (AGL) (ex : PACBASE).

Disposer d'une méthode de modélisation des données (ex : MERISE).

Automatiser le lien entre modèle conceptuel et modèles physiques de données.

Désigner les propriétaires des données.

Coter les critères D.I.C. sur 5 niveaux maximum, et définir précisément les mesures de protection associées à chaque niveau de chaque critère.

Respecter les normes externes existantes (CFONB, AFNOR, INSEE, ISO, EDIFACT...) pour la définition et le format des données.

Fiche 2 : Architecture client/serveur

Définition

L'architecture client/serveur se caractérise par la division d'un traitement informatique exécuté sur des plates-formes interconnectées en réseau.

Le traitement informatique représente ici l'ensemble des opérations déclenchées par une seule requête au Système d'Information.

L'architecture client/serveur recouvre des modèles techniques très diversifiés, depuis l'architecture centralisée d'une application dans laquelle les postes de travail "Clients" ne possèdent que la fonction de présentation des écrans jusqu'à une application réellement éclatée entre plusieurs ordinateurs spécialisés dans la gestion de certaines données et dans la réalisation de certains types de traitements.

Par ailleurs les différents ordinateurs impliqués peuvent être homogènes en terme de systèmes d'exploitation et gestion du réseau mais, le plus souvent, le modèle client/serveur est associé à des architectures hétérogènes, mainframes et systèmes d'exploitation propriétaires, serveurs gérés par des systèmes ouverts et stations de travail intelligentes pour lesquels une couche de logiciels supplémentaires, "middleware", gère l'interopérabilité entre les ordinateurs, les protocoles réseaux et les applications.

La mise en œuvre du modèle client/serveur peut remettre en question l'existence même du mainframe, remplacé par plusieurs ordinateurs plus petits reliés en réseau dans une évolution qualifiée alors de "downsizing" [voir fiche n° 13].

Risques

Les risques sont diversifiés à l'instar des architectures techniques mises en place.

La **mise en réseau des ordinateurs** constitue un premier domaine pour lequel il convient de s'assurer que les risques nouveaux ont bien été pris en compte. Le transit d'informations sur le réseau de télécommunication est-il protégé contre l'altération ou la perte de celles-ci ? Si les informations transmises sont confidentielles, quelles sont les garanties offertes par les moyens de télécommunication ? Est-ce que les accès à ce réseau sont bien contrôlés et peut-on garantir qu'il résistera à des tentatives malveillantes ? Le contrôle des flux par l'intermédiaire de technologies telles que "ponts", "routeurs", "passerelles"..., est-il bien maîtrisé et encadré par des murailles de Chine" ("firewalls") ? Par ailleurs, dispose-t-on de moyens de surveillance permettant de détecter et de gérer l'ensemble de ces dysfonctionnements ?

Le second domaine à examiner est constitué par les **couches logicielles "middleware"** et leurs aptitudes dans la gestion des habilitations utilisateurs et des protections d'accès.

L'offre des logiciels orientés micro-ordinateurs ou systèmes ouverts n'est pas toujours mature dans ce domaine et les solutions techniques proposant l'interopérabilité des gestionnaires de bases de données sont disponibles sur le marché avant d'offrir les mêmes facilités pour les bases des logiciels de sécurité.

La sécurité des environnements distribués, OSF/DCE, doit apporter une réponse fiable à ce sujet. Annoncée depuis deux ans, elle est sur le point de devenir une réalité pour plusieurs constructeurs et fournisseurs de logiciels.

Un autre point concerne la **disponibilité globale du service**. L'architecture client/serveur est souvent présentée comme une solution d'amélioration de la disponibilité puisque elle répartit les risques de dysfonctionnement entre plusieurs machines et plusieurs sites. Pour être valide, cet argument doit être assorti d'un certain nombre de mesures concernant la localisation des serveurs, la protection physique des accès, la fourniture d'énergie, le plan de sauvegardes ... Ces mesures sont familières des informaticiens qui ont connu l'installation et la gestion des mainframes, elles le sont moins des utilisateurs qui ont abordé l'informatique par la micro-informatique et qui, suivant les effets de mode et de médiatisation, maîtrisent seuls leurs stations de travail et leurs serveurs, voire réalisent eux-mêmes leurs applications.

Enfin, le dernier point concerne la configuration ou "poste client". L'offre du marché, en ce domaine, ne semble pas encore assez mûre pour "héberger", avec le niveau de sécurité souhaité, des applicatifs bancaires sensibles.

Parades

Le déploiement d'une architecture client/serveur doit être soumis aux mêmes exigences de sécurité que les mainframes, ces exigences étant bien entendu adaptées à la nature des données et des traitements impliqués.

La protection des échanges entre les serveurs doit garantir l'authentification des serveurs, l'intégrité des informations transmises (mécanismes de reprise en cas d'interruption ou de correction en cas d'erreur).

L'identité du demandeur doit être vérifiée sur tous les points d'accès au réseau et sur toutes les stations de travail accédant à des informations de l'entreprise.

Le transport des clés d'authentification du demandeur entre les serveurs doit être transmis par des canaux sécurisés.

Les mécanismes de protection d'accès aux données de l'entreprise doivent être opérationnels sur tous les serveurs et sur toutes les stations de travail.

En fonction de la taille de l'entreprise et de nombre des utilisateurs du Système d'Information, la charge de travail ou la complexité de l'administration de la sécurité, gestion des habilitations utilisateurs et protection des ressources, ne doit pas devenir intolérable en raison de l'absence d'un outil unique de gestion. Si une gestion décentralisée de la sécurité a été mise en place, celle-ci doit correspondre à l'organisation de l'entreprise mais elle ne doit pas être imposée par l'insuffisance technologique.

La protection physique des serveurs et des stations de travail doit être prise en compte au même titre que celle des mainframes.

Les sauvegardes des données et des programmes de l'entreprise, la conservation des supports de sauvegardes et les procédures de reconstitution sont mises en place de façon cohérente sur tous les serveurs et toutes les stations de travail, en fonction de critères de disponibilité attribués aux traitements correspondants [voir fiches n° 22 et 28].

Lorsque les sécurités logiques et physiques s'avèrent insuffisantes au regard du caractère confidentiel ou critique des informations traitées, l'architecture client/serveur doit être provisoirement abandonnée au profit d'une architecture éprouvée de type centralisé. Il convient donc, dans ce cas, de s'assurer que les postes "clients" ne contiennent que des modules de présentation.

Critères de qualité

L'existence d'une architecture cible proposée par les équipes informatiques est une garantie de cohérence de la sécurité. Elle permet d'anticiper sur les besoins utilisateurs tout en contrôlant l'intégration technologique.

L'intégration de l'administration de la sécurité à l'architecture client/serveur est également un critère de cohérence de la sécurité. Elle peut être réalisée par des interfaces spécifiques développées sur des systèmes a priori incompatibles ; elle sera prochainement possible grâce à la mise en œuvre du standard DCE de l'OSF.

La classification des données et des traitements du Système d'Information suivant les critères de Disponibilité, Intégrité et Confidentialité est un outil d'aide à la décision efficace pour le choix de décentralisation d'une application sur un modèle client/serveur. Il permet de valider que les moyens de sécurité offerts par l'architecture sont mis en adéquation avec les exigences de l'entreprise.

Fiche 3 : Archivage, gestion et contrôle des supports

Définition

L'archivage répond à un besoin fonctionnel qui vise à conserver des données ou informations, stratégiques ou non, mais nécessaires à l'entreprise sur le plan professionnel, social, fiscal ou juridique.

Ces informations pourront être utilisées à des fins de consultation et de recherche, pour extraire par exemple des statistiques, des historiques, ou servir de preuves. Cette rétention documentaire dont la gestion est assujettie à un plan de classement sera aussi le moyen, à partir de documents de base, de reconstituer de l'information. L'obligation de reconstitution est liée aux contraintes légales ou contractuelles (archivage obligatoire), aux besoins de consultation (archivage administratif).

Il faut distinguer archivage et sauvegarde, même si les recommandations générales de protection peuvent s'appliquer de l'une à l'autre. La sauvegarde, processus préventif géré par les exploitants des plates-formes informatiques, consiste, pour l'essentiel, à recopier périodiquement les fichiers et bases de données dans le but de reconstruire, en cas de besoin, un environnement technique qui préserve un certain niveau de fraîcheur de l'information et de service [voir fiche n° 28 : "sauvegarde"].

Le processus d'archivage de premier niveau est parfois immédiatement déclenché dès la réception d'un document dans l'entreprise (ex : enregistrement chrono et numérisation pour une diffusion électronique en interne).

Risques

Les études de risques amènent à prendre en compte des cas de sinistres immatériels (ex : pertes de données enregistrées sous forme magnétique), totaux ou partiels, avec obligation de reconstitution des fichiers et des bases de données.

Il convient donc de se prémunir contre ces éventualités, par la conception d'un système d'archivage documentaire afin d'endiguer les risques de pertes mais aussi de satisfaire un besoin fonctionnel de l'entreprise.

Tout procédé induisant son propre risque, il sera souhaitable de ne pas fabriquer un archivage dont les données ne seront pas facilement réexploitables, soit que l'intégrité des données d'origine n'y est pas garantie (ex : sauvegardes incrémentales déficientes), soit que ces données soient détériorées de façon non apparente (ex : bandes magnétiques dont le signal est trop atténué pour être lu), soit que l'environnement de stockage n'y est pas suffisamment contrôlé (ex : température, hygrométrie).

Parades

L'entreprise détermine ses modes d'archivages que les services concernés utilisent pour établir des classements fiables des principaux documents stratégiques et des justificatifs originaux, non reconstituable par des tiers. Il est recommandé de ne pas dépasser quatre ou cinq niveaux dans la classification qui caractérise le niveau de sensibilité, c'est-à-dire les conséquences d'une perte des informations répertoriées dans l'entreprise (ex : niveau 0 = document public, niveau 4 = document hautement stratégique) [voir fiche n° 26].

Le mode de classement, qu'il convient de distinguer de la classification par niveau de sensibilité, sera un compromis entre l'archivage classique, typologique ou historique, et l'archivage thématique, pour une reconstitution rapide.

Pour les données issues des traitements informatiques, il est souhaitable de décliner, dès la conception des applications, les procédures automatiques et organisationnelles d'archivage/désarchivage (différentes de celles de sauvegarde, notamment pour les conditions de réutilisation des supports et le site de stockage) et de préciser les domaines de responsabilité des acteurs tout au long du cycle de vie des applications. Les documents méthodologiques élaborés lors du développement d'une application seront archivés périodiquement. Les procédures, et donc les conditions de conservations à utiliser, incluront la sécurité liée aux bandothèques, médiathèques, cartouches, bacs de microfiches et seront spécifiques pour chaque type de support (microfiches, disques optiques numériques, cartes, formulaires, courriers, listings, ...).

Il sera parfois nécessaire d'effectuer un transfert de support afin de préserver durablement l'information (ex : papier thermique qui s'efface dans le temps). Une régénération annuelle des supports magnétiques est suffisante pour parer à la volatilité de l'information stockée sous cette forme.

Critères de qualité

Afin de préserver l'efficacité du système et de l'organisation adaptées aux contraintes d'archivage de l'entreprise, il conviendra d'assurer la maintenance des matériels, des logiciels et de la documentation associée.

Les archives seront alimentées périodiquement, le transport devant être adapté au niveau de sécurité accordé aux pièces archivées.

La gestion des supports doit être conduite sous l'autorité d'un seul responsable qui n'est pas un opérationnel des unités clientes du service d'archivage. Entrées, sorties, créations, transferts, effacements et destructions sont de sa responsabilité.

La classification doit apparaître clairement sur chaque support. En revanche, le marquage ne doit pas préciser l'identification.

L'utilisation d'un support doit être assujettie à une justification.

Les documents ou supports stratégiques sont à détruire avant leur mise au rebut.

Les locaux d'archivage sont distincts de ceux de sauvegarde, séparés physiquement des salles d'exploitation et protégés des risques accidentels et de ceux d'intrusion.

L'inventaire des supports, l'historique de la gestion des archives doivent être auditable et audité périodiquement. Le recours à des sociétés spécialisées offre des garanties de sécurité, d'intégrité et de confidentialité.

Des tests périodiques de désarchivage seront effectués sur des documents archivés et sélectionnés par échantillonnage.

Fiche 4 : Aspects juridiques

Définition

Les modalités de traitement, de circulation et de stockage de l'information font courir à l'établissement de crédit des risques juridiques divers. L'étude des aspects juridiques fait donc aussi partie des risques pesant sur les systèmes d'information.

Risques

Du fait d'un comportement volontaire ou laxiste de ses dirigeants ou de son personnel, une entreprise court le risque de se trouver en contravention avec les lois régissant la sécurité de l'information, d'être poursuivie par un tiers (client, fournisseur, concurrent, ...) et condamnée à de lourdes peines.

Bien que ces peines se traduisent essentiellement par des amendes infligées à la Société personne morale, la jurisprudence fait de plus en plus souvent état de condamnations (amendes, prison) infligées à des personnes physiques : PDG, mais aussi personnel(s) coupable(s) de l'infraction. Le risque de réputation porté à l'image de l'entreprise est également à prendre en considération.

Les risques juridiques peuvent se classer en deux grandes catégories :

- ceux relatifs aux obligations légales permanentes (respect du secret bancaire, déclarations à la CNIL ou au SCSSI, ...),

- ceux consécutifs au comportement indélicat de membres du personnel de l'établissement (fraude informatique, intrusion dans des systèmes externes, espionnage, piratage de logiciels du commerce, création de virus, ...).

Parades

La seule parade consiste à connaître les lois, et à les faire respecter dans l'entreprise ; l'esprit et les grandes lignes des principales d'entre elles sont rappelés ci-dessous :

Informatique et libertés (loi du 6 janvier 1978)

Son objectif est d'éviter que l'informatique "... ne puisse porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques".

Pour ce faire, elle crée les obligations suivantes :

- informer les personnes (physiques) fichées lors de la collecte des informations,
- leur donner un droit d'accès et de rectification,
- déclarer, préalablement à la mise en place des applications, les traitements à la CNIL (Commission Nationale Informatique et Libertés),
- assurer la confidentialité des informations nominatives.

Auxquelles s'ajoutent quelques interdits :

- collecter des informations sur la race, la religion, l'appartenance politique, ...
- divulguer les informations sur les personnes,
- détourner les traitements de leur finalité déclarée.

Elle expose les contrevenants à des sanctions :

- de 2.000 à 2.000.000 F d'amende,
- de 6 mois à 5 ans de prison.

Protection des logiciels (loi du 3 juillet 1985)

Son objectif est d'étendre aux logiciels le régime de protection du droit d'auteur (loi du 11 mars 1957), basé sur les principes suivants :

- sauf s'il est salarié d'une entreprise qui l'emploie à cette fin, l'auteur d'un logiciel en conserve la propriété intellectuelle,
- l'utilisateur "n'achète" pas le logiciel, mais seulement un droit d'utilisation,
- ce droit doit être défini dans un cadre contractuel.

La loi interdit toute modification ou duplication du logiciel, sans accord préalable de son propriétaire.

Elle prévoit les sanctions suivantes :

- de 6.000 à 120.000 F d'amende,
- de 3 mois à 2 ans de prison.

Fraude informatique (loi du 5 janvier 1988 - dite loi GODFRAIN)

Elle interdit :

- l'accès ou le maintien non autorisé dans tout ou partie d'un Système d'Information,
- d'entraver ou de fausser le fonctionnement d'un Système d'Information,
- d'introduire ou de modifier des données ou leur code de traitement ou de transmission,
- de falsifier des documents informatisés,
- de faire usage de documents informatisés falsifiés.

Les tentatives (même infructueuses) sont passibles des mêmes sanctions, soit :

- de 100.000 à 300.000 F d'amende,
- de 1 an à 3 ans de prison.

Protection des télécommunications (loi du 10 juillet 1991)

Son objectif est de préserver le "secret des correspondances émises par la voie des télécommunications" ; elle ne concerne pas que les écoutes téléphoniques, mais aussi les transmissions de données.

Elle interdit :

- d'installer des appareils d'interception,
- d'intercepter, de détourner, d'utiliser, de divulguer des informations transmises par télécommunication.

Elle prévoit les sanctions suivantes :

- de 5.000 à 100.000 F d'amende,
- de 6 jours à 1 an de prison.

Réglementation de la cryptologie

Le décret du 18 février 1986 assimile les matériels et logiciels de chiffrement à des armes de guerre, et donc les soumet au régime strict de l'autorisation préalable.

La loi du 29 décembre 1990 assouplit quelque peu cette réglementation, en instituant un régime de simple déclaration préalable (auprès du SCSSI), si l'utilisation est faite à des fins d'authentification ou d'intégrité (l'autorisation étant maintenue dans les autres cas, c'est-à-dire chaque fois qu'il y a chiffrement de fichiers).

Les défauts de déclaration ou d'autorisation sont sanctionnés de la façon suivante :

- de 6.000 à 500.000 F d'amende,
- de 1 mois à 1 an de prison.

Critères de qualité

Disposer d'un juriste (interne ou conseiller externe) spécialiste du droit de l'informatique.

Définir les responsabilités au sein de l'entreprise ; en particulier, lorsque il y a des délégations de responsabilités pour certains aspects de la sécurité, celles-ci doivent être formalisées.

Organiser la communication (voire la formation si nécessaire) sur ces aspects auprès du personnel concerné.

Doter les informaticiens d'un code d'éthique professionnelle ; à défaut, on pourra se référer à celui de l'AFIN (Association Française des Informaticiens) [voir fiche n° 24].

Mettre en place les moyens nécessaires pour éviter au personnel de se placer en situation illégale : habilitations d'accès aux systèmes informatiques, versions de progiciels en nombre suffisant, contrôles périodiques des logiciels installés, procédures et imprimés pour les déclarations obligatoires, ...

Négocier avec les fournisseurs des logiciels bureautiques, un droit de copie à usage domestique.

Adresses utiles

CNIL : 21, rue Saint Guillaume - 75007 PARIS
SCSSI : 18, rue du docteur Zamenhof - 92131 ISSY-LES-MOULINEAUX CEDEX
AFIN : Informat Cnit - 2, place de la Défense, Bureau 395 - BP 637 - 92053 PARIS LA DÉFENSE

Fiche 5 : Aspects socio-économiques

Définition

Le terme "*aspects socio-économiques*" définit un certain nombre de critères qui permettent d'analyser l'ensemble du comportement humain que l'on peut observer en milieu professionnel.

Chaque individu, dans un contexte professionnel, doit se plier à un certain nombre de règles préétablies et intégrées dans l'organisation de la société.

L'homme, par nature, est faillible volontairement ou involontairement. Il est donc un facteur important de risque direct ou indirect.

Certaines de ces actions, génératrices de sinistres, sont toujours influencées par l'environnement de manière implicite ou explicite.

Pour qu'un sinistre se réalise, il faut la conjonction de 3 éléments :

- l'homme (ses penchants),
- la cible (son attrait et sa vulnérabilité),
- et, les circonstances/l'environnement (en relation avec l'homme et sa cible).

Selon les estimations des services de police : 10 % des personnes sont foncièrement honnêtes, 10 % des personnes sont foncièrement malhonnêtes et 80 % peuvent devenir malhonnêtes en fonction des circonstances.

Risques

Les risques sont induits ou générés par différentes causes :

a) l'accident : événement fortuit, imprévu, extérieur à la victime et indépendant de sa volonté,

b) l'erreur : événement causé par une faute ou une méprise,

c) la malveillance : événement causé dans l'intention de nuire, de portée criminelle (vandalisme, sabotage, fraude, altération, détournement).

Ils peuvent dépendre d'une situation particulière :

a) l'homme clé (détenant un trop grand pouvoir : peut imposer une décision, refuser de faire, etc.),

b) la grève de personnel,

c) l'état moral d'une personne (situation personnelle délicate, stress, déstabilisation du personnel sensible, personnel sous tentation forte, etc.),

d) le manque d'information (des mesures de sécurité non annoncées peuvent entraîner des réactions d'hostilité).

Parades

Limiter les risques, c'est, d'une part, la mise en œuvre de moyens techniques (réduction des accidents, détection des erreurs) et, d'autre part (et surtout), maintenir la bonne qualité de l'environnement professionnel.

Agir sur le moral du personnel par un style de management ad hoc et consensuel (communication, écoute du personnel).

Avoir des capteurs du climat social.

Avoir un plan de Back-up social.

Les risques pris par une personne sont toujours calculés par rapport aux enjeux ; il ne faut pas que ces risques leur paraissent trop modérés : d'où la nécessité de mettre en place des moyens de dissuasion.

La connaissance doit être partagée par plusieurs personnes.

Différencier le travail effectué par le personnel interne et externe.

Assurer le respect des règles émises par le CHSCT.

Les actions possibles sont :

- les moyens procéduraux :
  * procédures encadrant les moyens techniques,
  * contrôle interne, audit de conformité ;

- l'action sur les agents internes :
  * action éducative et psychologique (prise de conscience, information, formation),
  * action réglementaire (règlement externe/interne, code d'éthique/de déontologie, engagement individuel),
  * sélection du personnel (détection de l'individu à risque),
  * contrôle et suivi de personne (enquêtes, pistages, diagnostic).

- l'action sur les agents externes :
  * sélection, contrôle et suivi (suivi rapproché),
  * engagement contractuel (responsabiliser les agents),
  * formation et information (réduite au minimum),
  * gestion ad hoc du personnel extérieur (SSII).

Critères de qualité

La prévention des risques se fait d'abord par des moyens techniques bien adaptés au contexte mais qui ont forcément leurs limites (elles peuvent donc être contournées).

Ces moyens sont, par exemple, des procédures de sauvegarde, une limitation des accès aux informations, etc.

S'assurer que les tâches spécialisées sont réalisables par plusieurs personnes.

En revanche, si l'enjeu en vaut la peine, aucune défense technique aussi complexe soit-elle, ne sera un frein pour le criminel. D'où l'importance des moyens de dissuasion.

La qualité se mesure par :

- un taux d'absentéisme faible et constant,
- un nombre de jours de grève faible, voire nul,
- une réduction des démissions, une faible rotation de personnel ("turn-over"),
- un bon climat social (meilleure condition de travail, salaire justifié, promotion possible) d'ailleurs difficile à apprécier, de perception subjective,
- un contrôle régulier pour s'assurer que les travaux critiques sont réalisables par plusieurs personnes.

Fiche 6 : Assurances

Définition

Une assurance est un contrat par lequel une personne, *l'assuré*, stipule qu'elle sera garantie, moyennant le paiement de primes ou cotisations, contre les conséquences préjudiciables d'un événement futur et incertain, ou *risque*, dont elle serait responsable ou victime, par un *assureur* qui accepte de la garantir. Le contrat d'assurance prend le nom de *Police d'assurance*.

Trop souvent, la souscription d'un ou plusieurs contrats d'assurance est le seul moyen de "sécurité" mis en place et, de plus, sans réflexion préalable.

Le premier conseil à donner aux responsables informatiques serait : "mieux vaut investir dans les systèmes de sécurité que dans les primes d'assurance". Néanmoins, l'assurance doit être considérée comme une garantie complémentaire, qui n'apporte que des compensations d'ordre financier.

Que peut-on assurer dans un système de traitement ? TOUT (ou presque). En corollaire, il faut que la perte financière engendrée par la réalisation d'un risque soit prouvable et quantifiable.

Risques

Alors faut-il tout assurer ?
Les assureurs assurent-ils tout et à n'importe quelles conditions ?

Appliqué à un système de traitement d'information, la couverture d'assurance concerne d'abord les grands classiques (incendie, dégâts des eaux, vol) de tout ou partie des matériels informatiques, mais aussi le bris d'un compresseur de climatisation, le détournement de fonds, de biens ou les infections virales sur micro-informatique.

Le contrat d'assurance ne garantit pas la reprise des traitements informatiques.

C'est à l'assuré d'analyser ses risques et de déclarer à ses assureurs tout élément susceptible d'influer sur leurs réalisations et leurs conséquences, et ce, y compris pendant la vie des contrats.

Toute éventuelle modification ultérieure doit faire l'objet d'une déclaration de la part de l'assuré de manière à ce que son plan d'assurance soit en parfaite adéquation avec la nouvelle situation face aux risques.

Par définition, un système de traitement d'information est à la fois *cible de risques* et *vecteur de risques*. Cela se traduit par des conséquences dommageables pour l'entreprise, et/ou des conséquences dommageables à autrui.

En langage "assurance", cela donne deux natures de contrats : les contrats d'assurances "Dommages" et les contrats d'assurances "Responsabilités".

Un point important est à souligner : faire attention aux contrats mal adaptés dès la souscription.

Parades

Comment s'assurer ?

Deux voies de couverture sont actuellement proposées par les assureurs, outre les polices d'assurances classiques (incendie, bris de machine, vol) :

- la voie informatique (événement assuré lié au système informatique),
- la voie sectorielle (événement assuré lié à l'activité de l'entreprise), couverture privilégiée des banques.

Quelques exemples de contrats garantissant les dommages :

- *Tous risques informatiques* (TRI) : couverture en risque direct (incendie, explosion, chocs, bris de machines, événements naturels, vol, attentat, sabotage).

- *Extension aux risques informatiques* (ERI) : couvre les pertes de fonds, pertes de biens avec possibilité d'extension aux pertes d'exploitation.

- *Fraude/Détournement* : couvre les pertes pécuniaires dues à une fraude, escroquerie, détournement, et les éventuelles pertes d'exploitation associées.

- *Pertes d'exploitation* : couvre les équipements purement informatiques, et les équipements d'environnement (alimentation, climatisation).

- *Sabotage immatériel* : couvre les dommages consécutifs à un sabotage immatériel, les frais de reconstitution de médias, les frais supplémentaires d'exploitation en option, les pertes d'exploitation.

Quelques exemples de contrats garantissant les responsabilités :

- *Responsabilité civile* : couvre les conséquences des dommages causés à des tiers du fait de l'utilisation d'un système de traitement d'information.

- *Bonne fin de projet* : couvre les conséquences de la "non arrivée" à bonne fin d'un projet informatique ; ces contrats sont assortis d'un nombre élevé de contraintes, sont réservés exclusivement aux SSII, peuvent se concevoir sous forme de contrats "dommages" pour un utilisateur final.

Cas particulier : "*l'assurance homme clé*" ; ils assurent, sous forme de versement d'un capital, les conséquences, pour l'entreprise, ou l'organisme employeur, de l'indisponibilité prolongée ou la disparition (décès) d'un collaborateur indispensable au bon fonctionnement d'un système pris au sens large. Attention aux nombreuses conditions du contrat et au régime fiscal en cas de versement du capital.

Un bon niveau de coopération entre les responsables informatiques et les personnes chargées de passer les contrats d'assurances peut clarifier et améliorer toute situation, en mettant l'accent sur le partage des responsabilités face aux risques.

Critères de qualité

Pour bien s'assurer, il faut :

- correctement effectuer l'inventaire des risques (emploi de méthode d'analyse de risques : par exemple, MARION et AROME),
- bien en estimer les conséquences s'ils se réalisent,
- analyser ce que vous pourriez supporter comme dommages ou pertes sans mettre en péril la "survie" de votre entreprise (est-il nécessaire d'assurer vos vieux PC 80286 ?).

Il faut faire une évaluation réelle du risque : le mode de calcul de la prime dépend des pertes financières résultant du sinistre (l'actif assuré sera-t-il totalement détruit ou non ?).

Ensuite et seulement ensuite, il convient de définir avec votre assureur le plan d'assurance destiné à prendre le relais pour les risques insupportables. Il faut privilégier les contrats de type "TOUT SAUF" et être très vigilant sur les exclusions qui sont bien mises en évidence. De plus, vous pouvez nuancer vos contrats, en faisant bien attention à certaines clauses ; à savoir : garanties/exclusions, capitaux assurés, montants des franchises, délai de préavis divers, délai de déclaration de sinistre.

Vérifiez aussi le statut de vos intermédiaires : agent d'assurance ou courtier ; l'agent d'assurance est mandataire de la compagnie qu'il représente alors que le courtier est mandataire de ses clients. En cas de doute, vous pouvez aussi vous référer à un professionnel de l'audit de contrat d'assurance.

Passer par un cabinet de courtage devrait offrir un meilleur service.

Tous les assureurs peuvent vous assister et vous conseiller utilement lors de la souscription du contrat.

Vous pouvez obtenir de meilleures conditions de garantie dès lors que vous regroupez tous vos contrats chez le même assureur et en lui faisant valoir une bonne qualité dans la gestion de vos risques.

Un point régulier entre les responsables informatiques et les personnes chargées de passer les contrats d'assurances doit permettre d'améliorer la situation.

N.B. : L'enquête menée par le S.G.C.B. a montré une certaine faiblesse sur ce point due au "maquis" des types de police et, sans doute, à un défaut de coopération entre les techniciens de l'informatique et ceux de l'assurance dans les banques.

Fiche 7 : Audit et contrôles

Définition

L'activité d'audit, qui peut être déclenchée pour les besoins d'un contrôle (ex : audit comptable, piste d'audit), permet :

- d'obtenir une appréciation générale de la qualité, de la pertinence d'un domaine d'activité,

- et de produire des recommandations visant à améliorer une des activités de l'entreprise.

L'activité de contrôle consiste à vérifier l'application des règles de gestion et d'exploitation de l'entreprise et, en cas de manquement, à faire prendre immédiatement les mesures correctives.

Les établissements de crédit et les maisons de titres sont soumis aux règlements édictés par le comité de la réglementation bancaire.

- Règlement n° 90-08 du 25 juillet 1990 qui fixe, pour les établissements assujettis, la nature des contrôles internes (voir annexes pour les implications techniques de sécurité informatique).

- Règlement n° 90-09 du 25 juillet 1990 relatif au risque de taux d'intérêt sur les opérations de marché (voir annexes pour les implications techniques de sécurité informatique).

- Règlement n° 91-04 du 16 janvier 1991 concernant l'organisation du système comptable et du dispositif de traitement de l'information des établissements de crédits et des maisons de titres (voir annexes pour les implications techniques de sécurité informatique).

Par ailleurs, chaque établissement se fixe des règles de fonctionnement et des objectifs internes.

Par conséquent, il est souhaitable que soit périodiquement contrôlée et auditée la réalisation des objectifs consignés, par exemple dans le schéma directeur de la sécurité du système d'information élaboré en fonction :

- des contraintes de pérennité, d'intégrité et de confidentialité des informations de l'entreprise, mais aussi afin de respecter,

- les contraintes légales de mise en œuvre des techniques de sécurité informatique (chiffrement, CNIL, ...).

La position administrative des instances d'audit et de contrôle doit être indépendante de l'informatique, afin qu'elles ne soient pas à la fois juge et partie. Les personnes chargées de ces fonctions doivent malgré tout posséder une grande technicité informatique, ce qui suppose une formation lourde et continue. Une veille permanente sur les travaux et chantiers que mènent les équipes informatiques permet, le moment venu, d'exercer un contrôle en connaissance de cause.

Risques

Dans le domaine de la sûreté d'exploitation du système d'information, les instances de contrôle et d'audit sont chargées de vérifier la conformité de mise en œuvre des mesures destinées au respect :

- des textes élaborés par le comité de la réglementation bancaire et aux obligations légales ;

  exemples : R 90-08 art. 2 - extrait - En ce qui concerne l'information comprise dans les comptes publiés, le système de contrôle interne doit garantir l'existence d'un ensemble de procédures, appelé piste d'audit, qui permet :

  a) de reconstituer dans un ordre chronologique les opérations ;

  b) de justifier toute information par une pièce d'origine à partir de laquelle il doit être possible de remonter par un cheminement ininterrompu au document de synthèse et réciproquement ;

  c) d'expliquer l'évolution des soldes d'un arrêté à l'autre par la conservation des mouvements ayant affecté les postes comptables.

  R 90-08 art. 3 - extrait - Les établissements assujettis élaborent et tiennent à jour un document qui précise les objectifs du contrôle interne et les moyens destinés à assurer cette fonction.

  R 91-04 art. 3 - Le contrôle des systèmes d'information s'étend à la documentation relative à l'analyse, à la programmation et à l'exécution des traitements.

- des règles et objectifs internes de l'établissement visant à maîtriser les risques.

  exemples : suivi de la mise en œuvre du schéma directeur de la sécurité du système d'information.

Pour le domaine de la sécurité des techniques informatiques, les risques sont d'exploiter des applications qui n'ont pas pris en compte les dimensions fonctionnelles de contrôle et d'audit.

Toutefois, les activités de contrôle et d'audit sont susceptibles d'induire des risques secondaires, comme provoquer des retards importants dans la livraison d'applications lorsqu'une direction tient à s'assurer du bon déroulement ou du bien-fondé de développement en cours. Mais l'expérience montre que l'intégration, dès l'étude préalable du projet, des aspects sécuritaires permet d'en diminuer le coût.

Parades

La permanence des missions d'audit et de contrôle est un élément déterminant de leur efficacité qui vise à détecter, le plus tôt possible, des dérives par rapport aux règles internes et externes. Par domaine d'activité, l'intervalle entre deux contrôles devra être ajusté pour minimiser le risque de recommandations tardives et coûteuses, voire d'éviter des constats d'échec. Par ailleurs, il est bon de prévoir des contrôles impromptus.

Les informations étant réglementairement soumises aux processus d'audit et de contrôle, il faut prévoir des mesures identiques sur les mécanismes informatiques et les structures qui automatisent la constitution du système d'information.

Pour l'aspect de "l'informatique moteur de l'audit" il faut veiller à intégrer les besoins de cette nature dès la conception d'un système ou d'une application.

Pour l'aspect du contrôle de l'activité informatique elle-même, il faut mettre en place une observation de plus en plus précise des événements qui s'y produisent. De la même manière que sont suivis les actes de production (horodatage d'exécution des travaux, opérateurs et données concernés, analyses des incidents ...) une précision identique peut être gérée pour les actes de développement (lien programmeur programme, lien programmeur poste de travail, horodatage module par module des étapes de réalisation : programmation, tests, recette, pré-exploitation, mise en production, maintenance). Cette précision suppose que l'on peut à la fois suivre et exploiter un historique (systèmes, machines, codes, ...).

Face au risque de perturbation d'un projet par un audit général, la méthode de développement utilisée doit produire, au cours de la réalisation, des éléments de suivi et de contrôle. Dès le lancement d'un projet informatique des points de décision doivent être prévus et à cette fin des éléments quantifiés seront produits pour apprécier que son intérêt demeure.

Critères de qualité

- Disponibilité d'une capacité d'audit et de contrôle (interne et externe).
- Auditeurs et contrôleurs formés aux techniques informatiques et utilisant des méthodes appropriées.
- Validation des développements liés à l'auditabilité de l'activité informatisée.
- Liste des événements et des informations consignés dans l'historique du développement et la production informatisée.
- Existence de critères systématiques pour lancer un audit (incidents, retards, montant du budget, alerte automatique, ...).
- Pratique de procédures aléatoires de contrôle et d'audit.
- Suivi par l'instance de contrôle de la mise en œuvre des recommandations.

Fiche 8 : Les consignes de sécurité

Les consignes affichées

Elles doivent être claires, précises, à jour, testées et doivent permettre de mettre en œuvre très rapidement les premières mesures d'urgence.

Les consignes de sécurité générale (urgences, SAMU, évacuation, ...) doivent être correctement affichées et testées de manière impromptue au moins une fois par an.

Il doit exister des consignes de sécurité physique spécifiques aux risques liés à l'informatique (incendie, dégâts des eaux, ...) correctement affichées et testées au moins deux fois par an.

Toutes ces consignes doivent faire l'objet de concertation, d'information, et de formation des personnels concernés.

C'est la Direction de la Sécurité qui est chargée d'assurer le suivi de l'ensemble des consignes.

Les consignes individuelles

Dans les locaux spécifiquement réservés à l'informatique, c'est le responsable hiérarchique qui doit prendre soin de nommer des équipes spécialisées en matière d'incendie et d'évacuation du personnel. Chacun des membres de son personnel doit recevoir ses propres instructions après avoir éventuellement subi une formation adéquate. Les tests doivent avoir lieu au minimum deux fois l'an.

Chacun travaillant dorénavant avec son propre micro-ordinateur, doit recevoir nommément les consignes de sécurité du système d'information de l'entreprise. Ces dernières ont pour objet de veiller à garantir en permanence la confidentialité, l'intégrité et la disponibilité du système d'information.

Adressées nominativement, ces consignes de sécurité permettent une meilleure compréhension de la sécurité globale de l'information dans l'entreprise.

Rappel des principales consignes en matière de sécurité micro :

- la protection du poste de travail, en empêchant tout accès à votre insu,
- la non communication des mots de passe,
- la sauvegarde de vos données, bien rangée à l'abri de tout ...
- le recensement de vos fichiers,
- le nettoyage périodique de votre disque dur ("faire le ménage"),
- l'attention aux logiciels que vous installez : ils peuvent receler des virus informatiques susceptibles de provoquer des destructions de données,

- l'installation et/ou l'utilisation de logiciels "pirates", c'est-à-dire pour lesquels les droits n'ont pas été régulièrement acquis, sont rigoureusement interdites quelles que soient les circonstances [voir fiche 4 "Aspects juridiques"],

- le respect des dispositions légales ; votre responsabilité juridique personnelle peut être directement engagée :

  * par la loi "Informatique et Libertés" du 06.01.1978, pour les infractions liées à la détention et à l'utilisation illicites de données nominatives,

  * par la loi sur la "Protection des Logiciels et Progiciels" du 03.07.1985, pour toute reproduction ou utilisation de logiciels non autorisées,

  * par la loi sur la "Fraude Informatique" du 05.01.1988, pour tout accès -ou tentative d'accès- frauduleux à un système informatique, même en l'absence d'altération du fonctionnement de ce système.

C'est le responsable de la Sécurité Informatique qui doit être chargé de maintenir l'ensemble des consignes touchant à la micro-informatique.

Fiche 9 : Contrôles d'accès logique

Définition

Moyen de reconnaissance en deux temps : l'identification et l'authentification, qui repose sur un dialogue entre l'utilisateur au sens large et une procédure gérée par un calculateur. Le premier temps consiste à décliner une identité qui n'est pas nécessairement une information secrète. Si l'ordinateur la reconnaît le second temps du dialogue consiste à demander une preuve associée à cette identité. Cette information ne peut a priori être fournie que par le bon individu. Si l'ordinateur vérifie la validité de l'association identifiant et preuve, il permet alors l'usage des ressources qui ont été affectées à cet identifiant.

Les identifiants sont généralement liés à la personne (nom, surnom, matricule) ou à la fonction (sigle du service et numéro d'ordre). C'est une information réclamée à l'utilisateur ou lue sur un support magnétique qu'il détient. L'authentifiant est souvent un mot de passe, d'autres solutions plus sophistiquées existent, par exemple la carte à mémoire ou la calculette qui sait répondre pertinemment à un aléa généré par l'ordinateur.

Lorsque cette personnalisation de l'accès n'est pas adaptée, on peut trouver des contrôles d'accès basés sur d'autres critères, par exemple la localisation géographique du point d'où provient la demande d'accès (reconnaissance de l'adresse du terminal), la détermination des droits en fonction de l'identifiant seulement ou la validité de la plage horaire pendant laquelle l'accès est tenté.

Les exigences de sécurité peuvent amener à combiner toutes ces procédures de contrôle d'accès.

Risques

Le principal est la possibilité pour une personne mal intentionnée d'élucider le couple identifiant-authentifiant.

Le mauvais respect des règles de gestion des procédures d'accès par les utilisateurs est aussi un facteur de risques. Il se produit lorsque les procédures sont nombreuses et incohérentes (par exemple identifiants et mots de passe de structures différentes depuis la station de travail, pour l'accès à l'émulation, l'accès au réseau, l'accès au serveur, l'accès à l'application et à certaines fonctions ou données consultées dans l'application ; et ceci pour les derniers niveaux multiplié par le nombre d'applications consultées depuis le poste de travail). Cette complexité incite l'utilisateur à se cantonner dans des solutions triviales qui augmentent la vulnérabilité des systèmes.

L'utilisateur peut aussi, par étourderie ou précipitation, s'éloigner de son poste de travail après avoir franchi toutes les barrières d'accès : il le laisse ainsi totalement vulnérable.

Parades

Certains identifiants sensibles comme ceux des gestionnaires de la sécurité ou des spécialistes système peuvent être tenus secrets et avoir une structure non explicite. Les bénéficiaires doivent être conscients de ce fait et les emplois de ces identifiants doivent être "tracés".

La détermination de l'authentifiant peut être rendue plus difficile en évitant que les mots de passe soient stockés en clair dans le système informatique et qu'ils transitent en clair sur les lignes de télécommunication. Les solutions classiques par mots de passe n'ont pas ces qualités, la calculette qui sait répondre à un aléa, les a. De plus, si le fonctionnement de la calculette personnelle dépend de la communication d'un code personnel, les détournements d'usage à la suite d'un vol seront évités.

La tentative d'intrusion par usage de la contrainte sur l'utilisateur peut trouver sa parade par l'emploi d'un couple d'identifiant-authentifiant de substitution qui génère une alerte auprès d'un centre de sécurité tout en préservant l'utilisateur.

Le risque de mauvaise gestion des procédures d'accès dû à leur multiplication trouve sa solution dans la mise en place d'un serveur de sécurité qui donne l'ensemble des accès à partir d'une seule identification-authentification. La mise en place d'une telle solution optimale reste aujourd'hui complexe et contraignante car elle introduit un point extrêmement sensible dans le réseau.

Pour se rapprocher de cette solution où l'utilisateur n'a qu'un seul identifiant-authentifiant, il faut d'abord avoir un seul référentiel de sécurité et reporter autant que possible le contrôle sur un outil unique et spécialisé de gestion des habilitations.

L'abandon involontaire d'un poste démuni de ses protections peut se contrer par la technique de la mise en veille (time-out). Après une durée prédéterminée d'inaction la session de travail ne peut être reprise qu'en réintroduisant un authentifiant valable. L'écran peut à cette occasion s'effacer ou afficher une mire pour préserver la confidentialité de l'affichage applicatif. Il est aussi possible de proposer une fonction de mise en veille activée par l'utilisateur pour lui permettre d'abandonner rapidement son poste de travail tout en préservant la sécurité du système informatique.

Critères de qualité

- la disposition d'un règlement sur les consignes de confidentialité à appliquer aux mots de passe,

- le chiffrement des mots de passe en stockage et en dialogue,

- l'analyse de l'adéquation du contrôle d'accès à la sensibilité du système accédé,

- le niveau de gestion du mot de passe (fréquence de renouvellement ; diversité des mots successifs ; syntaxe ; éléments de structure comme la présence de chiffres ou la longueur > 6 caractères ...),

- l'existence d'une procédure d'alerte en cas d'accès sous contrainte,

- le niveau de la gestion des exceptions (révocation après plusieurs tentatives ; temporisation dans le dialogue pour contrer les tentatives d'intrusion par des essais automatisés ...),

- le suivi du nombre moyen de couple identifiant-authentifiant gérés par les utilisateurs (indicateur de confort et d'efficacité du contrôle d'accès).

Fiche 10 : Contrôles d'accès physique

Définition

Sous le syntagme "contrôle d'accès physique", il est habituel de regrouper l'ensemble des moyens passifs ou actifs qui permettent de contrôler la circulation des personnes, des véhicules et des marchandises au sein de l'entreprise et à sa périphérie. Les fonctions développées dans ce cadre sont des fonctions de détection d'intrusion, de contrôle d'accès proprement dit, de gardiennage, de surveillance et de télésurveillance. La chaîne de sécurité est constituée par les maillons suivants :

- détection d'intrusion : elle permet le repérage de toute présence humaine, qu'elle soit normale ou anormale, dans une zone donnée,

- télésurveillance et/ou gardiennage : l'un ou l'autre de ces moyens permettent une levée de doute sur les intrusions signalées par les systèmes de détection, ou une intervention sur toute situation paraissant anormale,

- contrôle d'accès : ces dispositifs permettent de canaliser et reconnaître les flux de circulation indiqués ci-dessus. Ils permettent d'assurer l'identification et surtout l'authentification des personnes. Ils permettent également de gérer les habilitations qui leur sont accordées en fonction de leurs activités dans l'entreprise. Cela passe pour les personnes pénétrant dans l'entreprise par le fait de devoir se présenter à un agent de l'entreprise (personnel de sécurité ou hôtesse) ou à un équipement.

Les risques encourus sont de toutes natures :

- intégrité : risque de sabotage des données et/ou matériels par des tiers extérieurs, ou des personnels de l'entreprise, si les droits d'accès aux zones sensibles ne sont pas distribués avec une rigueur suffisante,

- confidentialité : risque d'accès à des documents confidentiels par des tiers extérieurs à l'entreprise ou des personnels de l'entreprise n'ayant pas à en connaître,

- pérennité : malveillance de tous types, risque de mauvaise manipulation volontaire ou involontaire par des tiers extérieurs à l'entreprise ou des personnels de l'entreprise.

Parades

Pour être efficace, cette chaîne de sécurité repose sur une analyse préalable des besoins de sécurité de l'entreprise et sur une adaptation des flux de circulation dans l'entreprise aux besoins de sécurité ainsi recensés. La conception à privilégier est celle des cercles concentriques. C'est-à-dire que les zones les plus sensibles, qui sont en général les zones les moins souvent accédées, doivent se trouver entourées par les zones moins sensibles. De cette façon, les atteindre demande de franchir un certain nombre de barrages, matérialisés par des systèmes de contrôle d'accès. Les locaux contenant les équipements les plus sensibles (CPU, unités de disques, etc.)

se trouvent aussi les moins fréquemment accédés alors que les locaux où le niveau d'intervention humaine est plus élevé (impression, façonnage, etc.) seront accessibles à un plus grand nombre de personnes.

Il est préférable de combiner plusieurs des moyens énumérés ci-dessus pour obtenir un meilleur niveau de sécurité :

- Le système de détection d'intrusion est destiné à permettre une détection de toute présence anormale, soit en fonction du lieu où elle est signalée (salle d'unités informatiques mortes, locaux techniques, etc.), soit en fonction de l'heure (nuit, jours fériés, etc.). Les moyens mis en œuvre sont des détecteurs de mouvements utilisant diverses technologies (infrarouges, micro-ondes, etc.). Son couplage avec un système de vidéo surveillance permettant l'enregistrement et la transmission d'images améliore son efficacité.

- L'exploitation rationnelle des anomalies reconnues par les systèmes de détection repose sur les fonctions de gardiennage et de télésurveillance. L'intervention aussi rapide que possible d'agents de sécurité de l'entreprise ou de sociétés tierces permet, si le système de détection est bien conçu, d'agir avant que le coeur du système ne soit atteint. L'utilisation de moyens vidéo, tels que des caméras disposées aux endroits sensibles, et au minimum sur les accès, est recommandable et permet la surveillance globale de l'entreprise à partir d'un point unique (Poste de sécurité).

- Le système de contrôle d'accès permet de filtrer les personnes et les véhicules qui manifestent l'intention d'accéder à l'entreprise. Toutes les personnes et tous les types d'intervenants dans l'entreprise doivent être pris en compte et effectivement contrôlés : personnel, sociétés de services, visiteurs, livreurs, etc. La routine ne doit jamais guider la délivrance des droits d'accès et la circulation des visiteurs et des prestataires de service doit être particulièrement surveillée. Il est recommandable d'être doté d'un système de contrôle des accès à base de sas et de lecteurs de badges (diverses technologies sont disponibles) permettant la reconnaissance individuelle du porteur et l'enregistrement des anomalies constatées par le système. La mise en place d'une fonction accueil permet d'associer sécurité et qualité dans la gestion des visiteurs. Tous les locaux considérés comme stratégiques doivent être dotés du système.

Pour assurer le fonctionnement des systèmes, ceux-ci doivent être gérés, administrés et contrôlés. En particulier, une procédure formalisée de délivrance des habilitations, responsabilisant la hiérarchie et fournissant une piste d'audit, doit être mise en œuvre. Les procédures de dépannage à mettre en œuvre en cas de perte de badge par le personnel de l'entreprise doivent être formalisées et connues. Il convient également d'assurer le suivi des systèmes et en particulier des détections de violation. C'est l'organisation propre de l'entreprise qui guide l'attribution de ces fonctions à tel ou tel service.

Il faut prendre garde au fait qu'un tel système de contrôle d'accès, géré sur informatique, doit respecter la loi sur l'informatique et les libertés et faire l'objet d'une déclaration préalable auprès de la CNIL.

Critères de qualité

Il s'agit de suivre via un tableau de bord des indicateurs tels que :

- nombre d'incidents réels détectés,
- nombre de badges d'accès perdus,
- nombre de pannes du système de contrôle d'accès.

Le bien-fondé des habilitations délivrées doit être examiné périodiquement, entraînant leur réajustage. Le cas échéant, un listage périodique peut être remis aux responsables hiérarchiques concernés. Il revient au service sécurité de l'entreprise de se préoccuper de ce contrôle. La gestion du système de sécurité doit se faire en temps aussi réel que possible. En particulier, les départs ou changements d'affectation de personnel doivent être traités sans délai.

Comme pour tout moyen de sécurité, de mauvais comportements humains peuvent annihiler les effets attendus. Aussi, on s'assurera que :

- les portes ne restent pas bloquées en position ouverte pour quelque raison que ce soit,

- les badges ne font pas l'objet de prêts entre employés (ce point devrait relever du règlement intérieur),

- les procédures d'accès font l'objet de règles écrites, diffusées et connues du personnel et, plus généralement, des personnes dont le lieu de travail habituel ou temporaire est l'entreprise,

- l'existence de moyens de vidéo surveillance a été portée à la connaissance du personnel,

- le personnel a fait l'objet de campagnes d'information relatives au système mis en place et à son utilité pour l'entreprise.

Fiche 11 : Contrôles programmés

Définition

Les contrôles programmés, représentent l'ensemble des contrôles qui peuvent être introduits dans des programmes informatiques et qui complètent, le plus exhaustivement possible, les contrôles manuels et permanents réalisés par les différents services de l'entreprise.

Ces contrôles peuvent se différencier en deux familles selon qu'ils méritent d'interrompre ou non les traitements. Si l'anomalie constatée est grave et constitue un risque sérieux d'incohérence de traitement et de résultat, le concepteur devra prévoir un contrôle bloquant. Dans les autres cas de détection d'anomalies, une alerte sera signifiée au gestionnaire sans pour autant interrompre le traitement. Charge à lui d'entreprendre l'action de validation ou de correction.

Ces contrôles traitent :

- de l'origine, (authentification, certification, non-répudiation des éléments d'entrées),
- de la validité des entrées (dates des mouvements, code émetteur/code client),
- de la cohérence des données, (des dates, des montants),
- de la vraisemblance des entrées, (client et produit existants),
- de la qualité et de la pertinence des sorties, (édition à bonne date, bon document, bonne imprimante),
- de l'exactitude des résultats, (balance carrée, calculs croisés, procédure de recalcul),
- du bon déroulement du processus (enchaînement exact des traitements, état de contrôle).

En s'appuyant sur la classification des données définie dans l'entreprise, les contrôles peuvent aussi gérer les accès, les authentifications et les habilitations. Des progiciels spécialisés existent sur le "marché", pour répondre à ces fonctionnalités. Selon les constructeurs informatiques, le choix est plus ou moins varié. Il est souvent préférable de les privilégier au développement interne car ils sont opérationnels immédiatement. L'acquisition ne dispense en aucune manière d'une étude interne et d'une expression de besoin.

Dès lors qu'une application informatique possède des éléments quantitatifs et factuels permettant de contrôler son bon déroulement, il est recommandé d'intégrer ces contrôles dans les programmes pour les systématiser et les automatiser.

Les contrôles programmés limitent l'intervention humaine en favorisant l'automatisation, stabilisent le résultat des traitements, autorisent le déroulement des applications en l'absence de personnel. La généralisation et la normalisation de contrôles programmés garantissent la cohérence des contrôles dans l'ensemble du système d'information.

Cette démarche doit s'accompagner dans l'entreprise d'une action méthodologique et normative. Ainsi, dans les spécifications applicatives, doit-on posséder des modèles conceptuels généralisables, pour aborder ces interrogations très tôt dans le cycle de

développement. L'utilisation de référentiels et de paramètres de contrôles (format, dates, bornes, etc.) facilitent la mise en œuvre de modules de contrôles réutilisables.

Trop de contrôles pourraient-ils nuire à la performance des développements ou des traitements ? S'ils répondent essentiellement à des risques évidents et confortent l'enjeu applicatif, ils sont certainement utiles. Les contrôles peuvent être améliorés et adaptés par les maintenances au gré des faiblesses constatées. Il faut noter cependant que les coût globaux de la sécurité sont nettement moindres si les risques sont appréhendés dès la conception et les contrôles intégrés dès la réalisation.

Il est donc conseillé d'avoir une méthode de développement comportant un volet sécurité obligatoire.

Risques

L'absence ou l'insuffisance de contrôles programmés ne permet pas de garantir une qualité constante du processus fonctionnel. La disponibilité, l'intégrité et la confidentialité du système d'information sont étroitement dépendantes du niveau des contrôles programmés intégrés dans les traitements.

Lorsque les contrôles sont laissés à l'appréciation des individus, leurs exécutions sont aléatoires et le jugement instable. Il peut s'ensuivre des erreurs importantes non détectées, qui pénalisent la gestion de l'entreprise et les clients. Des personnes mal-intentionnées pourraient, également, utiliser cette faiblesse pour s'introduire dans le système d'information et perpétrer des actes de malveillances ou des fraudes.

Enfin, des contrôles d'entrées insuffisants facilitent l'enregistrement de données incorrectes, entraînent des perturbations dans les traitements, et provoquent une pollution du système d'information.

Parades

Il faut inventorier, dès l'analyse de l'applicatif, tous les contrôles possibles qui peuvent être systématisés et automatisés. C'est une recherche qui entre dans la démarche d'une sécurité intégrée dans la conception d'application.

Les personnes participant au projet doivent être sensibilisées et formées à cette démarche. Les auditeurs doivent être associés à cette réflexion pour l'enrichir de leurs besoins et de leurs recommandations.

La classification des données est une réflexion importante sur laquelle va reposer une grande partie des contrôles. La notion d'authentification et d'habilitation est une autre étape autorisant l'automatisation des contrôles.

Des règles générales de contrôles des entrées doivent être établies et normalisées. Des modules généraux, mis en bibliothèque, peuvent reprendre l'application de ces contrôles.

Les procédures de mise en exploitation et de validation des maintenances doivent intégrer une revue des contrôles programmés.

Un suivi applicatif sérieux et des tableaux de bord de production permettent de suivre en permanence la qualité des traitements.

Des pistes d'audit devront être mises en œuvre, avec les éléments contrôlés, pour s'assurer de l'exécution convenable des processus de traitement.

Un audit périodique interne des contrôles programmés est toutefois nécessaire pour se garantir d'une dérive dans les nouvelles applications ou dans les programmes maintenus.

Critères de qualité

Les tableaux de bord font ressortir un taux d'anomalies minimum dans les services utilisateurs et à l'informatique (les risques d'erreurs et de malveillance sont très limités).

Les normes de développement intègrent les définitions des contrôles programmés, et les outils proposent les modules généraux de contrôle.

Les auditeurs participent à la définition des contrôles programmés et valident les pistes d'audit.

Les contrôles d'accès au système d'information et les habilitations sont gérés totalement, et de manière satisfaisante, par les traitements informatiques.

N.B. : L'enquête menée par le S.G.C.B. signale qu'il s'agit, ici, habituellement, d'un point faible.

Fiche 12 : Développements externes

Définition

Les développements informatiques peuvent être confiés, selon différentes modalités, à des personnes n'appartenant pas à l'entreprise :

- du personnel extérieur travaille dans vos locaux, il est embauché par l'intermédiaire d'une société de service, il fournit une assistance technique extérieure (ATE) ; cette assistance peut prendre la forme d'un travail en régie avec une grande intégration dans les équipes internes ;

- la totalité d'un développement est confiée à une société de service, sous la forme d'un forfait, son personnel n'est pas nécessairement intégré aux équipes internes ;

- seules les opérations de maintenance sont confiées à des sociétés extérieures (prestation désignée sous le nom de TMA Tierce Maintenance Applicative) ;

- les développements sont faits avec et autour d'un progiciel, l'interlocuteur étant alors le fournisseur du logiciel.

Risques

Dans ces différents cas, des risques particuliers existent.

- Le *personnel externe* peut manquer d'expérience dans votre domaine professionnel. Il peut être un sous-traitant de votre interlocuteur avec les contraintes et les difficultés que peut entraîner une cascade de contrats. Les relations avec le personnel interne peuvent devenir difficiles si le taux de personnel extérieur est important. Le personnel interne peut alors se transformer en recruteur, en superviseur, en intermédiaire ou en "bouche-trou" pour les tâches non explicitement prévues au contrat. Il est parfois difficile de segmenter le travail pour que le personnel extérieur reste cantonné dans un domaine non sensible. Le droit du travail réglemente les relations entre l'entreprise et ces travailleurs qui viennent ainsi renforcer ses effectifs. En cas d'infraction, les sanctions peuvent s'accompagner d'une obligation d'embaucher un personnel extérieur qui manifestement occupe un poste à caractère permanent.

- Un *travail confié au forfait* présente un risque financier si les différents niveaux de description ne restent pas parfaitement cohérents au long du projet (entre l'étude préalable et les spécifications par exemple).

- Dans le cas d'une *maintenance confiée à l'extérieur*, la formule peut apporter plus de rigueur dans les demandes. Le service rendu sera de qualité s'il reste rentable pour le prestataire ; il faudra donc éviter d'emploi d'outils exotiques et des taux d'intervention qui deviennent trop faibles pour justifier l'entretien d'une compétence.

- Le *recours au progiciel* correspond en principe à l'adoption d'une méthode de travail déjà familière à beaucoup d'entreprises. Toutefois, si l'on se distingue des acheteurs antérieurs, il y a un risque d'acquérir une solution qu'on ne pourra pas facilement faire évoluer, ou seulement au prix d'interventions spécifiques réalisées par des personnes non spécialistes des développements sur mesure. Il faut donc prêter une grande attention à l'achat d'un logiciel "exotique" par rapport aux "standards" du marché.
  Enfin, il est rare qu'un progiciel obéisse aux normes internes relatives à la codification des données, aux règles de programmation et de mise en production (par exemple critères de lisibilité des programmes et de mise en production module par module).

Parades

• Pour le *personnel extérieur*, il s'agit de conserver autant que faire se peut la maîtrise de cette force de travail. Un contrat unique et direct est préférable à un enchaînement de sous-traitance. Les dates de fin de prestation doivent être étudiées en fonction des étapes d'un projet. Il faut synchroniser les travaux confiés et les tâches induites en interne pour ne pas laisser un prestataire en sous-charge et pour lui permettre de rendre un travail bouclé (recetté et documenté). Les ressources mises à disposition doivent faire l'objet d'un PV à l'arrivée et au départ. Les autorisations d'accès doivent immédiatement être supprimées au départ du prestataire et une trace des documents sensibles qui ont été communiqués et étudiés doit être conservée. Enfin, les contrats doivent être établis pour des durées adaptées aux prestations attendues et expertisées sous tous les aspects (notamment juridiques ou législation du travail).

• Pour un *travail au forfait*, une expression fonctionnelle en terme de besoins à satisfaire peut éviter des discussions sur le gonflement du travail à réaliser.

• Une bonne visibilité doit être conservée sur les développements demandés dans une relation de *tierce maintenance applicative*. Ceci ne peut s'obtenir que par des interventions de techniciens entre les demandes des utilisateurs et les propositions de réalisation de la société de TMA. Des remises en cause périodiques de cette formule sont souhaitables, lors, par exemple, d'un nouveau développement où des hypothèses alternatives doivent être étudiées.

Dans tous les cas de relation avec des partenaires extérieurs, il convient d'imposer des clauses de confidentialité et de restitution de documents dans les contrats.

Dans ces trois premiers cas de développements externes, un problème de propriété du résultat peut, en plus, se poser. Cette propriété n'est pas toujours facile à attribuer rétroactivement ; elle dépend de la précision de la commande passée. Pour ne pas avoir à en débattre devant les tribunaux, il est prudent d'étudier cette question dès la rédaction des contrats.

• L'inertie naturelle liée à *l'emploi des progiciels* peut être compensée par le degré d'ouverture du progiciel : si son organisation interne (structure des bases de données, possibilité de greffer des programmes ...) est connue, des développements périphériques seront plus faciles et moins risqués. De même, l'évolutivité du coeur du produit dépend souvent de la pression d'un club d'utilisateur. Le dynamisme de ce club exprimé en nombre de résolutions acceptées par le fournisseur est à évaluer avant toute décision. Pour le cas où des difficultés naîtraient avec le fournisseur, des solutions de continuité doivent être prévues dès l'origine : le dépôt des programmes source est un minimum, un accord avec une entreprise de plus grande envergure est une meilleure garantie.

L'impact du non-respect des normes internes doit être apprécié dès que possible : il peut être un élément déterminant dans le choix d'un produit.

Critères de qualité

- Pour les ATE :

  - gestion d'un fichier des prestations (sujet, coût, technicité, satisfaction, documents consultés, documents produits),

  - délai de mise à disposition et de reprise des ressources,

  - maîtrise du taux d'ATE dans les équipes de projet,

  - respect de la nature souhaitée pour la prestation (renfort en nombre, transfert de technologie),

  - renfort de l'activité de recette en interne.

- Pour les forfaits :

  - maîtrise du nombre d'avenants au contrat.

- Pour la TMA :

  - réalité de la possibilité de mise en concurrence des prestataires,
  - amélioration des documentations des applications pour garder la visibilité sur ce qui est réalisé.

- Pour les progiciels :

  - activité du club d'utilisateur,
  - réalité des évolutions réalisées dans le cadre du contrat de maintenance.

[voir aussi fiche 16 "Facilities Management ; outsourcing"]

Fiche 13 : Downsizing et réseaux locaux

Définition

Le downsizing peut être associé à l'émergence de la micro-informatique, qui a généré ses informaticiens, renforcée par la baisse des coûts des matériels et l'apparition des réseaux locaux qui ont donné des raisons économiques et techniques pour tenter de reproduire sur ce type d'architecture les services que rendaient les ordinateurs centraux. Dans un premier temps l'offre sur réseaux locaux pouvait être qualifiée de "propriétaire" c'est-à-dire qu'il était préférable de s'équiper avec les solutions d'un même fournisseur pour être assuré d'un bon fonctionnement d'ensemble. Aujourd'hui avec le progrès de la normalisation et de l'interopérabilité le champ des solutions pour le downsizing s'élargit.

Dans la suite du texte nous ferons essentiellement référence aux développements sur réseaux locaux de PC, le downsizing étant aussi bien le choix de cette solution technique pour un nouveau développement que la migration d'une application centralisée vers cette architecture.

Une opération de downsizing ne doit pas s'analyser de la même manière selon qu'elle correspond à un choix technique et économique fait par des informaticiens professionnels ou qu'il s'agit à l'opposé d'une évolution en volume et espace de développements faits par les utilisateurs avec des logiciels grand public.

Risques

Les risques associés au Downsizing sont de plusieurs ordres :

Techniques :

Du fait de contraintes techniques, la couverture géographique des réseaux locaux n'est généralement pas celle d'un habituel réseau associé à un ordinateur central. Paradoxalement, elle peut donc se révéler inadaptée à certains groupes de travail ou à leur évolution. La mise en communication de plusieurs réseaux locaux ne peut pas se faire sans recourir aux spécialistes dont on pensait pouvoir se passer et dont l'exclusion constituait un élément économique favorable.

Un autre risque technique peut provenir de la pression commerciale ou plus exactement de l'engrenage que constituent les évolutions imposées par l'obsolescence rapide des produits de la micro-informatique. En effet une opération de downsizing impose encore la juxtaposition de nombreux composants (outil "client" sur le poste de travail, interface réseau, gestionnaire de réseau, serveur de fichier, serveur de données, éventuellement serveur de communication) qui sont en perpétuelle évolution (ajout de fonctionnalités, corrections de défauts) et, de plus, présentent fréquemment entre eux des incompatibilités (connues et maîtrisées par quelques rares spécialistes de l'intégration de logiciels micro). La demande de l'utilisateur qui a entraîné l'opération de downsizing ne s'éteint pas lorsqu'il reçoit ses équipements ; aujourd'hui les solutions qui sont en place depuis quelques années subissent une pression pour intégrer des interfaces graphiques de type Windows. La demande d'alignement sur la nouveauté commerciale est à contenir.

Humains :

Il y a d'abord la question des spécialistes systèmes. C'est le grand reproche adressé aux systèmes centralisés qui semblaient engendrer et entretenir des spécialistes ésotériques. On s'aperçoit à l'usage que ces spécialistes sont incontournables, nous les avons évoqués pour les liens entre réseaux, les installations elles-mêmes réclament leur intervention et leur contrôle. Le plein emploi des logiciels gestionnaires de réseau demande des compétences équivalentes, il en est de même pour le bon emploi des outils professionnels qui existent sur ces architectures (des SGBDR tels que SYBASE ou ORACLE ne se considèrent pas en concurrence avec PARADOX ou ACCESS, l'emploi correct des premiers requiert des compétences analogues à celles exigées des spécialistes DB2 sur gros système). Si les développeurs proviennent des services utilisateurs l'acquisition de telles connaissances représente une déperdition importante au niveau de l'entreprise.

Les architectures de type "downsizing" entretiennent l'ambiguïté sur la façon de développer, il peut s'agir d'une extension d'une approche personnelle avec des risques importants tels que la sous-estimation de l'investissement réalisé. Cette sous-estimation entraîne la négligence d'aspects considérés comme annexes -documentation des applications, procédures de recette, protection des équipements- et se prolonge par une absence de gestion du patrimoine -l'auteur disparaît sans passer le relais, ou au contraire reste (à vie) l'unique soutien à sa réalisation-. L'absence de conduite, avec méthode, d'un projet peut entraîner un manque de fiabilité du résultat et une grande dépendance par rapport à son auteur. Le downsizing, dans la mesure où il illustre la culture de l'informatique personnelle présente ce risque pour l'entreprise.

Intégrité :

La multiplication d'applications sur des architectures techniques réduites en taille, séparées, et placées sous des responsabilités décentralisées complique la maîtrise qu'une entreprise doit avoir de son système d'information. Les évolutions divergentes sont facilitées par cet éclatement des ressources et des compétences, elles peuvent mettre en péril l'intégrité générale des données gérées par l'entreprise. Pour le moins, elles compliquent les fonctions centralisées d'administration des données et d'administration de la sécurité. Sur le thème de l'intégrité rappelons que les matériels et systèmes retenus pour les opérations de downsizing sont extrêmement sensibles aux virus (ce risque porte aussi sur la disponibilité - voir rubrique micro-informatique). Il faut également prendre garde aux risques liés à la facilité d'accès (physique ou logique) aux serveurs de données et de communications (intrusion, sabotage...).

Parades

Il s'agit de retrouver les avantages annoncés du downsizing -ergonomie et faible coût- totalement ou en partie avec les solutions nouvelles ou des compléments d'organisation. La tendance actuelle à la normalisation est déjà une réponse du marché sous la pression des utilisateurs qui ont vécu des situations difficiles. Les architectures techniques qui utilisent des systèmes intermédiaires, moins vulnérables aux virus, basées sur des machines UNIX offrent des avantages comparables (concurrence et baisse des coûts, interface graphique ergonomique).

Pour lutter contre la fuite en avant commerciale, l'entreprise doit se doter d'une cellule pour choisir les matériels et logiciels. Si elle ne peut pas éviter les migrations, cette cellule pourra au moins les organiser et donc en réduire le nombre (synchronisation des migrations).

Le risque humain doit être traité comme il l'a été pour l'informatique centralisée qui, elle aussi, a connu son époque de pionniers et de découvreurs. Les méthodes de développements de projets informatiques ne doivent pas différer pour les phases, les contrôles, les points de passage obligés, selon la plate-forme technique qui en accueillera le résultat. Pour les réseaux locaux, en tant que centres de production informatique, on ne dispose pas encore de méthode d'évaluation de leur sécurité même si l'on peut d'ores et déjà s'entourer de précautions telles que des locaux sécurisés pour les serveurs. Il faut donc bien compenser dès que possible, les effets néfastes d'une approche de type informatique personnelle par une plus grande vigilance dans les développements en intégrant les préoccupations de sécurité aux développements comme le pratiquent les meilleurs professionnels.

Critères de qualité

- Mesure du coût total d'une opération de downsizing (y compris les reports de coûts de fonctionnement sur les utilisateurs = exploitation, gestion technique...).

- Possibilité de retour arrière en cas de migration depuis une solution centralisée.

- Conservation et mise en commun des compétences acquises (logiciels de gestion de réseau local, SGBDR de réseau local).

Voir aussi fiche n° 30

Fiche 14 : E.D.I.

Définition

L'Échange de Données Informatisé est un transfert de données, suivant des standards préétablis de messages, d'ordinateur à ordinateur par des moyens électroniques. Un système E.D.I. concerne généralement des partenaires juridiquement distincts. Destiné à supprimer les échanges sur d'autres supports, dont le papier, tout en conservant une même qualité sur le plan de la sécurité, un tel système doit s'intégrer dans les systèmes informatiques des partenaires pour qu'ils en tirent le meilleur profit -service continu, réaction immédiate, production en flux tendu, suppression des interventions manuelles...-.

Risques

Les risques associés à l'E.D.I. sont de plusieurs ordres :

Stratégique :

Se révéler incapable de suivre le rythme de mise en place de cette technique peut faire qu'une entreprise s'exclue d'elle-même du groupe de partenaires que constitue son milieu professionnel, concurrentiel.

De même un sous-emploi des conséquences économiques favorables que génère la bonne intégration de l'E.D.I. dans le système informatique de l'entreprise peut détériorer sa position concurrentielle (réception en continu de messages mais traitement aval par lot à heure fixe faute d'avoir adapté les applications concernées).

A contrario, l'E.D.I. offre des opportunités. Il peut permettre à une banque d'offrir un service permanent et en temps réel à sa clientèle, ce qui peut constituer temporairement un avantage compétitif.

Techniques :

L'E.D.I. s'appuie sur les télétransmissions qui présentent elles-mêmes des points de faiblesses :

- le recours à des spécialistes pointus sur lesquels un contrôle n'est pas aisé et qui ont parfois des autorisations de haut niveau ;

- la complexité technique qui est encore une caractéristique des télécommunications et qui fragilise les systèmes qui en font un usage exclusif.

L'E.D.I. apporte sa manière de coder les messages, c'est la couche de protocole de transmissions de messages :

- Pour cette couche plusieurs choix sont parfois possibles. Mais, il convient de noter que les protocoles les plus simples -donc les moins chers à mettre en œuvre-, sacrifient souvent la sécurité. Il y a un risque que dans les offres commerciales les mauvaises solutions chassent les bonnes.
- Dans ces protocoles, les incidents de pertes d'informations ou d'erreurs de destination ne sont pas toujours parfaitement traités. Ainsi une perte partielle de

message endommagera l'intégrité de la base de données en réception, une perte totale diminuera la disponibilité du système et un mauvais aiguillage portera atteinte à la confidentialité de l'échange.

L'E.D.I. par son principe d'intégration dans le SI récepteur constitue une fenêtre ouverte dans laquelle peuvent s'engouffrer des flux perturbateurs. L'entreprise qui ne maîtriserait pas son E.D.I. peut se rendre perméable aux intrusions. Dans cette situation elle recevra des flux indésirables qui peuvent être très nombreux et dont le traitement correctif (correction de bases de données ou pire contentieux divers) non anticipés restent manuels.

Juridique :

Les échanges classiques entre entreprises partenaires dans un processus productif bénéficient d'un cadre contractuel et juridique rôdé et efficace. L'E.D.I. doit reconstituer un contexte équivalent. Des juristes se sont déjà penchés sur cette question pour déterminer la valeur juridique d'une télétransmission des factures et des déclarations fiscales, des projets de loi ont déjà traité ces questions liées à la dématérialisation. La solution E.D.I. à retenir ne doit pas dégrader ces valeurs juridiques ou contractuelles des échanges. Or les télétransmissions n'offrent pas les mêmes qualités de support d'information et se prêtent à certains types d'actes de malveillance. Ainsi l'authentification d'un émetteur se fera grâce au protocole d'envoi d'un message et non dans le message lui-même. Des systèmes de signature électronique ont été imaginés, ils peuvent à la fois prouver une origine et l'intégrité du contenu (sceau) mais ils ne correspondent pas encore à une signature papier indissociable du message qu'elle conclue. Pour les malveillances, la répudiation, refus de reconnaître un envoi ou une réception, est possible et doit être contrée. Une autre technique perturbatrice dite de "mascarade" consiste à se faire passer pour l'interlocuteur agréé qu'on est pas et à s'intercaler dans les échanges entre deux partenaires.

Parades

Pour les risques que nous avons qualifiés de stratégiques :

Il convient certainement de suivre les travaux des associations professionnelles dans ce domaine et d'apprécier le moment idéal pour passer à cette technique ou, pour le moins, pour procéder à une opération pilote comme le préconise la méthodologie EDIFRANCE (association liée à l'AFNOR). Pour la bonne intégration de l'E.D.I. dans les systèmes internes les services informatiques doivent se tenir prêts à adapter leurs applications aux traitements en continu.

Les risques techniques :

Leur évaluation dans le domaine des télécommunications ne font pas encore l'objet d'une méthode reconnue. Des audits techniques peuvent, par analyse des chaînes de liaisons, révéler des faiblesses et recommander des solutions (par exemple des modems sécurisés capables de sélectionner des appels en fonction de leur origine physique).

Une méthode générale sur la sécurité des E.D.I. (MESSEDI promue par le CLUSIF) contient des éléments pour apprécier et renforcer la sécurité des réseaux. Pour la mise en place d'un E.D.I. il est déconseillé de généraliser un protocole simplifié comme il s'en établit parfois entre deux partenaires habitués à échanger. Il est préférable de retenir des solutions "haut de gamme" qui intègrent un maximum de mécanismes de sécurité (possibilité de scellement, de chiffrement, journalisation, contrôle d'authentification...).

Juridique :

Comme pour les risques techniques de haut niveau, la parade peut venir de la qualité du protocole d'échange. Là encore, des mécanismes tels que la notarisation -communication à un tiers de confiance de la copie de la trace des échanges- ou le séquencement des messages -attribution automatique d'un numéro d'ordre qui fait apparaître les manques- constituent une garantie et doivent être recherchés dans les protocoles E.D.I. Au-delà de la qualité du moyen d'échange, le contrat passé entre les partenaires, dénommé accord d'interchange, apportera tous compléments ou précisions utiles.

Critères de qualité

- Participation à une instance professionnelle sur l'E.D.I.

- Support d'un expert extérieur pour le projet pilote.

Voir aussi fiches n° 31
32

Fiche 15 : "EXOTISME"

"Solutions exotiques" versus "solutions standards du marché" : quelle stratégie optimale ?

Définition

Choisir une solution "exotique" c'est choisir une solution pour ses :

- matériels
- logiciels
- localisation de centres informatiques
- recrutements ou recours au SSII
- localisation des développements

qui s'éloigne complètement des solutions les plus habituellement utilisées, au point de présenter un risque technique ou financier.

Risques

Souvent choisie pour des conditions financières apparaissant avantageuses à court terme ou pour des raisons techniques, l'expérience montre que les solutions "exotiques" sont le plus souvent coûteuses ou dangereuses.

Matériels :

- suivi, continuité et développement pouvant être rendus difficiles ou tributaires de la survie du fournisseur
- maintenance, réparations, reventes aléatoires
- coût plus élevé que prévu au départ

Logiciels :

Risques identiques à ceux relatifs aux matériels mais rendus plus complexes par une reprise en main plus compliquée pouvant aller jusqu'à l'abandon pur et simple des applications "immaintenables".

Localisations :

Tant des centres informatiques que des lieux de développement des applications : risques divers (techniques, sociaux, "politiques").

Parades

- Abstenez-vous, sauf si vous avez décidé, coûte que coûte, contre vents et marées, de retenir la solution exotique qui a vos faveurs.
- À défaut, entourez-vous du maximum de garanties (juridiques, commerciales, techniques, assurances...).

Critères de qualité

- Évaluer les coûts/avantages sur tous les plans (et non seulement financiers) à court et à long terme et obtenir l'accord de l'instance qui chez vous valide les solutions techniques retenues (exemple : Comité Technique Informatique).
- Réexamen périodique des solutions exotiques.
- La stratégie optimale, sauf pour les institutions qui peuvent se le permettre n'est pas d'être "pionnier/leader" mais en général "suiveur agile". Cette dernière solution permettant d'évaluer avec un peu de recul les coûts, risques et avantages des nouvelles techniques.

NB : En ce qui concerne la localisation des centres informatiques, notamment ceux qui centralisent les informations comptables transmises à la Commission bancaire (BAFI), il est rappelé aux Etablissements de crédit que l'application des règlements du C.R.B. n° 90.08 et 91.04 leur fait obligation de pouvoir fournir, sur demande, les informations demandées, le détail des fichiers, leur organisation..., lors d'audit ou d'inspection sur place.

Une localisation hors de la France, dans un pays qui ne permettrait pas une inspection sur place, est susceptible d'être incompatible avec les obligations réglementaires.

De façon générale, une localisation hors de la CEE ou des pays du G10 est fortement déconseillée.

Fiche 16 : Facilities management - Out Sourcing
Externalisation - infogérance

Définition

Opération qui consiste à confier à une société de services tout ou partie de la gestion de son informatique. Cette démarche peut aller jusqu'à la disparition complète des moyens techniques et humains qui sont liés au traitement de l'information dans une entreprise. On parle alors d'outsourcing ou "externalisation", notamment lorsque l'opération s'accompagne d'un transfert du personnel (exemple : 1 500 personnes de Mac Donnell Douglas vers IBM) ce qui pose d'ailleurs de nouvelles questions juridiques. Les solutions moins radicales, de sous-traitance plus ou moins étendue, sont plutôt désignées par le terme de "facility management" ou "infogérance". Donc, bien que la terminologie soit encore mal stabilisée dans le public, nous désignerons par "FM" les cas de sous-traitance normale et par outsourcing les cas de cessions complètes.

Risques

- Disparition de la maîtrise des orientations à donner à son informatique. Il est, par exemple, illusoire de penser conserver la fonction de stratégie informatique sans avoir un contact direct avec les acteurs de la gestion des ressources ou du développement.

- Abandon de la supervision des compétences des informaticiens. Le prestataire proposant a priori, au départ, des interlocuteurs au moins aussi compétents que les informaticiens de l'entreprise, la question est d'être maître de l'évolution et de la répartition des compétences optimisées pour l'entreprise et non pour un ensemble de clients.

- Incohérence possible entre le coût à court terme et le coût à long terme. Le coût proposé pour une externalisation est un minimum dont il n'est pas sûr qu'il puisse effectivement être maintenu dans le temps. La fonction informatique ainsi déléguée risque de coûter plus cher que prévu. L'entreprise qui confie cette fonction n'aura pas facilement la possibilité d'en faire des audits ou elle perdra, peu à peu, la faculté de mener de tels audits faute d'entretien des compétences requises. En cas d'insatisfaction, la remise en cause du contrat sera un grand facteur d'inertie.

- L'engagement est nécessairement sur longue période. Les contrats actuels sont signés pour dix ans, cela traduit bien l'ampleur des investissements nécessaires pour une reprise correcte mais laisse aussi envisager la difficulté d'une remise en cause et le manque de souplesse pour faire jouer la concurrence de manière quasi-permanente. Ici, contrairement à ce qui se passe dans les cas de sous-traitance industrielle, on se place dans la dépendance d'une seule entreprise, il n'y a aucune division du risque.

- Sur de telles durées de contrat, on ne peut pas ignorer le risque de faillite ou de reprise du fournisseur par une entreprise qui n'aurait pas la même stratégie commerciale.

- L'entreprise qui confie son informatique ne peut plus bénéficier des progrès technologiques au rythme qu'elle peut souhaiter. Le fournisseur résistera à une mutation technologique si elle contrarie sa préoccupation de rentabiliser ses propres investissements. Dans ce cas, l'entreprise abandonne une partie de ses facultés d'anticipation, d'innovation et de réactivité

qui sont des atouts décisifs dans un environnement fortement concurrentiel. En réponse à une telle inertie, il y a là le risque d'être amené à recréer en interne une fonction informatique qui se consacrera dans un premier temps aux nouveautés technologiques. Conséquence qui est contraire à l'orientation retenue pour passer en "outsourcing".

- Le gestionnaire extérieur, qui s'est spécialisé dans cette activité, a généralement pris en charge l'informatique de plusieurs entreprises. Là encore, le risque est grand de perdre la maîtrise de ses propres priorités, s'il survient un conflit de ressources humaines (techniciens ou ingénieurs très spécialisés) ou matérielles (back-up de l'exploitation) : le meilleur client sera probablement le mieux servi.

- Dans le cas où le fournisseur extérieur a aussi les maintenances d'application sous sa responsabilité, il sera naturellement porté à faire une politique d'offre auprès des utilisateurs. En interne, on ne dispose plus d'intermédiaires pour chiffrer et évaluer, pour le compte de la Direction Générale, l'intérêt des demandes formulées par les différents services.

- Si les développements sont eux-mêmes confiés à l'extérieur c'est l'absence d'agents à profil double "métier de l'entreprise" et "informatique" qui risque de faire défaut. Dans le monde bancaire, la culture bancaire des informaticiens est toujours considérée comme un avantage déterminant pour la qualité du dialogue avec les utilisateurs. Cet avantage ne peut que se retrouver partiellement chez une société de services : il manquera toujours, en effet, l'expérience et la culture de l'entreprise cédante.

- Par l'intermédiaire de son service informatique, quand celui-ci maîtrise bien le système d'information, la Direction Générale peut disposer d'une connaissance précise de l'entreprise. En cas d'externalisation de l'informatique, c'est aussi cette possibilité de connaissance approfondie de l'entreprise qui est confiée à l'extérieur. Une Direction Générale ne pourra pas s'appuyer sur un prestataire extérieur pour obtenir les précisions, les détails, les explications, qu'il peut réclamer à son directeur des services informatiques.

- La distinction entre FM et outsourcing doit être faite car les risques entre la première -normaux, maîtrisables- n'ont rien à voir avec la seconde où la magnitude des risques peut être plus élevée.

Parades

Les risques étant connus, il convient de limiter le recours à l'extérieur aux cas où il est préférable à une prestation interne. Ce recours à l'extérieur n'est envisageable pour la totalité des prestations informatiques qu'en cas de carence manifeste des services en place. Il peut constituer un traitement de choc mais d'autres existent qu'il faut comparer -filialisation, renouvellement de la hiérarchie-. L'externalisation peut porter sans risque sur des fonctions parfaitement stabilisées dont on ne prévoit pas d'évolution à moyen terme. Il s'agit alors tout simplement de sous-traitance de fonctions de saisie d'informations et de production informatique. Ce qui se pratique couramment et ne mérite pas une nouvelle appellation ("FM ou Facility Management") qui n'a pour seul objet que de tenter de relancer et d'élargir le marché. D'autres fonctions informatiques peuvent utilement faire un court passage à l'extérieur : cela peut être le cas d'une reprise de maintenance. On peut très bien ne pas disposer en interne de l'expérience, des outils, des agents pour redocumenter et fiabiliser une ancienne application. Une telle opération ne doit toutefois pas sortir l'application donnée en tierce maintenance du contrôle de l'informatique interne (risque induit par le contact direct entre le fournisseur et les utilisateurs).

Les propositions de facility management ou d'outsourcing ont la particularité d'être souvent directement adressées à la Direction Générale. Celle-ci est sensible à un effet immédiat d'une telle opération : une proposition pour un coût total de l'informatique de l'entreprise avec des espoirs de réduction (qui bien sûr restent à vérifier) reste tentante en période de compression nécessaire des frais généraux. La DG sera d'autant plus réceptive à cet argument que le coût de l'informatique n'est pas toujours connu et justifié en interne. Pour aller plus loin sur ce terrain et anticiper les réponses à de telles offres, la DSI doit, fonction par fonction, analyser l'intérêt économique et stratégique d'une externalisation. Une telle vision de la variété des prestations informatiques sera favorable au déclenchement d'opérations de facility management sur les créneaux où elles s'avéreront rentables et efficaces.

Critères de qualité

- Évaluer les différentes fonctions informatiques selon l'intérêt et des risques de leur externalisation.

- Réaliser une consultation périodique et ouverte sur ce sujet.

- En cas d'externalisation, définir les rôles, la responsabilité et le niveau d'autorité des informaticiens qui demeurent dans l'entreprise.

- Ne s'adresser alors qu'à des sociétés présentant les plus grandes garanties (déontologie, références...).

- Les contrats doivent inclure les obligations des fournisseurs comme indiqué dans les ouvrages tels que le "Référentiel DUNOD" ou le "Droit de l'Informatique LAMY", prévoyant, en particulier, la réversibilité du contrat et la faculté de faire des audits chez le fournisseur.

IMPORTANT

Dans l'état actuel des techniques, en raison du caractère très spécifique du monde bancaire, le Secrétariat général de la Commission bancaire attire l'attention des établissements de crédit qui souhaiteraient procéder à une opération "d'outsourcing" total (cession complète des matériels, logiciels, personnels, développements et recherches) sur les risques très élevés qu'ils encourent. Un tel choix ne devrait être opéré qu'après que l'établissement (sa Direction générale, ses actionnaires et son comité d'audit) ne se soit assuré que cette solution est raisonnable, que le maximum de garanties a été obtenu et qu'elle permet de respecter les obligations réglementaires telles que les Inspections sur place de la Commission bancaire.

voir aussi fiche n° 12

Fiche 17 : G.E.D. : gestion électronique des documents

Définition

G.E.D. : Gestion électronique des documents.

Développements technologiques qui visent à dématérialiser des documents pour améliorer l'efficacité des travaux de bureau. La G.E.D. permet d'enregistrer des documents de structures variées (lettres, images, plans...) de les restituer à l'écran, de les enrichir de manière libre ou prédéterminée (circuit de traitement) et d'instruire ainsi des dossiers sans la contrainte du support matériel présent qu'à un seul endroit à un instant donné.

Les risques présentés par cette technologie sont d'abord de possibles échecs dans son adoption car les conditions et les habitudes de travail sont considérablement modifiées. La G.E.D. suppose une réorganisation du travail ; la période de transition peut être difficile à gérer et provoquer une réelle désorganisation. Les procédures nouvelles doivent présenter des qualités au moins égales aux anciennes en tous points. Les points les plus difficiles à restituer sont la confidentialité (un accès informatique peut être plus aisé que l'accès à un coffre), la valeur juridique (il n'est pas encore possible de retrouver simplement un équivalent d'une signature sur papier), l'unicité des supports (la gestion d'un dossier original -où l'on trouve toutes les pièces qui font foi- évite la multiplication des copies, le support informatique au contraire les facilite, des versions papiers peuvent être recréées, d'abord comme document intermédiaire puis comme support privilégié de travail).

La G.E.D. s'accompagne aussi d'une augmentation en volume de l'information mise à disposition. Par exemple, si des lecteurs de disques optiques sont installés il sera tentant d'acquérir des bibliothèques de documents. Il y a alors un risque de surinformation qui entraînera des pertes de temps pour les recherches des non spécialistes.

La rentabilité économique d'une G.E.D. est jusqu'à présent difficile à démontrer.

La décision d'implanter une G.E.D. devra donc être soigneusement étudiée (analyse de la valeur, utilisation des méthodes d'organisation...).

Parades

Le système retenu doit apporter une grande garantie de confidentialité et être capable de reconstituer les habitudes de travail. Pour être accepté par les utilisateurs, il doit apporter immédiatement des facilités nouvelles qui ne seraient pas imaginables avec des solutions non informatisées (outils de recherches documentaires, aide à la rédaction, aide sur les circuits et procédures à respecter). Le basculement vers de nouvelles procédures de travail viendra après une phase d'assimilation des outils.

La valeur juridique des documents en entrée et en sortie doit être préservée, ainsi les originaux sont soigneusement conservés (cf. fiche n° 3 : "archivage") et référencés dans le système informatique. Si des éditions papiers particulières doivent être faites pour servir de preuve ceci doit être indiqué par le système et, à nouveau, référencé.

La disparition des supports alternatifs n'est pas nécessairement totale. Le rôle de ces supports peut être précisé (papier comme brouillon par exemple) et ainsi limité.

Le risque de surinformation peut être contenu en concentrant ce type de base de données dans des services documentaires ou dans des services très spécialisés.

Le bilan économique d'une opération G.E.D. tiendra compte d'éléments de gain direct (gain de place évalué au prix du m², productivité des agents dans les temps d'accès aux dossiers) et aussi indirect (effet du raccourcissement de délai de traitements vis-à-vis des concurrents).

Critères de qualité

Possibilité de retrouver facilement les documents originaux qui ont alimenté une procédure.

Intégrer aux outils G.E.D. des éléments de mesure des temps de traitements pour détecter les points d'attente, les enchaînements séquentiels non indispensables et optimiser ainsi en continu les procédures d'instruction de dossier.

Vérifier qu'il n'y a pas résurgence de solution parallèle.

Mesurer les gains de productivité par rapport à la solution préexistante (temps de traitements, volumes de documents manipulés et stockés...).

Suivre le taux d'emploi des bases documentaires achetées et analyser l'usage qui en est fait.

Fiche 18 : Maintenance des matériels et logiciels de base

Définition

Pour exécuter dans de bonnes conditions des traitements informatiques, il ne suffit pas d'acquérir auprès de fournisseurs des matériels et des logiciels ; il est aussi très important de s'inquiéter de leurs évolutions dans le temps et de se garantir de leur disponibilité.

L'évolution des matériels et logiciels est assurée par le fournisseur. Il corrige et perfectionne en permanence ses produits afin d'améliorer leur fonctionnement et leur performance. Il en résulte des aménagements techniques ou de nouvelles versions de logiciels.

La disponibilité maximale des matériels et des logiciels peut être assurée, soit en remplaçant rapidement les éléments techniques défaillants, soit en corrigeant régulièrement les éléments imparfaits.

L'entretien préventif et correctif des matériels et des logiciels peut être réalisé contractuellement par le fournisseur, en contrepartie de redevances. Le niveau de la redevance est fonction de la garantie de fonctionnement souhaitée.

Ces contrats, dits de maintenance, permettent de maintenir la valeur de l'équipement, d'améliorer sa durée de vie, de garantir sa continuité de fonctionnement.

La télémaintenance est une technique utilisant les moyens de télécommunication ; elle est employée pour faciliter l'intervention à distance des techniciens du matériel et du logiciel.

Risques

Matériels :

- Les matériels sont susceptibles de subir des pannes intempestives, l'absence de contrat de maintenance ne permettrait pas d'obtenir une intervention du fournisseur dans les meilleurs délais et aux meilleures conditions. Le fournisseur, hormis pendant la période de garantie qui suit l'acquisition, n'a que très peu d'engagements et ses garanties sont limitées.

- Le vieillissement et l'usure de certains éléments sont naturels ; l'absence de suivi et d'entretien entraîne inéluctablement des arrêts imprévus.

  En cas de revente du matériel, l'absence d'entretien ne permet pas de garantir le bon état de celui-ci ; le prix en est bien sûr affecté.

- L'hétérogénéité des éléments, malgré le niveau de compatibilité déclaré, introduit un risque supplémentaire certain. Ce risque est dû à ce que la compatibilité n'est pas totale et au fait que l'évolution des équipements doit être strictement parallèle. Ainsi, si un incident survient, il sera très difficile d'en faire l'analyse et d'en reporter la responsabilité à l'un des fournisseurs. La durée d'indisponibilité en sera vraisemblablement prolongée.

Logiciels :

- Les logiciels ne sont pas exempt d'erreurs. Certaines de ces erreurs sont connues et le fournisseur propose des corrections qu'il faut intégrer. D'autres se produisent en cours d'exploitation, et seul le fournisseur possède les éléments pour les analyser et apporter les corrections. Le code de base des logiciels n'est plus disponible pour les spécialistes systèmes de l'entreprise, le fournisseur se protègeant du piratage de son "œuvre". Il faut faire appel nécessairement au fournisseur pour corriger les anomalies. En l'absence de contrat de maintenance, le fournisseur n'est pas obligatoirement tenu d'assurer les corrections. Il pourra intervenir sur demande mais ses tarifs et ses délais seront plus pénalisants.

- La multiplicité et la diversité des produits installés sur un centre en font généralement un site spécifique. Ce qui limite défavorablement l'utilisation d'outils d'installation. La mise en œuvre d'une nouvelle version logicielle doit être rigoureuse et elle nécessite des procédures de changement strictes incluant des tests généraux et la validation de l'ensemble "logiciel".

- Lorsque des techniciens de maintenance interviennent, ils ont à leur disposition des outils qui leur permettent d'accéder au système d'information : l'intégrité et la confidentialité des informations peuvent être amoindries. De plus, les changements opérés par les intervenants peuvent être imparfaits et entraîner des interruptions sérieuses.

- La télémaintenance introduit de nouveaux risques dès lors qu'elle permet à des intervenants extérieurs de pénétrer le "système" en fonctionnement, qu'elle les autorise à y effectuer des changements ou des visualisations.

Parades

Tout d'abord, il est nécessaire de posséder une installation conforme aux normes en usage et aux règles d'installation du fournisseur.

Pour se garantir du bon fonctionnement des matériels et des logiciels de base, il faut souscrire des contrats de maintenance appropriés à l'utilisation des équipements et au niveau de service souhaité. Il existe des contrats de maintenance adaptés à toutes les situations. Selon que le matériel est acheté, en location ou en crédit-bail, la responsabilité de la maintenance incombe à la banque ou au propriétaire.

En fonction de l'importance des matériels, il est nécessaire de prendre en compte divers critères pour la rédaction du contrat :

- intervention sur appel
- intervention périodique
    - sur les lieux de l'installation
    - dans les locaux du fournisseur
- équipe d'intervention sur place
- facturation à l'intervention comprenant le coût réel de la main d'œuvre et du matériel
- base d'un abonnement périodique, intégrant le coût de la main d'œuvre et du matériel.

Pour la maintenance du matériel, il peut être fait appel soit au fournisseur soit à un tierce-mainteneur. Si le professionnalisme est un critère important, il ne se substitue nullement à l'établissement d'un contrat de qualité. Les clauses de garanties, d'obligations réciproques, de résiliation et d'achèvement doivent être clairement décrites, ainsi que la certification de qualification.

Si des équipements de fournisseurs différents sont négociés dans la configuration, il peut être plus efficace de faire réceptionner l'ensemble par le fournisseur principal, charge à lui d'animer la réflexion et la recherche en cas d'incident.

Quant à la télémaintenance, il est important d'en peser l'intérêt, d'en limiter les fonctions, d'en contrôler l'usage. Il est indispensable de prévoir une procédure obligeant les techniciens de maintenance à faire une demande d'accès à l'équipement, à se conformer aux procédures de contrôle d'accès en vigueur dans l'entreprise.

Les changements opérés dans une opération de maintenance doivent faire l'objet de tests et de qualification. Il peut être prudent d'envisager le retour à la situation antérieure au cas où le changement ne serait pas opérationnel.

Critères de qualité

Le tableau de bord fait ressortir un taux de disponibilité optimum.

La gestion des incidents fait ressortir les problèmes de compatibilités des différents fournisseurs.

Des contrats de maintenance adaptés au niveau de sécurité souhaité par la Direction Générale, ont été souscrits.

Des procédures sécurisées ont été formalisées pour réglementer l'accès et l'intervention des techniciens de maintenance.

Fiche 19 : Messageries

Définition

On appelle messagerie un système d'échange électronique d'informations, qui peut faire appel à des ressources informatiques internes ou externes à l'entreprise.

Ses utilisations possibles sont :

- l'échange de messages interpersonnels,
- le courrier électronique,
- le transfert de fichiers de données,
- la diffusion de logiciels,

qui peuvent être complétées par de nombreuses fonctions annexes :

- gestion d'agendas individuels ou collectifs, de salles de réunions,
- classement et archivage des messages,
- etc.

Les objectifs poursuivis par la mise en place d'un tel système :

- faciliter la communication (en adressant un message à un interlocuteur occupé ou absent ou en dehors des heures ouvrées),
- gagner du temps (en réduisant les délais d'acheminement),
- diminuer la masse de documents papier circulant (et donc les frais de courrier, de secrétariat...).

Risques

Perte de confidentialité (accès aux messages par des tiers autres que les personnes concernées) :

- en utilisant un système externe non maîtrisé,
- en laissant la messagerie en libre accès (depuis un minitel banalisé, par exemple),
- en ouvrant une voie d'accès au système informatique de l'entreprise,
- par absence ou insuffisance de protection des messages.

Indisponibilité (impossibilité ou difficultés pour utiliser l'outil dans certaines circonstances) :

- utilisation abusive pour des transferts de fichiers volumineux perturbant ou saturant le système,
- saturation par pollution (intrusion de "vers"),

- absence de secours alors même qu'en situation critique (ex : back-up), la messagerie peut devenir un moyen de communication stratégique,

- désintérêt des utilisateurs par manque de convivialité (saisie de volumes importants à partir d'un minitel, mode courrier sans logiciel de traitement de texte...), ou par manque d'assiduité de certains interlocuteurs (en particulier de la part de la direction). La messagerie électronique exige que chacun vérifie régulièrement le contenu de sa boîte à lettres.

Lors de la diffusion de logiciels, la messagerie peut devenir un vecteur involontaire (mais efficace !) de propagation de virus.

Parades

Utiliser la messagerie strictement pour les usages définis et prévus ; prévoir des procédures spécifiques et réservées pour les utilisations non-standard (par exemple, dans le cas d'une messagerie destinée à des échanges interpersonnels : les transferts de fichiers, les diffusions de logiciels, la génération de télex ou de fax).

S'il s'agit d'un outil stratégique, le gérer en interne et s'assurer de sa disponibilité ; prévoir une sauvegarde des messages et un secours des moyens de traitement et de communication.

Mettre en place des mesures de protection adaptées à la nature des informations véhiculées (contrôle d'accès, chiffrement...).

Edicter des règles simples pour inciter le personnel à une utilisation régulière et homogène de la messagerie : consultation quotidienne, canal obligatoire de diffusion de certaines informations, mode unique d'organisation des réunions...

Critères de qualité

Donner au message électronique la même valeur que toute autre forme de communication écrite ; pour cela, il doit pouvoir être conservé, édité, protégé autant que de besoin.

Prévoir pour les messages des modes :

- urgence (avec retour d'informations aux interlocuteurs),

- secret (pas d'accès par un assistant, une secrétaire, un groupe d'usagers...).

S'il existe un besoin de confidentialité, effectuer un chiffrement des messages de bout en bout (transmission et stockage).

Prévoir une formation minimale des utilisateurs et la distribution d'un guide d'utilisation.

Soigner l'interface utilisateur ; donner la possibilité de créer des listes de diffusion ; si les messages doivent être formatés (courrier, télex, formulaires...), prévoir l'accès via un traitement de texte évolué. Prévoir l'envoi automatique d'un accusé de réception à l'envoyeur lorsque le message envoyé a été lu par le destinataire.

Demander aux utilisateurs de s'identifier et de s'authentifier, si possible avec les mêmes codes que pour les autres fonctions accessibles à partir du poste de travail.

Inciter la hiérarchie à utiliser systématiquement et exclusivement la messagerie pour certaines fonctions, par exemple pour l'organisation des réunions.

Désigner un administrateur de la messagerie.

Effectuer un suivi statistique de son utilisation (par exemple, le délai moyen de réponse aux messages est un bon indicateur d'efficacité) et une journalisation de l'accès aux fonctions réservées.

Fiche 20 : Méthodes et outils de développement

Définition

Il s'agit des méthodes de conception employées par les développeurs informatiques et les outils de génie logiciel qui leur sont associés.

Risques

L'adoption d'une méthode et d'un atelier de génie logiciel (AGL) dans une entreprise est toujours un moment délicat, d'abord par la diversité du choix offert et surtout par la révolution culturelle que cela entraîne. En privilégiant la généralisation d'une solution unique pour plus d'efficacité, on peut se priver de la richesse donnée par la diversité et figer une situation pour un long moment. En plus du risque de "monoculture", du lien privilégié et difficilement réversible avec un fournisseur que représente la mise en place de son outil de génie logiciel, les solutions existantes ne sont pas toujours suffisantes sur le plan de la sécurité.

Parades

La diffusion d'une méthode de développement peut sans risque être étendue à tous les développeurs. Elle facilite les dialogues en tous sens et permet de produire des documentations homogènes. Ces documents seront bientôt rendues obligatoires par les normalisations (ITSEM). L'emploi d'outils informatiques bien intégrés à la méthode en facilitera la production (par exemple grâce à des plans types disponibles au sein même de l'outil de modélisation).

Les dérogations à la méthode doivent être justifiées par l'originalité des domaines traités (modélisation de la connaissance, techniques temps réel...).

L'outil de développement peut aussi intégrer de la génération de code. Il doit alors en faciliter le contrôle (visualisation de la structure des programmes, vérification de la correspondance spécification-code pour éviter les codes morts propices aux bombes logiques). En plus de l'assurance sur la qualité du code qu'il peut donner, l'outil facilitera les historicisations de version et la répartition du travail dans une équipe (lien développeur programme). L'adoption d'un AGL, ou d'un langage de 4ème génération pour les développements ne doit pas nécessairement faire disparaître toute compétence en langages plus basiques (assembleur, C, cobol...). Mais ces autres langages seront employées pour des optimisations ou des cas spéciaux et non comme une alternative de programmation. Ces compétences se trouveront par exemple dans des équipes systèmes et non dans les équipes de développement.

La prise en compte des facteurs de sécurité ne se trouve pas d'origine dans les méthodes classiques de conception et les outils associés. Il faudra donc ajouter ce type d'information (facteurs DICP) aux modélisations des données et des traitements. Les mesures de sécurité décidées en étude préalable sur des données sensibles (par exemple un chiffrement) devront être affectées précisément dans les modélisations et "propagées" jusqu'à la réalisation.

Critères de qualité

- Mesure de la conformité de la documentation aux plans-types
- Taux de quantification en facteurs DICP pour les données, les flux et les traitements élémentaires
- Facilités de gestion d'un groupe d'utilisateur pour un AGL (affectation développeur programme)
- Recours aux outils de contrôle de code
- Revue de code par une société spécialisée pour les applications les plus sensibles.

Fiche 21 : Modifications applicatives

Définition

La vie d'un système d'informations entraîne en permanence des aménagements de programmes -aménagements planifiés ou corrections d'erreurs...- lesquels ont pour conséquence des navettes permanentes entre les niveaux "programme en test" - "programme en production". Ces échanges doivent se faire dans le respect des règles classiques de sécurité : disponibilité, intégrité, confidentialité (le cas échéant). Dans ces échanges sont impliqués les développeurs des études informatiques, les cellules assurant le recettage, la production informatique, les utilisateurs.

Risques

Les risques concernent essentiellement :

- l'intégrité des programmes mis en production, soit que les modules exécutables ne correspondent pas aux programmes sources, soit qu'une fois mis en service les programmes soient modifiés, soit que les procédures ne garantissent pas dans certains cas l'étanchéité entre environnements,

- la disponibilité des applicatifs, si la modification apportée entraîne des dysfonctionnements sur d'autres points.

Les aménagements peuvent être faits à froid, sans contrainte de temps, ou à chaud, sur blocage de traitements dus à un "plantage" ou à une anomalie constatée par rapport aux résultats attendus.

Parades

Les procédures de recettage et mise en production doivent être parfaitement codifiées et contrôlées de façon à assurer leur respect. Elles doivent en particulier être partie intégrante de la méthodologie de développement. Il doit exister plusieurs environnements cloisonnés et pour lesquels les droits d'accès sont différents. Les modifications sont faites par les développeurs sur leur environnement spécifique, les programmes sources et objets sont ensuite transférés vers un environnement de recette. Il est souhaitable de refaire à ce niveau une compilation afin de garantir la concordance source-objet. Après recettage, un nouveau transfert est fait vers l'environnement production. Les programmes une fois mis en production doivent être verrouillés et servir de référentiel unique pour d'éventuelles modifications ultérieures par recopie vers l'environnement de test. Il doit donc exister un outil de gestion, sécurisé, assurant les fonctions ci-dessus. Il est souhaitable de contrôler périodiquement par sondage l'adéquation entre la modification apportée et la fonctionnalité concernée, ceci pour éviter, par exemple, l'introduction d'un "Cheval de Troie". Cette charge peut être attribuée à la Sécurité informatique dans le cadre d'un plan de contrôles récurrents ou à l'Inspection.

Les mêmes règles devraient s'appliquer au logiciel de base et aux produits "système".

Le plus grand soin est à apporter aux procédures dites d'urgence, consécutives à des corrections d'anomalies. Celles-ci peuvent avoir pour effet de court-circuiter les procédures de recettage ou d'entraîner des modifications directes de fichiers. Elles doivent donc être autorisées par une signature ad hoc et faire l'objet d'un enregistrement et d'un suivi de contrôle particulier. Si elles ont eu pour effet la modification directe de fichiers, la correction des programmes concernés ne doit pas être oubliée.

Les modifications applicatives doivent être enregistrées et archivées de façon à permettre un retour en arrière en cas de problème. La procédure éventuelle de retour arrière doit être particulièrement étudiée lorsqu'il s'agit de migrations conséquentes, telles que le changement de niveau d'applicatif et les changements de "release" des logiciels système.

Critères de qualité

Il s'agit de suivre via un tableau de bord des indicateurs tels que :

- nombre d'applications livrées,
- nombre d'utilisations de procédures d'urgence,
- nombre d'interventions à chaud,
- nombre d'anomalies sur les documents de validation.

Les documents de demande de mise en service doivent être consultables.

Fiche 22 : Moyens et procédures de secours

Définition

Compte tenu de l'importance actuelle prise par le développement de l'informatique dans l'entreprise, il convient d'analyser l'impact de l'arrêt partiel ou total des outils informatiques dont elle dispose. En fonction de la nature des sinistres considérés, et à partir des scénarios opératoires correspondants qu'elle aura élaborés, l'entreprise est conduite à mettre en œuvre ce que l'on désigne sous le terme de "plan de secours" informatique qui s'appuie sur des moyens techniques connus sous le nom courant de "back-up". Ce plan de secours s'intègre dans le "plan de continuité des activités" qui intègre les schémas fonctionnels et organisationnels complétant les moyens matériels.

Risques

Si le déploiement d'un tel plan lors d'un sinistre majeur est de nature à permettre à l'entreprise de reprendre et poursuivre ses activités dans les meilleures conditions et à diminuer le montant des pertes financières liées à la situation de catastrophe, son absence est un risque majeur pour la banque.

Les sinistres pris en compte doivent être analysés en fonction de leur impact potentiel sur la vie de l'entreprise. Le plan mis en œuvre doit prévoir non seulement de pallier l'indisponibilité des équipements informatiques, mais doit aussi intégrer l'environnement interne (utilisateurs, logistique) et externe (télécommunications).

Faute de quoi, un sinistre de quelque origine qu'il soit (humaine ou matérielle) est de nature à perturber gravement l'activité de l'entreprise, voire à compromettre sa poursuite.

Ces procédures appliquées au système constituent une partie du plan de survie global de l'entreprise qui prend en compte d'autres types de sinistres que les sinistres informatiques.

Parades

Il s'agit de doter l'entreprise des moyens humains, organisationnels et matériels correspondant à la définition ci-dessus. Ceux-ci peuvent être de diverse nature en fonction des besoins de l'entreprise et de la plus ou moins grande sensibilité des fonctions à dépanner. Les modalités de reprise des activités sont à examiner en fonction de la criticité pour l'entreprise des systèmes concernés.

Pour les cas où le délai d'interruption de l'activité doit être nul ou aussi réduit que possible, la solution du basculement automatique d'un environnement vers un autre et la redondance interne peuvent être étudiées. D'autres solutions peuvent être envisagées lorsque le problème des délais est moins crucial (retour du service sous 24 ou 48 h) :

- mutualisation d'équipement par montage d'un back-up interprofessionnel,
- souscription de contrat auprès d'une société spécialisée, avec déplacement sur un site de dépannage et mise à disposition de moyens matériels et/ou humains par le prestataire,
- back-up interne.

La solution retenue (ou les solutions), quelle qu'elle soit, doit être parfaitement formalisée et reposer sur un contrat externe ou interne (contrat de service). Le coût des moyens mis en œuvre doit être comparé aux pertes provoquées par la dégradation de services liée au sinistre. La gradation de ces moyens doit s'adapter aux diverses situations pouvant être rencontrées en termes de matériels, de temps de reprise, de procédures d'organisation et de pertes potentielles.

Pour que le plan de reprise soit effectif, il doit intégrer des procédures d'organisation couvrant toutes les phases du transfert vers les moyens de secours et du retour au mode normal d'exploitation, et des ressources humaines permettant de faire fonctionner le système d'informations hors de son contexte habituel.

Il est indispensable de procéder régulièrement aux essais des matériels et procédures, faute de quoi, l'entreprise s'expose à les voir lui faire défaut le jour où elle en aura besoin. Ces tests peuvent être faits en double, donc sans risque pour l'entreprise, mais aussi avoir pour objet de s'assurer que les procédures élaborées sont opérationnelles en déportant effectivement la production informatique sur le site de secours pour une durée plus ou moins grande. Les résultats des tests doivent faire l'objet d'un rapport détaillé et objectif et être examinés d'un oeil critique. Les procédures doivent être réactualisées en permanence pour rester en conformité avec les parcs matériels et applicatifs de l'entreprise. Pour être efficace, leur établissement doit être intégré à la vie courante des services touchés par leur mise en œuvre et leur utilisation.

Afin de faciliter l'établissement des procédures, leur entretien et leur diffusion, il est utile de se doter d'un logiciel spécialisé de gestion de plan de secours.

Critères de qualité

Il s'agit de suivre via un tableau de bord des indicateurs tels que :

- nombre de tests en double et en réel du plan de secours,
- existence de comptes-rendus de test,
- temps passé à la restauration du système,
- % de succès des tests par rapport aux objectifs initiaux fixés.

Il convient également de s'assurer que :

- la documentation nécessaire est bien détenue en dehors de l'entreprise,
- les listes de personnes, adresses, numéros de téléphone, fax télex, sont tenues à jour et accessibles.

IMPORTANT

NB : Pour chaque établissement de crédit, il est indispensable qu'existe un plan de secours opérationnel sérieusement pensé et testé, au moins pour les informations (données, fichiers, bases) jugées stratégiques.

La définition, dans l'ensemble du SI, de la partie stratégique relève de la responsabilité de la Direction générale. Il est impératif qu'elle soit faite.

Fiche 23 : Organisation de la sécurité ; responsabilités

Définition

Il s'agit d'apporter un éclairage sur la fonction "Sécurité des Systèmes d'Information" et sur les moyens à mettre en œuvre, sur le plan organisationnel, pour que cette fonction puisse être exercée avec le maximum d'efficacité.

Risques

Il est souvent dit que ..."la sécurité est l'affaire de tous"... Il ne faudrait donc pas oublier qu'elle est l'affaire de chacun. C'est ainsi qu'une mauvaise organisation, ou même une absence de définition des "droits et devoirs" en matière de sécurité, peut entraîner une dilution des actions de sécurité, voir même une absence de celles-ci.

L'utilisation malveillante ou accidentelle d'une faille dans la Sécurité des Systèmes d'Information de la Banque, peut mettre en péril son exploitation, sa survie, voire même celle de ses contreparties. Des parades existent en matière d'organisation.

Parades

Le Responsable de la Sécurité des Systèmes d'Information ou RSSI est le garant de la sécurité des systèmes d'Information de la Banque. Ses domaines d'action sont multiples mais ils répondent à un seul objectif : assurer l'intégrité, la cohérence et la confidentialité des données de tous les Systèmes d'Information de la Banque.

L'originalité de son statut et de son organisation actuelle réside dans le fait qu'il cumule trois fonctions réparties habituellement dans plusieurs Directions.

Contrôle-Audit

Cette fonction assure la définition des règles de sécurité et les contrôles de leur mise en application.

Architecture-Conception

Cette fonction prolonge le diagnostic émis par la fonction Contrôle Audit pour définir les moyens de la mise en œuvre des règles de sécurité.

Administration

La fonction d'administrateur et de gestionnaire s'exerce sur les systèmes de gestion de la confidentialité : le RSSI est "maître d'ouvrage" de la sécurité.

Parmi les avantages que présente cette organisation, il convient de souligner :

- Le rattachement du RSSI au plus haut niveau hiérarchique (un poste spécifique, avec un budget spécifique et un rattachement de niveau Direction Générale) lui confère une réelle crédibilité vis-à-vis du personnel "informaticien" de la Direction Informatique comme de tous les autres utilisateurs des Systèmes d'Information de la Banque.

- Les interventions menées en synergie avec la Direction Informatique évitent à celle-ci de pourvoir des postes sécurité au niveau de la Production et des Développements Informatiques.

- L'administration quotidienne du système de gestion de la confidentialité permet d'entretenir les compétences nécessaires à son évolution et à son amélioration. Ces compétences s'avèrent également déterminantes dans l'élaboration des règles de sécurité.

- La surveillance quotidienne et le "support" aux gestionnaires décentralisés de la Sécurité permettent des actions de formation, sensibilisation et promotion de la sécurité auprès des utilisateurs des systèmes d'information.

- Le cumul des fonctions du RSSI lui assure plusieurs sources d'informations (interventions en production, tableaux de bord RACF, exploitation de l'exit SME, sécurité de nouveaux projets...) et lui donne une visibilité suffisante des risques et des faiblesses du Système d'Information, pour apprécier les priorités des actions qui doivent être engagées. Le RSSI assure à la fois des fonctions d'audit et de contrôle, et des fonctions opérationnelles d'administration et de gestion au quotidien. Cette situation lui donne une partie de son efficacité et de sa crédibilité dans la Banque. Elle est aussi à l'origine de la motivation de son équipe.

Critères de qualité

Dans cette perspective, des principes de base doivent être acceptés et une organisation doit être mise en place devant permettre de répondre aux objectifs suivants :

Les objectifs généraux :

- Les principes généraux de sécurité sont formalisés par cette unité de rappel.

- Les principes généraux de sécurité doivent être respectés et mis en œuvre quels que soient les environnements, les implantations géographiques, la taille des équipements informatiques (micro-ordinateur, réseau local, site départemental, régional ou central), les applications, les types de matériels... Toute dérogation à ces principes généraux nécessite l'accord de cette unité.

- Les évolutions de logiciels système, les choix de nouvelles technologies et les choix d'architectures doivent être étudiés obligatoirement en collaboration avec cette unité pour qu'une analyse de vulnérabilité soit effectuée.

- Toute création ou modification importante de logiciel applicatif développé en interne, ou tout achat de progiciel applicatif doit faire l'objet d'une analyse de vulnérabilité donnant lieu à l'établissement d'un chapitre sécurité formalisé : consultable, maintenable et accessible.

- Cette unité devra pouvoir maîtriser l'administration décentralisée de la Sécurité. Elle doit pouvoir contrôler l'attribution des droits et des privilèges de chacun et l'utilisation qui en est faite.

L'Organisation de la Sécurité sur le terrain :

Les responsables des différents secteurs géographiques sont généralement responsables de toutes les fonctions de leur secteur ; ils sont donc responsables de la sécurité de l'Information dans leur domaine et doivent faire respecter les principes généraux de sécurité.

Dans le même esprit, le Chef de métier est responsable de la sécurité dans son métier. Il doit donc faire respecter les principes généraux de sécurité.

Cas particulier de la Direction de l'Organisation et des Systèmes d'Information :

Compte tenu de son rôle stratégique vis-à-vis du système d'information de la Banque, des relations privilégiées doivent exister avec cette unité de rappel de la Direction Générale. Il s'agit essentiellement d'une collaboration étroite pour tous les problèmes de sécurité tels que les télécommunications, les choix d'architectures, les évolutions de logiciels "système"...

Fiche 24 : Personnel informatique ; fonctions, éthique

Définition

Les métiers de l'informatique peuvent se classer grossièrement en 5 grandes catégories :

- les maîtres d'ouvrage (de projets informatiques)
- les gestionnaires (d'applications informatiques)
- les développeurs (chefs de projet, analystes programmeurs, mainteneurs...)
- les exploitants (pupitreurs, opérateurs...)
- les spécialistes système.

Ils sont de plus en plus proches de "la machine" lorsque l'on descend cette liste, et ils ont donc de plus en plus besoin de possibilités d'accès (ou privilèges) à cette machine et aux informations qu'elle contient pour exercer leurs talents. Tout ou partie de ces fonctions peuvent être remplies par des prestataires de services externes à l'entreprise.

Par ailleurs, il se trouve que, par leur culture et leur formation, les informaticiens n'ont pas une grande sensibilité au problème de protection des informations, surtout par comparaison avec leurs collègues banquiers ; ce comportement, qui peut être perçu de manière occasionnelle dans la pratique, a été démontré dans une étude de l'Association Européenne Culture et Informatique, réalisée à l'instigation des ministères français de l'Intérieur et de la Justice.

Risques

Indiscrétion : on pense naturellement aux spécialistes système, qui -quoi qu'on fasse- pourront toujours se donner les moyens d'accéder à la totalité des données magnétiques, mais on n'oubliera pas les développeurs, qui ont accès à de multiples sources documentaires, parfois confidentielles, dans le cadre de leur activité d'étude.

Détournement d'informations, au profit de tiers ou à des fins d'enrichissement personnel.

Fraudes.

Introduction ou maintien de failles dans la sécurité par négligence ou indifférence.

Comportement illégal vis-à-vis de sites informatiques externes (intrusions).

Parades

Séparer les fonctions : il est beaucoup plus difficile de générer un faux ordre de transfert quand on ne connaît qu'une partie des procédures ou des données nécessaires.

N'accorder que les droits d'accès indispensables à l'exécution d'une fonction : un mainteneur n'aura jamais besoin, quoiqu'il puisse prétendre, du niveau de privilèges d'un spécialiste système.

Pister systématiquement l'utilisation qui est faite des niveaux de privilèges élevés.

Doter le personnel informatique d'un code de déontologie maison (dont on trouvera les grandes lignes ci-dessous), ou utiliser celui publié par l'AFIN (Association Française des INformaticiens).

Imposer aux prestataires externes, par des clauses contractuelles, le respect du code déontologique de l'entreprise, ou à défaut d'un code d'éthique reconnu par la profession (par exemple, pour les prestataires intervenant sur la sécurité, le Code d'Ethique des Métiers de la Sécurité des Systèmes d'Information, publié par le CLUSIF).

Code de déontologie de l'informaticien

Il doit comprendre au minimum :

- son champ d'application (quels métiers ? quels prestataires de services ?)
- un exposé des motifs (pourquoi imposer des règles propres aux informaticiens ?)
- des règles générales (ex : respect des méthodes, respect de la disponibilité, de l'intégrité et de la confidentialité des données...)
- des règles faisant appel au principe de loyauté (ex : non-concurrence, respect de la législation à laquelle est tenue l'employeur...)
- des règles s'appuyant sur le respect de la propriété (utilisation de l'outil informatique, propriété des logiciels...)
- les règles particulières à l'entreprise visant à protéger la sécurité de ses informations.

Critères de qualité

Disposer d'une bonne organisation pour dispenser la culture sécuritaire, avec des relais ou des correspondants dans toutes les entités (y compris l'informatique).

Disposer d'un code de déontologie interne clair, précis, connu, admis par tous (et existant si possible pour l'ensemble des métiers considérés comme sensibles) ; inclure certains éléments dans les contrats de travail et dans le règlement intérieur.

Attention : les règles énoncées dans ce code ne doivent pas être plus contraignantes que la réglementation en vigueur (lois, règlement intérieur, instructions internes) !

Remettre ce Code personnellement et solennellement à tous les agents concernés.

Accompagner cette remise d'une large communication auprès de tout le personnel.

Mettre au point avec les S.S.I.I. des contrats-cadres incluant des clauses de sécurité et d'éthique, et les faire respecter.

Fiche 25 : Procédures de recette

Définition

Entre la phase de développement d'un projet applicatif et la phase de mise en production effective se situe la phase de recette. Il est en effet nécessaire qu'une application donne les résultats attendus, ce qui se fait à travers la recette technique (ou tests d'intégration), qu'elle corresponde aux besoins des utilisateurs, ce qui se vérifie à travers la phase de recette utilisateur ou bancaire, qu'elle soit apte à être mise en production ce qui est vérifié dans la phase de recette de certification ou pré-production ; enfin la cohérence de l'ensemble applicatif doit être vérifiée en réel à travers une phase de recette sur site-pilote.

La phase de recette est indépendante de la phase des tests unitaires de programmes qui est à la charge des développeurs.

Risques

Les risques encourus touchent à l'intégrité et à la disponibilité des données et traitements. En effet, une application qui n'a pas été recettée correctement peut, soit ne pas correspondre aux desiderata des utilisateurs et du maître d'ouvrage, soit ne pas correspondre aux normes d'exploitation, soit présenter des "bugs" ou des interférences avec l'existant applicatif non détectés au niveau des tests unitaires ou d'intégration, soit pour les applications temps réel, présenter des temps de réponse désastreux. Dans tous les cas, les services rendus aux utilisateurs et aux clients s'en ressentiront.

Parades

Les procédures de recette doivent être complètement intégrées à la méthodologie de développement utilisée dans l'entreprise (exemple : MERISE). Elles doivent donc faire l'objet d'une formalisation détaillée. Les activités de recette s'intègrent dans les activités de test. Elles doivent donc se faire sous la responsabilité d'une personne nommément désignée qui en assure le suivi et le contrôle. Il s'agit du responsable de recettes qui fait partie de l'équipe projet. Pour concrétiser la mise en œuvre de cette méthodologie, il est bon de créer des procès-verbaux de recette qui attesteront, à chacune des étapes du recettage indiquées ci-dessus, de l'étendue des tests réalisés et des résultats obtenus. Signés par les parties concernées, ils seront conservés dans un dossier-projet gérant la partie administrative de la vie du projet. Parallèlement, il faut se doter des moyens de reconstituer les tests à tout moment en cas de problème de déroulement des traitements.

Les tests réalisés auront les fonctionnalités suivantes :

- tests de recette technique : vérifier l'enchaînement fonctionnel des divers composants des traitements et le bon interfaçage avec l'environnement,

- tests de recette bancaire : vérifier les fonctionnalités de l'application par rapport aux spécifications exprimées par l'utilisateur,

- tests de certification : assurer la réception technique de l'application dans un environnement de pré-production, et avec les procédures d'enchaînement réelles, afin en particulier de tester les performances et les charges associées aux traitements,

- tests de recette sur site-pilote : vérifier l'intégrabilité sur site bancaire réel.

Afin de ne pas perturber le fonctionnement normal de la production informatique, il est préférable de travailler sur des environnements dupliqués. A l'inverse, il faut prendre garde à correctement gérer l'espace disque engendré par la démarche.

Critères de qualité

Il s'agit de suivre via un tableau de bord des indicateurs tels que :

- pourcentage d'applications suivant la démarche de recettage complète,

- nombre "d'abends" constatés dans le mois suivant la mise en production,

- nombre de retours pour modification dans le mois suivant la validation de la recette.

Existence de procès-verbaux de gestion.

Fiche 26 : Propriétaires et classification des informations

Propriété d'informations

Le système d'information et son environnement logistique sont considérés comme étant un gisement de risques important. S'il paraît aisé de se prémunir des risques matériels, il en va tout autrement des risques liés aux informations proprement dites.

L'information représente l'élément de base d'un système d'information. Son immatérialité la rend très vulnérable aux interventions et à la confidentialité. Elle constitue un risque important à la fois dans la qualité d'un processus applicatif, mais aussi dans la qualité du système décisionnel. L'information doit être sécurisée.

Il est vraisemblable que l'ensemble du personnel soit très différemment sensibilisé à la qualité et à la sécurité de toutes les informations. Il faut pourtant garantir que les informations et les traitements soient justes, que la confidentialité soit assurée, que les mises à jour soient opportunes, que les habilitations soient respectées. La solution réside dans la définition d'un responsable fonctionnel dont la mission serait de définir et de choisir ses données, charge à un gestionnaire de les saisir et de les entretenir.

Classification des données

Les informations ne représentent pas pour l'entreprise un même niveau de sensibilité. Il serait soit imprudent soit utopique de vouloir les traiter et les contrôler avec un même niveau de sécurité. La classification des données permet de sérialiser les risques et de les traiter selon leur degré de priorité.

La définition de ces classifications est à l'appréciation de chaque entreprise, mais elles doivent correspondre aux niveaux de protection souhaitée. L'expérience a démontré qu'il faut se limiter à 4 ou 5 classes. Les principes de classification s'appuient tout d'abord sur les attributs de la sécurité que sont la disponibilité, l'intégrité et la confidentialité. L'intensité de l'attribut associée à une information, détermine le niveau de caractère de sécurité. Ainsi un niveau de disponibilité élevé pour une information détermine-t-il un caractère particulièrement vital de celle-ci. Un niveau d'intégrité élevé souligne une information à caractère extrêmement sensible. Et enfin un niveau de confidentialité élevé caractérise une information excessivement confidentielle. Dans cette dernière classification il est nécessaire de distinguer les niveaux de confidentialité selon le type de population auquel ils s'appliquent : interne, interne/restreint, interne/secret.

Pour obtenir un classement graduel des informations, il est courant (valorisation Marion) d'attribuer une valeur numérique de 0 à 4 à chaque information et pour chaque caractère de sécurité DIC. Ainsi pour une information nécessitant une bonne disponibilité, une forte intégrité et une confidentialité de type interne, on attribuera respectivement les valeurs 3, 4 et 2. Un poids particulier (ou coefficient de pondération) peut être appliqué à chacun des attributs de sécurité pour renforcer son caractère stratégique ; par exemple : 2 pour la disponibilité, 3 pour l'intégrité et 1 pour la confidentialité. L'impact absolu pour cette information s'obtiendra de la manière suivante : (3x2) + (4x3) + (2x1) = 20, sur une échelle dont le maximum est de [(4x2)+(4x3)+(4x1)] = 24.

Pour reprendre les niveaux de confidentialité cités plus avant, nous proposons la définition suivante des classes de confidentialité :

*banale** : informations non-confidentielles qui peuvent circuler librement en interne comme en externe.

interne : informations qui peuvent circuler librement dans l'entreprise. Elles nécessitent une protection, soit qu'elles appartiennent au client soit qu'elles présentent un risque pour le développement de l'entreprise.

interne/restreinte (sensible) : informations dont la divulgation nuirait au fonctionnement d'une entité. Elles ne doivent être communiquées (même à l'intérieur de l'entreprise) qu'aux personnes directement concernées, et n'être manipulées que par des personnes précisément identifiées.

interne/secret (stratégique) : informations (rares) dont la divulgation pourrait porter atteinte aux intérêts, à la sécurité ou même à l'existence de l'établissement.

Risques

L'absence de propriétaire/responsable et de classification entraîne un manque de concertation dans la définition et la manipulation des informations :

- les responsabilités sont diffuses et délicates
- les règles de gestion ne sont pas suivies
- les informations ne sont pas protégées
- il y a un risque de multiplication de données
- les définitions et le mode de gestion peuvent être incohérents (cloisonnement par activité)
- les contrôles programmés ne peuvent pas être généralisés et normalisés.

Dans ce cas, il est difficile voire improbable d'être efficace dans la sécurisation d'un système d'information. Toutefois la mise en œuvre d'une telle organisation est délicate, car elle nécessite une cohérence et une précision parfaites dans l'attribution des responsabilités des "propriétaires". Des conceptions et des règles de gestion individualisées et personnalisées par les propriétaires iraient inévitablement à l'encontre de la démarche.

Parades

Ainsi donc, si nous voulons être assurés de la qualité et de la sécurité des informations, il faut en attribuer formellement la responsabilité à quelques dépositaires. Il convient pour cela de découper le système d'information en domaines d'activités, puis d'attribuer une responsabilité fonctionnelle pour la gestion de chaque domaine. La règle consistera alors, à ce qu'aucune information d'un domaine ne puisse être créée, traitée ou sortie sans l'accord et le contrôle du responsable.

* ou "publique", ou "externe".

L'appellation de cette fonction et son champ d'intervention peuvent varier selon les établissements, mais naturellement ils doivent être décrits et valorisés dans une démarche de Direction Générale. L'institution d'une administration de données permet d'animer, de surveiller et d'assurer la cohérence du système d'information. Il reviendra à cette fonction "informatique" de communiquer les définitions des données, d'en gérer la signification, d'en élaborer les modèles...

Ce propriétaire/responsable, nommément désigné, sera chargé de la définition de l'évaluation et de la classification des informations dont il a la charge. Il assumera aussi la définition et la révision périodique des règles, procédures, et autorisations d'accès des informations.

La classification stratégique des données, des règles et des documents, prendra en compte les critères d'intégrité, de disponibilité et de confidentialité des informations.

La classification minimum consiste à identifier les informations stratégiques qui, en cas de destruction, vol, perte, etc., peuvent entraîner un préjudice grave pour l'entreprise.

Les droits devront être précisés en terme de : visualisation, création, suppression et mise à jour, en spécifiant les identifiants, authentifiants et circonstances. Un tableau des domaines pourra être élaboré, reportant les propriétaires, les accédants, les délégués, les gestionnaires...

Cette démarche d'affectation et de classification -similaire à la définition de la partie stratégique du SI- doit faire l'objet d'une information et d'une sensibilisation générale, car cette organisation s'impose à toutes les fonctions de l'entreprise.

Critères de qualité

Dans le système d'information, chaque fichier et chaque information ont un propriétaire/responsable et un seul.

Le propriétaire/responsable est le seul à donner les habilitations d'accès à ses informations. Il possède un moyen de contrôler les différents accès.

La classification des données est arrêtée et des procédures spécifiques sont définies pour garantir leur sécurité.

La réglementation interne institutionnalise ces nouvelles dispositions.

L'Audit intègre cette réglementation dans ses contrôles et vérifie la bonne application.

Le classement des informations est revu périodiquement avec les interlocuteurs concernés.

Les méthodes et normes de développement informatiques ont été adaptées aux réglementations de propriété et de classification.

Fiche 27 : Relations utilisateurs/informaticiens

Définition

Toute prestation met en relation un groupe de personnes constitué d'utilisateurs et d'informaticiens.

Les deux protagonistes de cette prestation sont :

- le Maître d'ouvrage (le Demandeur)
- et le Maître d'œuvre (le ou les Réalisateur(s)).

Cette prestation peut se formaliser sous forme de contrat de service entre le Maître d'ouvrage et le Maître d'œuvre. Ce contrat s'appelle :

- soit un contrat de développement ou cahier des charges, s'il s'agit d'études informatiques,

- soit un contrat de service (ou convention de service), s'il s'agit de production informatique.

Les attributions du Maître d'ouvrage sont :

- montrer le bien-fondé de la partie économique de la prestation

- exprimer un besoin et le détailler en terme de fonctionnalités et de budget.

Le Maître d'œuvre satisfait le besoin en mettant en œuvre des moyens de réalisation et de production.

Un contrat de service est un engagement volontariste de progrès de la part des intervenants amenés à fournir une prestation.

Ce contrat se matérialise sous forme d'un accord cadre simple et sans ambiguïté.

Cet accord peut concerner une prestation interne ou externe à l'entreprise sur un objectif d'études informatiques (projet/développement) et/ou de production (exploitation/maintenance des applications).

En fait, toute relation client/fournisseur devrait faire l'objet d'un contrat de service.

Risques

Au départ, les informaticiens étaient une population à part détenant pour beaucoup les clés du mystère de l'informatique. Cela est de moins en moins vrai : la vulgarisation de l'outil informatique y est pour beaucoup.

Cependant, bon nombre de personnes touchant à l'informatique se croient "informaticien" : chacun est convaincu de parler le même langage. Point s'en faut ; il en résulte une mauvaise compréhension, une mauvaise concertation.

De cette situation est née une série de problèmes, malentendus et autres aléas de la vie professionnelle. L'objet de la prestation est alors mal défini (rôles mal délimités, réflexions omises, expression des besoins incomplète, critères de productivité et de qualité non définis). Ceci engendre une insatisfaction des utilisateurs, un dépassement des budgets, des ressources supplémentaires.

Pour couper court à cette situation inconfortable, les relations Utilisateurs/Informaticiens doivent être clairement exprimées ; ne pas y adhérer peut entraîner à une perte de productivité.

Parades

Le contrat de service ou de développement, entre maître d'ouvrage et maître d'œuvre, permet d'y faire face.

Le contrat de service doit indiquer :

- l'objectif de la prestation énoncé par le maître d'ouvrage,
- le nom des intervenants ou de leurs représentants ayant pouvoir à s'engager,
- le champ d'action,
- la date de validité ou de reconductibilité par période de tacite reconduction
- le système de référence de mesure retenu pour analyser les prestations tant pendant le développement qu'une fois le produit fini,
- les délais,
- les normes et procédures de sécurité, ainsi que le niveau de sécurité.

Tout contrat doit décliner,

- Un Maître d'ouvrage (le demandeur) :
  - # il assume la responsabilité d'ensemble, prend les décisions et arbitre le cas échéant.
  - # il est responsable de la conduite globale du projet (vérification des moyens alloués, maîtrise du budget et respect des coûts et délais, fourniture des standards à respecter).
  - # il s'assure que le produit livré est conforme aux besoins exprimés.
- Un Maître d'œuvre (le réalisateur) :
  - # il est responsable du projet informatique proprement dit (conception, équipe de développement, documentation).
  - # il doit rendre compte au maître d'ouvrage.

Critères de qualité

La signature d'un tel contrat suit une démarche méthodologique basée sur 5 étapes :

1) Cadrage de la prestation (identification des représentants, rôle des acteurs, objectifs et missions précises, limites, charges, délais, engagements réciproques, groupe de travail).

2) Schéma général de traitement (schéma d'organisation, documentations, exigences, modalités de mise en place, tableau de bord, ébauche du plan du contrat).

3) Rédaction du contrat (Plan du contrat : objet du contrat, définition du champ d'application, condition de production et engagement, définition de procédures spécifiques en cas d'incident, suivi des résultats, règle de gestion du contrat, conditions financières, cadre juridique).

4) Mise en place du contrat (signature bipartite, probatoire, opérationnelle et contractuelle).

5) Gestion et suivi du contrat (planning des réunions, compte-rendu, état d'avancement, suivi d'activités, comparaison d'objectifs).

D'autre part, en terme de sécurité, le demandeur doit exprimer ses besoins, s'ils sont spécifiques, mais le réalisateur doit respecter au minimum les standards de l'entreprise.

Fiche 28 : Sauvegardes : procédure et conservation

Définition

Pour permettre le redémarrage d'un système informatique après un sinistre, matériel ou logique, ayant détruit ou altéré de façon importante les supports de données, il est nécessaire d'avoir préalablement effectué des copies de celles-ci afin de disposer de l'image du système à un moment aussi proche que possible de celui du sinistre. A ce titre, le plan de sauvegarde des données informatisées (et éventuellement non informatisées) est le complément indispensable du plan de secours, l'un ne pouvant aller sans l'autre. Pour être établi, il doit tenir compte des scénarios retenus pour la construction du plan de secours. On distinguera plusieurs types de sauvegardes :

- les sauvegardes pour plan de secours,
- les sauvegardes applicatives destinées aux reprises de traitement,
- les sauvegardes de très haute sécurité (THS) dont l'objet est la restauration d'un système à la suite d'un sinistre immatériel partiel ou total.

Les besoins réglementaires peuvent conduire à l'établissement de sauvegardes spécifiques (délai de reprise de la Direction générale des impôts ; délais exigés par la Commission bancaire ...).

Parades

Il est souhaitable de mettre en œuvre un plan de sauvegarde complémentaire du plan de secours et permettant de satisfaire aux besoins de celui-ci. Au minimum, il faut établir sur une base régulière une copie des données de l'entreprise, aussi bien pour les grands systèmes que pour la micro-informatique. Pour les établir il est préférable d'utiliser un produit du marché plutôt qu'un outil-maison. La périodicité d'établissement des sauvegardes doit être compatible avec les besoins déterminés pour la mise en œuvre du plan de secours. Il est en effet souhaitable de minimiser les traitements de restauration permettant de reconstituer la situation au moment du sinistre. Les sauvegardes doivent être collectées et conservées hors de l'environnement immédiat des machines dans des locaux adaptés (conditions climatiques) et protégés (feu, dégât des eaux, contrôle d'accès). Au moins pour les gros systèmes, il est souhaitable de les conserver hors de l'entreprise. Il est nécessaire de contrôler en permanence l'état d'inventaire des sauvegardes. Ces sauvegardes dites "de plan de secours" ne devraient jamais être utilisées à d'autres fins, ceci pour en garantir la disponibilité permanente et immédiate. L'accès à ces sauvegardes doit faire l'objet de procédures strictes afin d'en garantir autant que faire se peut l'intégrité et la disponibilité. Les essais du plan de secours permettront de valider le plan de sauvegarde. Il est souhaitable par ailleurs de contrôler périodiquement le contenu de ces sauvegardes afin de vérifier leur lisibilité d'une part et, d'autre part, l'intégrité de leur contenu.

S'agissant des sauvegardes micro-informatiques, si celles-ci sont établies par les utilisateurs, il convient de leur donner des moyens ergonomiques de réaliser celles-ci, et leur collecte pour mise en lieu sûr est souhaitable. Celles-ci pourront être utilisées en cas d'incident disque ou de problème de virus. Le système d'établissement des sauvegardes doit être aussi automatisé que

possible. Un transfert automatique des données vers un niveau serveur ou central permet de dégager l'utilisateur des contraintes liées au lancement périodique d'un traitement. L'information des utilisateurs vis-à-vis de la nécessité d'établir des sauvegardes reste indispensable.

Critères de qualité

Il s'agit de suivre via un tableau de bord des indicateurs tels que :

- nombre des tests périodiques de sauvegarde,
- respect des horaires d'établissement des sauvegardes,
- nombre d'anomalies constatées sur le stock de sauvegarde,
- contrôle de qualité des sauvegardes.

voir aussi fiches n° 3
n° 22

Fiche 29 : Sécurité des bâtiments, des locaux et de l'environnement

Définition

La sécurité d'un site informatique est liée :

Au choix de la localisation géographique du bâtiment qui abrite les salles informatiques.

À l'implantation des plates-formes informatiques dans le bâtiment.

Risques

La localisation géographique du bâtiment qui héberge les installations informatiques peut induire des risques liés à l'environnement. Des activités industrielles ou des phénomènes naturels locaux peuvent donner lieu par exemple à :

- des pollutions atmosphériques : proximité d'un aéroport avec émanation de kérosène qui se dépose en fine pellicule sur les radiateurs de refroidissement qui sont ventilés et diminue considérablement leur efficacité.

- des pollutions sismiques : proximité d'une autoroute ou d'une voie ferrée qui transmet des vibrations nocives dans le bâtiment.

- des pollutions électromagnétiques : proximité d'installations rayonnantes d'autres activités industrielles.

- des risques majeurs : accident dans un couloir aérien, explosions, incendies, émanations de substances toxiques dans une zone portuaire ou provoquées par le passage d'un transport à risque (ferroviaire, routier, fluvial), inondations et glissements de terrains.

L'implantation géographique et l'environnement urbain ou rural ne sont pas neutres pour des agressions d'origines humaines (ex : envoi ou dépôts d'explosif...). Un site à l'écart d'infrastructures collectives sera par exemple plus aisément coupé de ses sources d'alimentation ou de ses flux de communications.

L'exploitation du bâtiment (entretien courant, travaux d'aménagement...), dont la maîtrise est souvent confiée aux services généraux des entreprises, induit des risques spécifiques aux vulnérabilité des équipements informatiques (ex : ponçage près d'une batterie de disques...).

Parades

Les risques liés à la localisation géographique doivent être appréciés avant la décision d'installer un centre de calcul. Quand cela est possible, la construction du bâtiment sera adaptée aux contraintes de sécurité propres aux centres informatiques. Les différents corps de métiers et entreprises qui participeront à l'installation des infrastructures du bâtiment seront sélectionnés sur leurs capacités réelles à traiter ce type de chantier.

Une localisation géographique non isolée et une banalisation du bâtiment éviteront d'attirer l'attention depuis l'extérieur sur un point particulièrement sensible. Au sein même du bâtiment les matériels seront placés dans les parties les plus centrales, elles-mêmes compartimentées (ex : cloisonnement entre les calculateurs et les moyens d'impressions...). On évitera qu'ils soient visibles de l'extérieur ou même qu'ils soient situés sur la périphérie du bâtiment. On rencontre souvent deux types d'implantation :

- plate-forme informatique au milieu d'un premier étage ceinturée par des bureaux à accès bien contrôlés ;

- centre de calcul en sous-sol bien protégé des risques de dégâts des eaux et correctement isolé des installations techniques à risque (ex : chaufferie...).

Tout entretien ou aménagement des infrastructures du bâtiment sera obligatoirement supervisé par le service technique immobilier de l'entreprise qui est responsable du maintien de la cohérence des mesures de sécurité.

Critères de qualité

- Suivi des incidents induits par la localisation du bâtiment, les interventions sur les infrastructures (service interne ou prestataires de service), l'exploitation du bâtiment.

- Nombre de points extérieurs ayant vue sur les locaux sensibles.

- Perméabilité aux influences extérieures (ex : vibrations, pollutions...).

- Nombre de visiteurs ou de passages à proximité des zones sensibles qui ne sont pas liés directement à l'activité du centre de calcul.

- Consignes particulières élaborées et communiquées dans l'entreprise ainsi qu'auprès des prestataires de service.

- La sécurité du bâtiment, les procédures d'exploitation (ex : visite des pompiers de la localité) et de maintenance de celui-ci seront périodiquement auditées.

- Des tests d'évacuation du personnel seront menés et des constats seront dressés.

- La diversification d'approvisionnement des sources d'énergies et des flux de communication sera répertoriée.

Fiche 30 : Sécurité des micro-ordinateurs

Définition

La micro-informatique permet aux Établissements de Crédit de répondre efficacement à leur besoin d'industrialisation et de productivité. Cependant ce mouvement de modernisation a été trop souvent réalisé, par étapes, en réponse à des besoins ponctuels et individuels, sans qu'aucune réflexion générale n'ait été entreprise.

Certains établissements se trouvent ainsi en présence d'un parc non négligeable d'équipements "micro" voire même "réseau", alors que les répercussions inévitables sur les structures organisationnelles et les règles de gestion n'ont toujours pas été analysées.

Il est naturel de constater, dans ce cas, que les résultats attendus de productivité sont loin d'être atteints. Le constat est d'autant plus décevant que la vulnérabilité de l'entreprise s'est accrue, du fait des risques induits par un outil mal maîtrisé, et par les risques inhérents à ce type de matériel "léger".

La sécurité des ordinateurs est un des points faibles de la micro-informatique, et il est évident que la portabilité de certains d'entre-eux accroît le risque de l'entreprise et dégrade sensiblement son niveau de sécurité.

Risques

L'absence d'une organisation structurée dédiée à la micro-informatique, expose l'établissement à un nombre important de risques de gestion, d'intégration et de fiabilité. Ces risques sont à apprécier en regard des bénéfices évidents de la micro qui sont la souplesse, la réactivité et l'adéquation aux besoins de l'utilisateur.

La vulnérabilité de ce nouvel environnement repose sur des faiblesses d'ordre organisationnelles et réglementaires dont voici les principaux éléments :

- l'absence de maîtrise du parc en nombre, en localisation, en configuration matérielle et logicielle,
- l'anarchie dans les commandes non-centralisées, de matériels et de logiciels hétérogènes,
- l'autonomie extrême dans les choix d'outils, les développements et les procédures de gestion,
- l'absence de structure pour l'accueil, l'assistance, l'intervention, la formation,
- la potentialité d'action importante et non maîtrisée dans les accès ou la manipulation d'informations,
- les potentialités d'illégalités : fraude, malveillance, vol, piratage, accès illicite étranger,
- la fragilité et la sécurité relative du poste de travail : virus, sauvegardes, documentation, environnement,

- l'intégration relative des applications micro dans le système d'information,
- la dilution de la responsabilisation et la mauvaise appréhension de la continuité de fonctionnement.

L'individualisme apporté par la "micro" rend plus difficile la tâche au "manager" qui a pour responsabilité la cohérence de ses outils, la normalisation de ses procédures, la fiabilité et la pérennité de ses développements.

La mobilité des portables accentue la vulnérabilité de l'entreprise en l'exposant à des risques supplémentaires. En effet, un portable est plus soumis à certains risques qu'un poste fixe, par exemple le vol, la perte, le bris de machine, le détournement d'informations, l'introduction de virus, etc. Le risque s'accroît dès lors que les matériels sont transportés en dehors de l'entreprise.

La vulnérabilité s'applique non seulement au matériel, mais aussi aux informations contenues sur le disque dur. La perte et le dégât matériels ne sont pas les incidents les plus graves, il est beaucoup plus traumatisant et stratégique de perdre des données soit du fait de leur reconstitution difficile, soit du fait de l'utilisation incontrôlée du nouveau possesseur.

Il existe enfin un risque plus général qui est la méconnaissance de l'environnement. Cette situation entraîne très souvent des manipulations hasardeuses de la part des utilisateurs qui ont pour effet de dégrader sensiblement la qualité et la productivité du service.

Parades

Pour qu'une démarche de généralisation de la "micro" soit positive, il est nécessaire de l'aborder d'une manière globale. Elle doit nécessairement relever d'une volonté de la Direction générale, passer par la sensibilisation et la responsabilisation des utilisateurs, intégrer la mise en place d'une organisation, reposer sur une réglementation.

La sensibilisation et la responsabilisation du personnel est un des points clefs de la sécurité "micro". Il faut entreprendre des rencontres avec le personnel afin qu'il adhère à la politique de l'entreprise, à l'organisation mise en place, et au respect des moyens mis à sa disposition. Cette démarche est d'autant plus nécessaire s'il est mis en œuvre des portables.

Une organisation structurée dédiée à la micro-informatique, c'est le point de départ incontournable d'une bonne sécurisation.

- En premier il faut gérer le parc. Cela consiste à identifier et inventorier le parc, puis à suivre précisément son évolution. Il faut ensuite homogénéiser et centraliser les achats de matériels et de logiciels, puis élaborer des règles de gestion rigoureuses. L'organisation en place reposera sur des méthodes et des règles qui justifieront la démarche et garantiront le bon fonctionnement de l'ensemble. L'étiquetage sécurisé est une des solutions répondant à la nécessité d'inventaire et à la sécurisation des postes (un atout pour les portables).

- L'organisation permettra d'effectuer une veille technologique pour favoriser l'évolution logique des équipements et des logiciels et orienter les demandeurs vers des solutions à jour.

- Le déploiement de la "micro" correspond à une période propice où la sensibilisation et la formation des utilisateurs concernés doit être réalisée. Des guides d'utilisation et des consignes doivent être commentés et distribués afin d'éviter les manipulations et initiatives hasardeuses.

Des conseils et des normes de développement peuvent être formalisés pour orienter ou réglementer les initiatives individuelles. Une assistance méthodologique, assurée par un service technique, permet aux responsables d'entités d'utiliser efficacement leurs équipements et d'en maîtriser les limites de sécurité.

- L'utilisation des portables doit faire l'objet d'une réflexion particulière pour apprécier le risque encouru et limiter les domaines d'activités. La sensibilisation spécifique du personnel concerné, sa responsabilisation et le développement d'une réglementation interne appropriée, doit permettre l'application de contraintes particulières à ces équipements. (Données confidentielles sur disques amovibles, données cryptées, logiciel de contrôle d'accès, immobilisation du matériel en dehors du transport). L'opportunité d'un tel équipement doit être comparée aux enjeux et aux risques de l'entreprise.

- Il faut que l'organisation intègre l'assistance de l'utilisateur pour limiter les pertes de temps et répondre efficacement au souci de fonctionnement. Cette fonction d'assistance doit comprendre à la fois l'administration et la résolution des problèmes.

Cela nécessite de prendre en charge complètement le support des utilisateurs. C'est une charge non négligeable qu'il faut impérativement chiffrer et inclure dans le budget de développement de la micro.

L'accroissement des risques "viraux" et la complexité de la réparation incitera à la mise en place d'une méthode et de procédures pour rétablir au plus vite et dans les meilleurs délais l'environnement de travail.

Une réglementation générale incitera les utilisateurs et les responsables à respecter les règles de fonctionnement et les règles légales pour se prémunir des risques spécifiques à la micro (virus, copyright et vol).

Une réglementation spécifique devra définir le cadre des développements particuliers autorisés : le contexte, le cadre du développement, la documentation, la sécurité, et la qualité.

Dans les procédures d'intervention, il est bon d'intégrer un contrôle systématique de l'installation par le technicien (architectures matérielle et logicielle) puis de comparer le résultat à la fiche inventaire.

Critères de qualité

Les demandeurs de micro et de logiciels s'adressent à une seule entité fonctionnelle pour exprimer leurs besoins.

L'entreprise possède un inventaire exhaustif permanent de toutes ses installations micro.

Les types d'équipements et de logiciels sont limités et cohérents.

Une gestion permanente des incidents matériels et logiciels permet de situer le niveau de fonctionnement et de satisfaction des utilisateurs.

Toutes les applications sensibles sur micro sont répertoriées et contrôlées sur leur forme.

La fonction micro est maîtrisée dans ses coûts d'investissements et de fonctionnement.

Une politique anti-virus a été arrêtée et mise en œuvre. Une structure d'intervention et une méthode a été mise en place. Il existe un processus spécifique de traitement des supports externes.

Le règlement intérieur interdit le piratage de logiciel, des procédures permettent d'en contrôler la bonne application.

Utilisation d'outils de sécurité selon le niveau de sécurité souhaité : contrôle d'accès, authentification, chiffrement, anti-virus, sauvegarde.

Affectation d'un local pour les sauvegardes utilisateurs.

Environnement en conformité avec les règles et standards (climatisation, électricité, câblage...).

Les portables font l'objet d'une procédure particulière de sensibilisation et de responsabilisation. Un procédé permet de les attacher au poste de travail.

Fiche 31 : Sécurité des télécommunications

Définition

La télécommunication est un réseau de communication informatique basé sur le principe de la transmission à distance de l'information entre ordinateurs : c'est l'ensemble des procédés de transmission d'information à distance.

Le but recherché est la réduction des délais de transmission des informations, l'élimination des saisies multiples (saisie à la source) et l'amélioration de la fiabilité des informations.

Ce type d'échange de données facilite une politique de gestion industrielle, voire une standardisation de l'échange.

L'échange peut concerner divers domaines : virements et prélèvements bancaires, ordres financiers, positions de comptes, statistiques, etc.

Risques

La généralisation de la micro-informatique et le développement des réseaux de transmissions des données accessibles par téléphone (TRANSPAC, par exemple) sont d'autant de facilités pour les fraudeurs.

Deux niveaux de risques :

1) les risques physiques inhérents au Terminal et/ou à l'Ordinateur central.

De par le fait qu'ils sont logés dans un local privé, les conséquences sont peut être moins importantes que les risques logiques. Ces risques peuvent être réduits grâce à des moyens appropriés mis en œuvre par l'intéressé.

Par ailleurs, le risque de détérioration physique de la ligne est peu probable eu égard l'importance des dégâts que peut provoquer une attaque logique.

2) les risques logiques dus au transfert de l'information par ligne téléphonique publique

Malgré une transformation en tonalités sonores, l'écoute passive en ligne permet, en toute facilité, de quérir une foule de renseignements (mot de passe, données). Les conséquences ne sont pas toujours faciles à évaluer.

Rien n'empêche un tiers non autorisé de s'interposer entre deux correspondants : l'intrus pourra se brancher sur la ligne et tenir le rôle d'un véritable réémetteur (écoute active).

Ces deux types d'écoutes (passive ou active) sont difficilement décelables ; en effet, actuellement les détecteurs d'écoutes téléphoniques sont peu efficaces. Il existe une offre dans ce domaine par des sociétés spécialisées.

Parades

Si prendre la ligne grâce à un terminal, directement ou par modem, en connaissant le mot de passe est aussi facile, il faut prévoir un certain nombre de protections physiques ou logiques à tous les niveaux du réseau.

Au niveau Terminal :

assignation physique (le terminal est dédié à faire des actions limitées et répertoriées)
surveillance locale de l'activité sur le terminal
blindage ou faradisation (protection contre des ondes électromagnétiques)
gestion des mots de passe
authentification par carte à mémoire
dévalidation des fonctions du terminal : activation d'un TIME-OUT, terminal hors service
code d'urgence (blocage du terminal par code programmé).

Au niveau Modem :

protection mécanique du matériel
redondance des frontaux (doublement du parc, back up)
redondance des liaisons primaires
coffrets ou processeurs de chiffrement
surveillance des têtes de ligne (analyse de l'activité des messages réseau)
si Réseau Commuté : procédure de rappel RC, protection des numéros de téléphones RC (appel des lignes réseau, prise de ligne).

Au niveau de la Ligne :

type de liaison (fibre optique, faisceau hertzien)
redondance (doublement des lignes, maillage du réseau)
protection et surveillance des chemins de câble
détection des écoutes (repérage de toute activité anormale)
chiffrement
type de réseau (public, privé...).

Au niveau de l'Ordinateur central :

contrôle des accès (autorisation aux ressources)
journalisation des accès (signalétique de l'utilisateur)
gestion des anomalies (tentatives d'accès avortées)
contrôle et analyse des transmissions
stockage des mots de passe.

En conséquence, il est recommandé d'avoir :

- Un service de maintenance du matériel (service interne ou contrat auprès de sociétés externes),
- Une cellule de surveillance et de pilotage du réseau,
- Une cellule d'assistance technique compétente pour tout dépannage sur demande des utilisateurs.

Critères de qualité

L'état du réseau doit toujours être opérationnel, donc disponible.

Le débit du réseau doit être fluide et régulier.

L'information doit être chiffrée afin de garantir la confidentialité et l'intégrité des données (emploi d'un outil de chiffrement) dans le respect de la réglementation.

L'accès aux ressources est fonction de l'identification et de l'authentification des usagers.

Toute tentative avortée doit être analysée précisément, et comparée aux précédentes (un système de contrôle d'accès doit être opérationnel en permanence). L'échange de données par télécommunication passe par un échange d'authentification réciproque géré par un outil approprié.

La transmission des données est soumise au principe de la non-répudiation,

>> origine : l'émetteur ne peut contester l'envoi,
>> délivrance : le récepteur ne peut contester avoir reçu le message.

Une architecture redondante ou de secours est également un gage de qualité.

NB : POINT SENSIBLE

Fiche 32 : Sécurité d'accès aux réseaux

Définition

Le développement des réseaux fait naître de nouveaux besoins en matière de sécurité des Systèmes d'Information que ce soit pour les communications interentreprises ou pour les besoins internes à l'entreprise.

- La multiplication des échanges de données informatisées (EDI) entre partenaires multiples génère de nouvelles difficultés, notamment en matière de preuve des transactions réalisées. Ces exigences en matière de sécurité ne sont réellement abordées qu'au travers des réseaux professionnels, représentés principalement dans le domaine bancaire par GSIT, RCB ou SWIFT, mais ne sont que peu ou pas appliquées dans les réseaux d'entreprises sauf recours à un tiers assurant la conservation de la preuve de l'échange (VERIDIAL) ou utilisation du protocole ETEBAC5.

- L'évolution technologique a conduit l'entreprise vers une répartition du Système d'information sur des machines de taille et d'architecture variables, des micro-ordinateurs aux systèmes centraux communiquant par des voies privées ou des réseaux publics (RTC, Transpac, Numeris).

Risques

Pour éviter des risques évidents, l'authentification et la gestion des droits des utilisateurs devraient pouvoir être gérées de façon homogène et cohérente sur l'ensemble du Système d'Information.

Ces fonctions peuvent être correctement maîtrisées à partir des logiciels disponibles sur les systèmes centraux, mais sur les réseaux locaux ou les systèmes départementaux l'offre du marché ne présente pas une maturité suffisante dans ce domaine. Or le besoin actuel se situe déjà au-delà du niveau contrôle d'accès sur chacun des systèmes. Ce besoin est bien au niveau réseau, dès l'établissement d'une communication, et ce pour garantir la disponibilité du réseau. Pour s'en convaincre, il n'est que d'imaginer les possibilités d'un opérateur mal intentionné pour perturber voire bloquer le fonctionnement du réseau à partir d'une entrée sur le réseau téléphonique commuté RTC accessible à 700 millions d'abonnés au moins de par le monde.

Par ailleurs l'administration des droits d'accès ne peut garantir l'exhaustivité et la cohérence des contrôles sur l'ensemble du Système d'Information si elle doit être gérée indépendamment sur chaque système avec des logiciels n'offrant pas des possibilités équivalentes. Le besoin se situe donc au niveau d'un système de sécurité global offrant une gestion distribuée des contrôles d'accès sur des machines et des systèmes hétérogènes.

Parades

En attendant la maturation des travaux engagés par les constructeurs informatiques participant à l'OSF (OPEN SOFTWARE FOUNDATION) et la disponibilité du modèle DCE (Distributed Computing Environment) dans tous les environnements informatiques, de MVS à OS/2, les réseaux doivent être mis sous haute surveillance.

L'architecture du réseau, généralement choisie par les Banques, banalise l'accès des terminaux, c'est-à-dire que tout terminal peut en principe atteindre toute application hébergée sur l'un des trois niveaux de machines : ordinateur central, machine départementale ou serveur de réseau local.

Les seules restrictions à ce principe d'ouverture sont introduites au niveau du paramétrage du réseau où les terminaux et applications candidats pour des communications inter-sites sont explicitement décrits dans des tables.

Cette protection étant bien sûr insuffisante, la Banque doit introduire le contrôle d'accès au niveau du réseau, dans la fonction accueil des terminaux, au travers d'un outil généralisé d'accueil dont la fonction première sera de garantir la convivialité des accès à plusieurs machines et plusieurs systèmes. Cet outil peut dans le même temps se voir confier le soin de contrôler l'identité des utilisateurs et leurs autorisations afin de leur présenter un menu personnalisé et de les diriger sûrement vers l'application de leur choix.

Dans un contexte homogène d'ordinateurs centraux IBM, cet outil assure d'une part le contrôle d'accès au niveau du réseau et d'autre part la cohérence entre les systèmes de sécurité RACF des différentes partitions système. Dans l'attente d'une extension de ses fonctionnalités au niveau de tout le réseau, systèmes départementaux et serveurs de réseaux locaux OS/2, une surveillance est nécessaire.

Critères de qualité

La mise sous surveillance du réseau peut être faite à partir de tableaux de bord.

Un suivi quotidien de l'activité du réseau doit pouvoir présenter une synthèse des principaux indicateurs. Par ailleurs des audits spécifiques peuvent être déclenchés afin de reconstituer un événement ou une succession d'événements, grâce à l'enregistrement systématique des connexions effectuées.

* *Surveillance du réseau interne*

  - Applications actives
  - Applications coopératives actives
  - Connexions inter-domaines

* *Surveillance des connexions partenaires*

  - Partenaires JES2
  - Partenaires CFT
  - Partenaires SNI
  - Sessions inter-réseau

La disponibilité d'un logiciel de sécurité logique contrôlant tous les accès d'un environnement distribué et hétérogène (constructeurs et systèmes d'exploitations différents) n'est pas encore annoncée malgré l'avance des travaux de l'O.S.F. Dans ce contexte, l'exploitation quotidienne de tableaux de bords des accès réseau permet de couvrir les risques spécifiques aux réseaux.

Fiche 33 : Sécurité incendie et dégâts des eaux

Définition

En termes de sinistres matériels, il s'agit là des principaux ennemis d'une salle informatique. De nombreux exemples de tels sinistres existent y compris ceux paraissant les plus improbables (par exemple inondations catastrophiques comme celles de Nîmes ...). Leur conséquence est la mise hors service définitive ou pour une longue durée des matériels touchés.

Concernant l'incendie, les dégâts provoqués aux équipements informatiques peuvent tenir aux effets directs du feu ou à des effets induits (fumées, suies). Plusieurs dizaines d'exemples de tels sinistres sont recensés chaque année. Parmi les causes les plus courantes d'incendie figurent les travaux à feu. Si les structures du bâtiment sont atteintes, celui-ci peut être indisponible pour une durée plus ou moins longue. La conséquence en est la mise en œuvre du plan de reprise des activités.

S'agissant des dégâts des eaux, ceux-ci peuvent provenir de débordements de cours d'eau, refoulement d'égouts, défauts d'étanchéité, ruptures de canalisation, etc.

Risques

Evidents !

Parades

La conception du bâtiment doit intégrer la sécurité incendie en termes de structures et de compartimentage, ceci afin de limiter l'étendue et les conséquences d'un sinistre. De plus, toute salle informatique devrait être dotée de systèmes de détection et d'extinction automatiques, reliés à un PC de surveillance. De préférence, les locaux adjacents doivent être également dotés au minimum de systèmes de détection automatique. Ces dispositifs se trouveront à la fois dans l'ambiance, les faux-plafonds et les faux-planchers. On insistera particulièrement sur les aspects de formation et sensibilisation du personnel au risque incendie. Les consignes de sécurité indiquant au personnel la conduite à tenir en cas d'alerte seront clairement affichées et régulièrement mises à jour. Des consignes d'exploitation spécifiques au risque incendie sont à rédiger et tester plusieurs fois par an. Il est utile de donner à l'ensemble du personnel une formation théorique et technique concernant le risque incendie. Des exercices d'alerte seront régulièrement organisés et leurs résultats analysés et commentés. Le risque de survenance de l'incendie peut être diminué en appliquant des règles simples telles que mise hors tension de certains appareillages électriques, interdiction de fumer en salle machine, usage de poubelles métalliques anti-feu. Il est utile de faire visiter le site par les pompiers qui auraient à intervenir en cas d'incendie et de faire contrôler les installations par des cabinets spécialisés. A cette occasion, il est bon d'indiquer aux pompiers les spécificités des matériels situés dans les zones visitées vis-à-vis des moyens d'intervention.

S'agissant des dégâts des eaux, l'implantation d'un site informatique doit tenir compte de ce type de risques et éviter en particulier la proximité des cours d'eaux. Il est souhaitable de disposer dans les faux-planchers de détecteurs adaptés. Un cuvelage et des pompes d'extraction permettront d'évacuer l'eau provenant de fuites ou de pertes d'étanchéité.

Critères de qualité

Il s'agit de suivre via un tableau de bord des indicateurs tels que :

- nombre de tests d'évacuation
- nombre de personnes formées aux consignes,
- conformité aux normes APSAD,
- rapport d'expert sur la qualité des équipements.

Fiche 34 : Suivi et contrôle des travaux d'exploitation

Définition

Les "travaux d'exploitation" consistent à exécuter un certain nombre d'applications informatiques (ensemble de programmes) sur un site informatique (salle d'ordinateurs).

Le traitement de ces applications est occasionnel ou permanent ; il met en jeux un certain nombre de données stockées, le plus souvent, sur des supports magnétiques (fichiers).

Chaque traitement est subordonné à des modalités d'exécution.

Lors de l'exécution d'une application, des incidents de traitement peuvent se produire.

Risques

- Sélection mal appropriée des travaux à exécuter (omission, erreur de périodicité, décalage horaire, etc.)
- Saturation ou surcharge de la machine pendant l'exécution des travaux
- Non exécution de travaux pourtant sélectionnés
- Non conformité des programmes et/ou des données (source erronée/déphasée, fichier altéré/manquant)
- Non conformité dans l'installation de nouveaux traitements (suite à une maintenance)
- Documentation inexistante, non adaptée (consignes en cas d'incident, traitement particulier, etc.)

Parades

Il faut planifier les travaux, donner les consignes de traitement et contrôler les résultats.

Il faut assurer au minimum :

- une surveillance de l'activité des machines (suivi de la bonne marche des machines),
- une surveillance de l'exécution des travaux (suivi de la bonne marche des travaux),
- une gestion des programmes et des fichiers (répertoire, contrôle, validation),
- une gestion des changements (modification des chaînes d'exploitation),
- une gestion des incidents de l'exploitation (historisation, remontée aux développeurs, correction).
- un contrôle de "bonne fin" des travaux.

Critères de qualité

Séparation stricte des ressources entre l'environnement "tests/études/développement" et l'exploitation.

Analyses périodiques des performances du système (répartition des fichiers, suivi des charges, temps de réponse, optimisation des ressources de l'exploitation, etc.).

Mise au point, suivi et analyse quotidienne du Journal des Opérations [ACCOUNTING] et des rapports d'activité des travaux [REPORTING].

Ordonnancement des travaux : établissement d'une liste chronologique de tous les travaux (manuelle et/ou automatique) en fonction de l'interdépendance des travaux (fichiers communs à plusieurs travaux).

Automatisation des chaînes d'exploitation (utilisation appropriée de robots, d'automates, etc.).

Documentation à l'usage des pupitreurs (appel au secours, conduite à tenir en cas d'incident, appel à la maintenance).

Documentation d'exploitation (procédures et consignes par application, hiérarchisée par fonction, mode dégradé et/ou éclaté, remise à jour périodique, stockée en lieu sûr avec copie à l'extérieur).

Contrôle de production (vérification de la qualité des travaux, conformité des résultats) en liaison avec les contrats de service (voir fiche n° 27) et les contrôles programmés (voir fiche n° 11).

Procédure et moyens de détection des incidents (contrôle des sources à l'arrivée, définition des travaux stratégiques, étalonnages périodiques, comparaisons des sources avant/après maintenances).

Procédure de correction/remise en l'état des supports en cas d'altération physique ou logique du support.

Procédures de recette des nouveaux travaux ou des maintenances sur travaux existants et gestion des versions de programmes.

Procédure de distribution des résultats (états hiérarchisés en fonction de la classification des documents).

Une amélioration de la qualité de l'exploitation se mesure également par une diminution des fins anormales de travaux et des réfections de travaux.

NB : POINT SENSIBLE

Fiche 35 : Système d'exploitation

Définition

Le système d'exploitation est un logiciel de base qui constitue le point d'entrée incontournable d'un système informatisé. Il est généralement fourni par les constructeurs, et son rôle est d'exécuter les fonctions essentielles de l'équipement :

- gestion des périphériques,
- exécution de programmes
- gestion des fichiers,
- communication

Il existe de nombreux systèmes d'exploitation qui se distinguent selon les familles d'équipements (grands, moyens, minis et micros systèmes) et selon leur compatibilité (systèmes propriétaires ou systèmes standards). Chaque famille d'équipements possède son système d'exploitation "propriétaire" ce qui peut rendre problématique la portabilité de ses applications.

Certains systèmes représentent un marché important et sont devenus des standards de fait. Mais contrairement à des systèmes standards réels, ils ne favorisent pas toujours l'intégration des normes et standards, ni l'interfaçage avec d'autres sous-systèmes.

La convergence d'intérêts des utilisateurs et des constructeurs favorise l'émergence de systèmes ouverts tel "UNIX" qui, selon les constructeurs, intègrent diversement les nouveaux standards :

- système de base : Posix, XPG... - les langages : C, C++... - les communications : X400, X500...

- l'informatique distribuée : ONC, DCE, NFS... - les moniteurs transactionnels : CICS, Tuxedo

Ces systèmes ouverts normalisés et standardisés répondent essentiellement au souci de portabilité des applications et à l'unification des compétences, mais la sécurité n'en est pas pour autant résolue.

Risques

Les grands et moyens équipements sont représentatifs des systèmes centralisés. Leurs systèmes d'exploitation sont anciens, plus fiables, plus complets et plus matures. En contrepartie de leur stabilité, ils souffrent de leur rigidité et de leurs difficultés à intégrer les nouvelles normes et nouveaux standards.

Les minis et micros ont des systèmes d'exploitation plus souples et plus ouverts qui favorisent la portabilité des applications. Mais ils sont très souvent victimes de leur jeunesse et donc de leurs imperfections (DOS : virus/intrusion/protection, UNIX : accès).

L'objectif est de réduire les risques de dégradation de la disponibilité, de l'intégrité et de la confidentialité du système d'information.

Les dysfonctionnements constituent les principaux facteurs d'indisponibilité : ils peuvent être dus soit à des erreurs du système soit à des paramétrages incorrects ou bien encore des intrusions incontrôlées. Ces interruptions intempestives peuvent être aggravées par une assistance imprévue ou incompétente, un contrat de maintenance inadapté, une pérennité médiocre du fournisseur.

Une parfaite maîtrise du système d'exploitation pourrait encourager à développer par soi-même des produits sophistiqués, alors que le "marché" offre des logiciels dont les fonctions sont approchantes. Il existe des avantages et des inconvénients pour chacune des solutions. Une étude approfondie, assortie de conseils précieux de la part des spécialistes systèmes, permet de choisir l'option la plus efficace pour l'entreprise.

Les accès logiques non maîtrisés constituent, quant à eux, le facteur de risque essentiel susceptible de dégrader l'intégrité et la confidentialité d'un système d'information. En cela ils facilitent les intrusions, les malveillances, ils ne protègent pas des erreurs de manipulations, des interventions non-autorisées...

Un système d'exploitation qui ne facilite pas l'identification et les contrôles fonctionnels (autorisation, habilitation, permission) fait courir un risque grave au système d'information.

Parades

Il est recommandé de rechercher un système d'exploitation bien diffusé, opérationnel, incluant des standards qui garantissent la portabilité et les communications.

Les informations de classification de type "orange book" ou "ITSEC" peuvent apporter des réponses au niveau de sécurité d'un système d'exploitation. Il faut demander au fournisseur quel est le niveau de sécurité atteint par son produit. Possède-t-il la certification ISO 9001 ?

Si le produit ne possède pas toutes les fonctionnalités requises, d'autres produits complémentaires peuvent être mis en œuvre pour y remédier : contrôles d'accès, chiffrement, audit, habilitations, etc. Un système de grande diffusion peut vous ouvrir un marché très diversifié de progiciels, sinon vous devrez les développer en interne.

Vous devez souscrire un contrat de maintenance adapté au niveau de disponibilité souhaité. Il vous garantira en outre, des interventions dans les délais, le suivi des évolutions systèmes et l'assistance à l'exploitation.

Une fonction technique doit être définie en interne ou en externe pour assister le fonctionnement. Les interventions dans le système devront être préparées, testées et validées (gestion des changements).

Assurez-vous de la qualité de la formation et de la documentation, c'est la garantie de votre autonomie d'exploitation.

Le système d'exploitation doit comporter des fonctionnalités particulières en matière d'accès pour :

- identifier et authentifier les personnes,
- limiter et contrôler les accès et interventions dans le système,
- séparer les fonctions de production, de développement et de système,
- limiter et contrôler les accès aux programmes, aux procédures, aux fichiers et aux données,
- tracer les différents accès exceptionnels.

Des outils et des procédures doivent limiter et contrôler les accès au système d'exploitation.

Le système d'exploitation doit permettre de réaliser et de gérer efficacement les sauvegardes.

La journalisation ou la comptabilisation des travaux sont utiles pour suivre l'activité globale et reconstituer un enchaînement de travaux.

Un audit périodique du système d'exploitation est une solution efficace pour s'assurer de la qualité de son fonctionnement.

Critères de qualité

Une fonction spécifique a été définie pour suivre l'évolution du système, la métrologie, les accès, les incidents, la maintenance.

Un tableau de bord qualifie le fonctionnement du système d'exploitation : taux de disponibilité, performances, délai moyen d'intervention...

Un outil de suivi permet de connaître toutes les interventions et tous les changements à caractère "protégé" opérés sur le système d'exploitation.

Un audit des systèmes d'exploitation est réalisé périodiquement.

Une partie du contrôle interne rapporte annuellement le fonctionnement du système.

NB : POINT SENSIBLE

Fiche 36 : Télémaintenance

Définition

La télémaintenance consiste à exécuter une intervention à distance sur un système informatique.

Cette intervention peut être de nature :

- préventive (tests de fonctionnement, analyses, mise à niveau de logiciels systèmes ou applicatifs, modifications planifiées),
- curative (télédiagnostic de pannes, modifications impromptues de programmes ou de données...).

Elle peut porter sur :

- le matériel (tests et télédiagnostic),
- les logiciels de base,
- les applications et leurs données.

Elle peut être effectuée par :

- un fournisseur de matériel ou de logiciel,
- une société spécialisée dans la maintenance,
- une équipe déportée.

Les avantages suivants sont généralement attendus :

- réduire les délais d'intervention,
- disposer de spécialistes à tout moment,
- diminuer les coûts en supprimant les frais de déplacement,
- supprimer l'accès physique aux locaux informatiques.

Risques

Les risques sont ceux induits par l'accès au système informatique de l'entreprise par des intervenants externes, généralement de haut niveau technique, dotés par nécessité de privilèges importants, et dont l'activité est difficilement contrôlable :

- Perte de confidentialité : le télémainteneur peut avoir accès, volontairement ou accidentellement, à la totalité des informations stockées sur le système.

- Perte d'intégrité : modification ou destruction, volontaire ou accidentelle, de données ou de programmes accédés par le télémainteneur.

- Fraudes, sabotages : mise en place de programmes "cheval de Troie", "bombe logique" ou "virus".

- Modification des contrôles d'accès (identifiants, mots de passe, privilèges) facilitant les intrusions ultérieures.

- Vol de temps machine à des fins personnelles.

Par ailleurs, l'accès au système ouvert pour les besoins de la télémaintenance peut être utilisé par des pirates informatiques, avec les mêmes conséquences que ci-dessus.

Parades

Éviter le recours à la télémaintenance dans toute la mesure du possible.

Toutefois, si les avantages l'emportent sur les risques énumérés ci-dessus, prendre les mesures suivantes :

- Ne laisser le télémainteneur accéder au système qu'à travers un environnement réseau sécurisé (ligne privée, GFA, contre-appel...).

- Mettre en place un contrôle d'accès ; n'attribuer l'identifiant et le mot de passe qu'au coup par coup et limiter sa validité à la durée de l'intervention ; ne donner que les privilèges strictement nécessaires pour l'intervention prévue.

- Définir formellement (contractuellement s'il s'agit d'un prestataire externe) la procédure d'intervention.

- Enregistrer (dans un fichier journal) toutes les manipulations effectuées par le mainteneur ; lui interdire l'accès au fichier journal.

- Si l'état du système le permet, effectuer une sauvegarde complète avant le début de l'intervention de télémaintenance.

- Prononcer une recette après chaque intervention ; vérifier entre autres que le nombre et la taille des fichiers et programmes non concernés n'ont pas été modifiés.

Critères de qualité

- Ne jamais laisser en service les numéros de compte standard des constructeurs installés à l'initialisation du système ; les renommer en cas de besoin de réutilisation.
- N'accorder les privilèges d'accès maximum que si la nécessité en est dûment justifiée.
- Ne jamais laisser en fonctionnement un modem accessible par un réseau public.
- Chiffrer les données confidentielles.
- Désigner un responsable de la sécurité du système.
- Exploiter les fichiers journaux (logs).
- Tenir un journal de bord des interventions.

ANNEXE V

Les risques, les facteurs de sécurité et les méthodes d'analyse du risque (un exemple)

(Autres méthodes : MARION, MELISA, CRAMM, BUDDY...)

LES RISQUES ET LES FACTEURS DE SÉCURITÉ

Introduction

L'un des problèmes de la politique de sécurité d'un système d'information est le caractère très aléatoire du risque informatique, qui se présente comme la composante d'éléments négatifs, non prévus par les concepteurs et dont ils n'ont souvent pas l'initiative.

On peut faire la même observation dans de nombreux cas d'innovation technique, comme, par exemple, celui des moyens de transport qui sont apparus depuis le siècle dernier : les transports maritimes, le chemin de fer, l'aviation, l'automobile. On vise tout d'abord un objectif valable, une "bonne cause", qui représente un progrès ; les effets pervers n'apparaissent que dans un deuxième temps, plus ou moins provoqués et plus ou moins graves : accidents, anomalies de fonctionnement, mais aussi actions délictueuses, le nouveau domaine se trouvant également ouvert aux "mauvaises causes".

Il ne faudrait pas en conclure que le risque informatique est le prix à payer pour profiter d'une certaine forme de progrès. L'application, à bon escient, de mesures répondant aux besoins de sécurité à un prix acceptable, peut garantir un fonctionnement satisfaisant du système d'information.

À cet égard, on observe diverses attitudes face au risque informatique, le plus souvent de façon chronologique :

- L'ignorance ou la contestation de la notion même de risque informatique est la plus mauvaise.
- Sa reconnaissance est généralement suivie de l'application de mesures de sécurité globales (mise en place d'un progiciel de contrôle des accès, chiffrement systématique des échanges) qui rassurent les responsables, mais qui ont peu de chance d'être efficaces, faute d'une analyse préalable.
- Une attitude plus responsable consiste à appliquer les mesures de sécurité en fonction de risques identifiés.
- L'évaluation du coût des mesures de sécurité, comparé à celui des risques, justifie leur application et complète la démarche idéale.

En se basant sur les travaux des experts de la sécurité des systèmes d'information, il est possible d'aborder le risque informatique, phénomène aléatoire, selon une démarche précise et de définir des mesures de sécurité adaptées, en fonction des facteurs de sécurité : disponibilité, intégrité, confidentialité et preuve.

1. LES PRINCIPES DE BASE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

Les risques d'un système d'information résultent des menaces qui pèsent sur ses éléments. Ils illustrent sous forme négative, un état de sécurité : tel système d'information a un niveau de risques égal à X ; pour améliorer sa sécurité, on s'efforcera d'abaisser ce niveau.

1.1. LES MENACES

Les menaces sont, soit passives (sinistres, incidents, erreurs), soit actives (indiscrétion, fraude, sabotage, etc). Leur origine se situe aussi bien à l'intérieur qu'à l'extérieur de l'entreprise. Toutefois, notamment dans les cas d'actes de malveillance, les motivations et les moyens d'action sont souvent plus forts pour le personnel de l'entreprise que pour les utilisateurs externes (qui, d'ailleurs, assez souvent, arrivent à bénéficier de complicités internes).

Cette constatation s'applique aux banques et, en général, aux services ; elle est moins vraie pour la Défense Nationale, l'industrie et le secteur médical.

1.2. LES MESURES DE SECURITE

On abaisse le niveau des risques par l'application de mesures de sécurité adaptées à chacun d'eux. Afin de refléter le plus exactement possible le niveau de sécurité d'un système d'information à un moment donné, l'analyse des risques inclut celles des mesures de sécurité déjà mises en place.

1.3. LA PROBABILITE ET L'IMPACT DES RISQUES

Les risques représentent la probabilité d'une menace portant atteinte à l'un des éléments du système d'information (dit "élément vulnérable"), avec un impact variable. On peut les classer grossièrement en trois catégories, en fonction de leur impact : faibles risques, risques courants et risques maximaux.

1.3.1. Faibles risques

Les faibles risques se manifestent sous forme d'erreurs de saisie, de micro-coupures d'alimentation, etc. Ils s'intègrent à la gestion courante, dans la mesure où toute activité s'accompagne d'un minimum de risques, et n'exigent que des mesures simples : vérification de la saisie, procédures automatiques de reprise.

1.3.2. Risques courants (ou "moyens")

Les risques courants ont un impact moyen : perte d'un fichier, arrêt prolongé de la production, accès indu aux données, répudiation d'un virement émis par télétransmission, etc. Ils peuvent entraîner des préjudices graves ou des pertes financières importantes, mais ils sont clairement identifiés, et l'on s'en protège par des mesures de sécurité standard : plan de sauvegarde, plan de secours, mise en place d'un contrôle des accès, signature des échanges.

1.3.3. Risques maximaux (ou "élevés")

Les risques maximaux ont un impact fort : destruction d'un centre d'exploitation, en l'absence d'un plan de sauvegarde et de secours, sabotage "immatériel" des données ou des programmes, etc.

Alors que la probabilité des faibles risques et des risques courants est variable, celle des risques maximaux ne peut être que faible car la survie d'une entreprise subissant des risques élevés avec une probabilité moyenne ou forte serait compromise à court terme : risque d'incendie d'un site informatique, plusieurs fois par an, par exemple.

Leur gestion est plus délicate car, bien souvent, ils ne sont jamais concrétisés au sein de l'entreprise et il est difficile de les faire admettre, surtout par les décideurs qui doivent investir parfois lourdement pour ne parer qu'à des éventualités. La comparaison avec des cas similaires, qui se sont produits dans le même secteur d'activité, et l'analyse les conséquences d'incidents qui se produiraient dans l'entreprise, constituent généralement de bons moyens de sensibilisation.

1.4. LES CIBLES DES RISQUES

Les risques varient en fonction de la nature des composants du système d'information et des menaces provenant de l'environnement.

Tel site exposé à la vue du public, et donc susceptible de subir des attaques directes, ou bien construit dans une région inondable ou volcanique, présente un niveau de risques plus élevé que tel autre, situé au sous-sol d'un immeuble construit sur un terrain sec et stable.

La micro-informatique et la télématique présentent des risques spécifiques.

1.4.1. Les risques de la micro-informatique

Les applications traitées sur micro-ordinateurs sont souvent gérées par un personnel manquant de qualification. Elles sont particulièrement exposées aux virus, en raison du caractère très ouvert des systèmes d'exploitation, et par l'intense circulation des disquettes dans le public.

1.4.2. Les risques des réseaux

Les réseaux de télétransmission, qui constituent un puissant moyen de communication, permettent l'accès aux systèmes d'information d'utilisateurs éloignés et invisibles. On les compare parfois à des glaces sans tain. Ils doivent être protégés de façon à identifier à coup sûr les correspondants et éviter les accès des personnes non autorisées. Leur interruption peut perturber l'activité de nombreux utilisateurs. Les échanges très rapides qu'ils permettent peuvent accélérer un processus d'anomalie, notamment dans les applications d'échanges financiers, et provoquer une succession d'incidents avant que l'on constate l'erreur.

1.5. LE DOMAINE D'APPLICATION DE LA POLITIQUE DE SECURITE

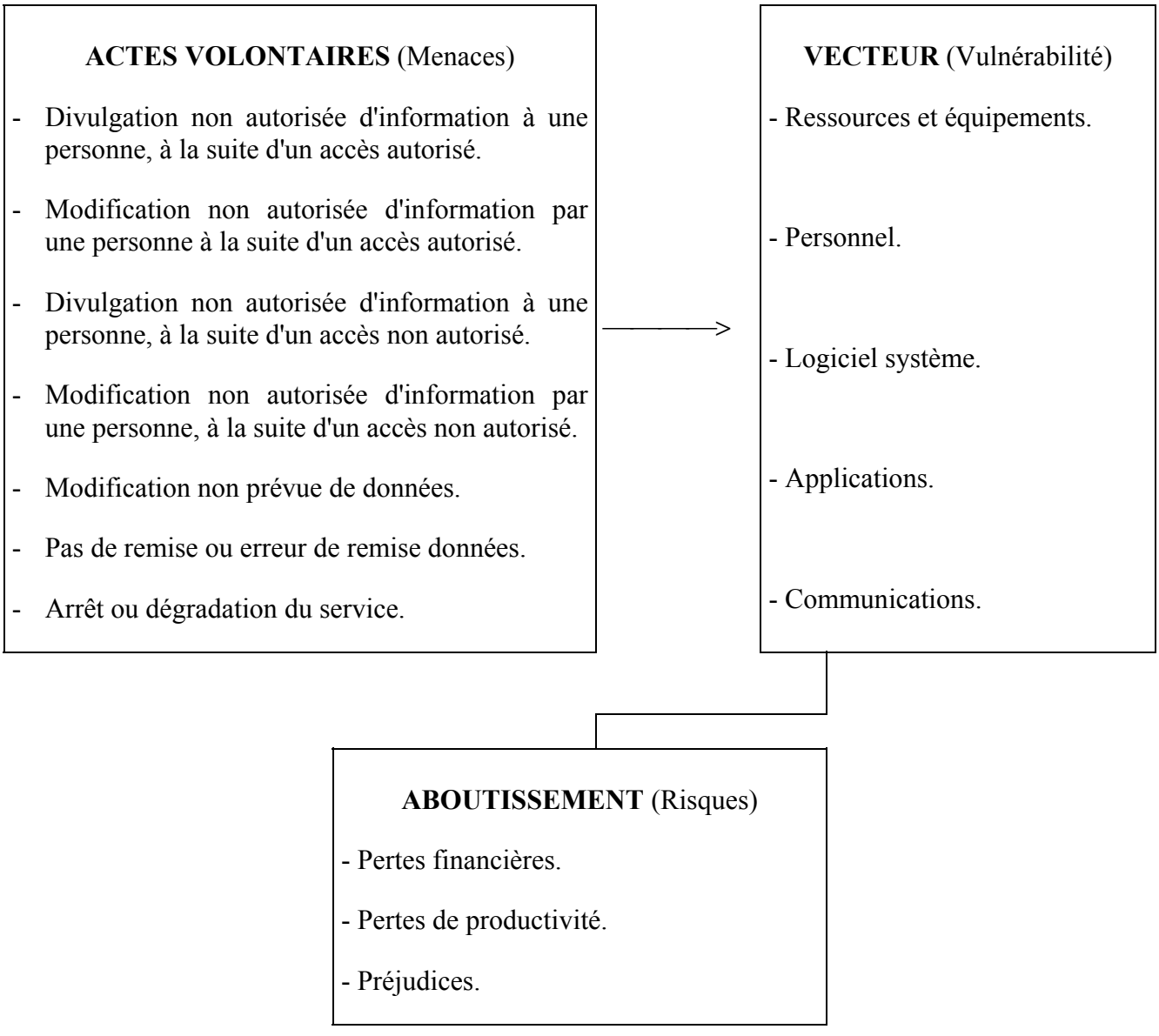
Le risque informatique concerne directement les composants du système d'information, considéré, au sens étroit, comme l'ensemble des traitements et des données auxquels on ajoute, pour le définir au sens large, les documents sur papier, les informations orales et les procédures manuelles. Il résulte également, de façon indirecte, de menaces portant atteinte à l'environnement du système d'information : le matériel informatique, les supports, les installations techniques (alimentation électrique, climatisation), les locaux, les immeubles, et encore, l'organisation, les méthodes, le personnel.

En matière de gestion de la sécurité des systèmes d'information, il existe donc également un besoin de sécurité, au niveau de cet environnement, et de cohérence des mesures. Il importe, par exemple, de prendre des mesures de sécurité de niveaux comparables pour assurer l'intégrité d'une certaine information, quelle que soit la forme ou sa situation : sur un document d'entrée ou de sortie, sur disquette, sur bande, sur disque, en mémoire centrale, etc. Et la première mesure à prendre, pour assurer cette cohérence, est la création d'une fonction administration de la sécurité. C'est-à-dire la désignation d'un responsable de la sécurité des systèmes d'information (RSSI) qui mettra en œuvre la politique de sécurité décidée, sous forme de schéma directeur de la sécurité (SDSSI), traduite, ensuite en plan sécurité.

2. EXEMPLE DE MÉTHODE D'ANALYSE DU RISQUE

2.1. DEFINITIONS

Objectif : Définir les mesures de sécurité, applicables à un secteur d'activité, qui peuvent réduire le niveau de risques résultant des menaces, sources des vulnérabilités du système d'information.



2.1.1. Analyse des risques

Il y a beaucoup de méthodologies d'évaluation du risque. Cependant, elles ont toutes en commun une définition des risques basée sur le jugement et sur la responsabilisation de la Direction.

En analysant une application d'après une liste de facteurs de risque, le responsable de la sécurité peut déterminer l'ampleur des mesures de sécurité à appliquer. Mais, en dernier lieu, c'est la Direction générale qui doit déterminer le niveau de risque qu'elle est décidée à assumer.

La méthodologie exposée ci-dessous vise à aider la Direction et le RSSI à évaluer les vulnérabilités et les niveaux de risques d'une application. A partir de cette évaluation, l'analyse des risques fera apparaître les vulnérabilités et les mesures de sécurité correspondantes pour assurer la continuité du service et pour atteindre un niveau acceptable de sécurité et d'intégrité de l'information.

Le RSSI doit évaluer chaque application d'après les facteurs de risques. L'évaluation doit prendre en compte à la fois la possibilité qu'un événement se produise et l'impact de cet événement sur les traitements. Par exemple, l'activité quotidienne d'un service peut dépendre de la bonne fin d'un programme. L'évaluation des risques devra considérer à la fois la possibilité que le programme ne se déroule pas normalement (pour cause de sabotage, panne système, erreur de programme...) et le résultat du déroulement anormal du programme (retard de production, frais financiers, baisse de qualité...).

Pour compléter une telle évaluation, le RSSI (ou la Direction opérationnelle) doit aussi identifier au sein de la Direction opérationnelle analysée les correspondants (personnes, services, organismes) avec lesquels elle échange des informations. Certaines applications peuvent être en relation avec plusieurs secteurs. D'autres n'ont que la Direction elle-même comme seule bénéficiaire. Par exemple, le service des Transferts de fonds peut avoir plusieurs correspondants (les banques centrales, les établissements de crédit et leurs clients, le service de comptabilité), alors que, par exemple, l'application du service chargé du suivi des dépenses n'aura qu'un impact limité à l'extérieur. Pour déterminer le niveau de risque acceptable dans une application, la Direction opérationnelle doit identifier qui lui fournit des informations et qui utilise ses résultats (les sous-systèmes d'informations et "bases-relais" peuvent être déterminées ainsi que leurs liens réciproques).

2.1.2. Les trois catégories de risques

Il y a trois catégories principales de risques à considérer dans une évaluation de risque.

- La perte financière

  Dans une banque, les pertes financières sont communément définies comme des pertes de valeurs (encaisse, réserves, fonds). En ce qui concerne l'évaluation de risque d'une application, cette définition doit inclure d'autres formes de pertes telles que le vol, les litiges judiciaires, les revenus de service facturés, etc... En général, le risque de perte financière augmente aussi bien en fonction du montant des pertes réelles qu'en fonction des pertes potentielles. Plus le risque de pertes financières réelles ou potentielles est élevé, plus l'application sera sensible.

- La perte de productivité

  Les pertes de productivité se produisent quand le personnel ne peut pas exécuter les travaux ou lorsqu'il doit les reprendre. Cela peut se produire lorsque les applications sont indisponibles ou lorsqu'elles fournissent des résultats erronés.

- Les préjudices causés à l'établissement

  Ce dernier facteur concerne les risques pouvant entraîner des préjudices indirects à l'établissement (par exemple : des situations dans lesquelles la réputation de la banque auprès du public peut être affectée).

2.1.3. Les cinq domaines de vulnérabilité

Avant d'évaluer le niveau de risque d'une application ou d'un système, il est bon d'en connaître les domaines de vulnérabilité. Une architecture de sécurité distingue typiquement cinq catégories de vulnérabilité dans l'organisation d'une banque et identifie les mesures de sécurité correspondantes.

Par exemple, il est évident que la sécurité des transferts de fonds doit être d'un niveau plus élevé que celle d'un message administratif. La sécurité est nécessaire dans les deux cas ; tout réside, cependant, dans le niveau des mesures de sécurité mises en œuvre.

2.1.4. Processus d'évaluation de risques

Le Direction opérationnelle doit considérer soigneusement chacune des trois catégories de risques en relation avec les cinq domaines de vulnérabilité. Par exemple, le risque de perte financière due au personnel peut être relativement faible, mais le risque de préjudice dû à l'erreur d'un logiciel d'application peut être relativement élevé. Les catégories de risques et les domaines de vulnérabilité s'entendront de différentes façon selon les applications.

2.1.5. Choix des mesures de sécurité

L'étape suivante du processus d'évaluation de risques consiste à choisir les mesures de sécurité appropriées pour protéger les données des menaces, causes des vulnérabilités. La Table d'Evaluation des Risques est conçue pour évaluer les différents niveaux de risque d'une application. Pour une catégorie de risques et un domaine de vulnérabilité donnés, on évalue le niveau de risque au moyen de trois notes : "faible", "moyen" ou "élevé". La Table d'Evaluation des Risques réalisée, on détermine, ensuite, un niveau de risque général de chaque domaine de vulnérabilité en utilisant les mêmes notes.

Le niveau de risque général de chacun des cinq domaines de vulnérabilité est alors pris en compte pour apprécier les mesures de sécurité à appliquer.

En général, il n'est pas possible d'appliquer toutes les mesures indiquées dans la table. Le RSSI ou la Direction générale doit les passer en revue et choisir celles qui conviennent à l'application.

2.2. ÉTAPES

Étapes de l'analyse de risques

- Identifier les **correspondants** spécialistes de chaque secteur avec lesquels on se trouve en relation, au niveau des entrées, du traitement ou des sorties.

- Pour un type de menace et un domaine de vulnérabilité donnés, poser les questions :

  - Comment cela peut-il se produire ?
  - Quand cela peut-il se produire ?
  - Qui peut le faire ?
  - Quelles en sont les conséquences ?

  Sur cette base, évaluer les risques de chaque domaine de vulnérabilité (table 1) qui sont les matériels, le personnel, le logiciel système, les applications et inscrire les résultats sur le formulaire. Les "Eléments à prendre en considération pour l'évaluation des risques liés aux vulnérabilités" (table 2) peuvent aider à faire cette évaluation.

- Pour chaque catégorie de risque, attribuer une note ("élevé", à "moyen" ou "faible"), à chaque domaine de vulnérabilité dans la Table d'Evaluation des Risques (table 3). Les réponses inscrites sur le formulaire d'évaluation peuvent aider à l'attribution du niveau de risque. Entrez "élevé" si les risques sont significatifs. Entrez "moyen" si le risque est limité. Entrez "faible" si le risque est nul ou peu important. S'il y a un doute entre "faible" et "moyen", entrez "moyen". S'il y a un doute entre "moyen" et "élevé", entrez "élevé"[44].

- Après avoir noté chaque risque "élevé", "moyen" ou "faible", pour un domaine de vulnérabilité, attribuer une note globale. Procéder avec soin pour déduire cette note des trois notes attribuées par catégorie de risque.

- En se basant sur la note générale de chaque domaine de vulnérabilité, se reporter aux tables des mesures de sécurité (tables 4 et 5) et appliquer toutes les mesures de niveau égal ou inférieur à celle qui s'appliquent à ce domaine ;

- si le risque pour un domaine de vulnérabilité est "faible", appliquez les mesures correspondantes à la note "faible" ;

- si le risque pour un domaine de vulnérabilité est "moyen", appliquez les mesures correspondantes aux notes "moyen" et "faible" ;

- si le risque pour un domaine de vulnérabilité est "élevé", appliquez les mesures correspondantes aux notes "élevé", "moyen" et "faible".

44 Il s'agit ici d'une échelle de risque simplifiée, à trois niveaux.

Table 1
Évaluation des risques
(consiste à valoriser en risques "élevés", "moyens" ou "faibles", les cinq domaines de vulnérabilité)

Matériels	Pertes financières	Pertes de productivité	Préjudices
Divulgation non autorisée d'information à la suite d'un accès autorisé	E M F	E M F	E M F
Modification non autorisée d'information à la suite d'un accès autorisé	E M F	E M F	E M F
Divulgation non autorisée d'information à la suite d'un accès non autorisé	E M F	E M F	E M F
Modification non autorisée d'information à la suite d'un accès non autorisé	E M F	E M F	E M F
Pas de remise ou erreur de remise	E M F	E M F	E M F
Arrêt ou dégradation du service	E M F	E M F	E M F

Personnel)
Logiciel/Système)
Applications) mêmes matrices
Communications)

Table 2
Éléments à prendre en considération pour l'évaluation des risques liés aux vulnérabilités

Insertion de messages au moyen d'écoutes téléphoniques
Modification de messages au moyen d'écoutes téléphoniques
Écoute indiscrète
Rayonnement électronique
Indiscrétion visuelle
Accès télématique aux ressources d'automation et de communication
Utilisation non autorisée de terminaux
Erreurs de transmission
Moyens disponibles sur la console de l'opérateur
Moniteurs de communication et équipement de diagnostic
Conception et développement des logiciels d'application
Maintenance des logiciels d'application
Maintenance du logiciel système
Changement de logiciels
Interfaces logiciels pendant les changements de système
Panne de logiciel système
Panne de logiciel applicatif
Données de production
Programmes source et données associées
Librairies système
Temps partagé
Langage de requête
Utilitaires de maintenance et de diagnostic
Langages et ressources de la gestion des données
Ressources de conduite de performances
Connaissance de la sécurité et sensibilisation
Standards de sécurité et contrôles
Procédures d'entrée des transactions
Coupure et surveillance des terminaux
Cas d'opérations anormales
Fin d'activité d'un employé
Turnover du personnel
Conflit dans le personnel
Erreur d'utilitaire
Erreur de liaison télécom
Catastrophe naturelle ou d'origine humaine
Laisser traîner les listings
Divulguer des données anciennes
Ne pas conserver de données anciennes

Table 3
Table d'évaluation des risques (récapitulation)
Vulnérabilité par domaines

Catégories de risques	Ressources et équipements	Personnel	Logiciel système	Applications	Communications
Pertes financières					
Pertes de productivité					
Préjudices					
RISQUES GLOBAUX					

Pour chaque catégorie de risques, entrez le niveau de risques correspondant à chaque domaine de vulnérabilité. Les niveaux de risques doivent être évalués selon l'échelle : "faible", "moyen" ou "élevé". Après avoir évalué chaque catégorie de risques, attribuez un niveau global de risque à chaque domaine de vulnérabilité.

Table 4
Architecture de sécurité
Classification des mesures de sécurité

1. Domaine de vulnérabilité : ressources et équipements

Mesures de sécurité à appliquer	Domaine de risque élevé
	1.1. Revue du journal de la console
	1.2. Contrôle de l'opérateur de la console
	1.3. Commandes système de journalisation
Plus "moyen"	1.4. Mise à jour du planning des changements
	1.5. Emploi restrictif des fonctions réseau de la console
Plus "faible"	1.6. Back up du matériel et des lignes de communication
	1.7. Back up de l'énergie électrique
Mesures de sécurité à appliquer	Domaine de risque moyen
	1.8. Accords de sécurité avec les fournisseurs
	1.9. Problèmes de rapports et de traces
	1.10. Mise à jour de la documentation du système
Plus "faible"	1.11. Contrôle des accès aux circuits de télécommunication
	1.12. Etablissement de plans de maintenance préventive
	1.13. Vérification des contrôleurs de matériel
	1.14. Collecte de statistiques d'utilisation
	1.15. Protection des accès physiques aux terminaux
Mesures de sécurité à appliquer	Domaine de risque faible
	1.16. Compte-rendu des tentatives de violation des mesures de sécurité
	1.17. Contrôle non autorisé / Accès du personnel des sociétés de service

2. Domaine de vulnérabilité : personnel

Mesures de sécurité à appliquer	Domaine de risque élevé 2.1. Mise à jour de la documentation du planning 2.2. Risques d'accès aux informations classifiées par lecture ou par captage de conversation
Plus "moyen"	2.3. Examen de la personnalité des employés 2.4. Travail en double dans l'exercice de fonctions sensibles
Plus "faible"	2.5. Séparation appropriée des fonctions 2.6. Rotation des fonctions
Mesures de sécurité à appliquer	Domaine du risque moyen 2.7. Nomination d'un administrateur de sécurité du secteur 2.8. Compte-rendu des tentatives de violation des mesures de sécurité
Plus "faible"	2.9. Protection des rapports classifiés 2.10. Sécurisation des lieux de travail en fin de journée 2.11. Back up approprié
Mesures de sécurité à appliquer	Domaine de risque faible 2.12. Politique en matière de sécurité et de secret 2.13. Droits d'accès - Classification des informations 2.14. Compte-rendu des tentatives de violation des mesures de sécurité 2.15. Domaines d'audit 2.16. Gestion des mots de passe 2.17. Employés en fin de carrière en position sensible 2.18. Responsables de formation 2.19. Formation à la sécurité 2.20. Formation aux travaux de sécurité

3. Domaine de vulnérabilité : logiciel système

Mesures de sécurité à appliquer	Domaine de risque élevé 3.1. Intégrité du système d'exploitation 3.2. Back up des données, des logiciels et des procédures
Plus "moyen"	3.3. Violation du système d'interruption, de journalisation et d'alarme
Plus "faible"	3.4. Protection des objets sensibles 3.5. Programmes et ressources de contrôle et de diagnostic

Mesures de sécurité à appliquer	Domaine de risque moyen 3.6. Accords de sécurité avec les fournisseurs 3.7. Problèmes de rapports et de traces 3.8. Revue des dispositifs de sécurité des logiciels système
Plus "faible"	3.9. Participation de l'Audit dans le développement du système 3.10. Contrôle de la librairie des programmes et des procédures 3.11. Procédures de test des logiciels système 3.12. Procédures de modification des logiciels de secours 3.13. Administration des bases de données 3.14. Restauration et reprise du logiciel système 3.15. Synchronisation restauration / reprise 3.16. Restauration de données 3.17. Utilisation des possibilités de suivi du système 3.18. Conservation des statistiques de trafic des messages 3.19. Ressources de contrôle d'accès globaux 3.20. Identification et authentification des utilisateurs 3.21. Gestion des identifiants et des mots de passe des utilisateurs 3.22. Compte-rendu des tentatives d'accès non autorisées 3.23. Erreur de journalisation
Mesures de sécurité à appliquer	Domaine de risque faible 3.24. Compte-rendu des tentatives de violation des mesures de sécurité 3.25. Mise à jour de la documentation du système 3.26. Dumps de vérification 3.27. Changement de la table de sécurité du journal

4. Domaine de vulnérabilité : applications

Mesures de sécurité à appliquer	Domaine de risque élevé 4.1. Codes d'authentification de message ANSI 4.2. Reconnaissance de bout en bout
Plus "moyen"	4.3. Sécurisation de la documentation du logiciel
Plus "faible"	4.4. Vérification des procédures de restauration et de reprise du logiciel 4.5. Modifications 4.6. Back up des données, des logiciels et des procédures 4.7. Mise à jour du planning des changements

Mesures de sécurité à appliquer

Plus "faible"

Domaine de risque moyen

4.8. Accords de sécurité avec les fournisseurs
4.9. Problèmes de rapports et de traces
4.10. Participation de l'Audit dans le développement du système
4.11. Journalisation complète des transactions
4.12. Documentation du traitement des cas exceptionnels
4.13. Contrôle du transfert manuel des données
4.14. Procédures de test des applications
4.15. Environnement dédié au test des logiciels
4.16. Procédures de contrôle et de mise en œuvre des changements
4.17. Procédures de modification des logiciels de secours
4.18. Edition
4.19. Restauration des données
4.20. Ressources de contrôle des accès globaux

Mesures de sécurité à appliquer

Domaine de risque faible

4.21. Compte-rendu des tentatives de violation des mesures de sécurité
4.22. Standards de documentation
4.23. Manuels condensés et développés
4.24. Procédures écrites de back up et de reprise

5. Domaine de vulnérabilité : communications

Mesures de sécurité à appliquer

Plus "moyen"

Plus "faible"

Domaine de risque élevé

5.1. Vérification des appels téléphoniques
5.2. Identification des messages
5.3. Accusés de réception de bas niveau
5.4. Réconciliation de messages
5.5. Sécurité de la documentation des logiciels
5.6. Back up des données, des logiciels et des procédures
5.7. Mise à jour du planning des changements
5.8. Chiffrement
5.9. Utilisation de chiffrage des ANSI
5.10. Gestion des clés
5.11. Traitement des aléas et des exceptions
5.12. Groupes fermés d'utilisateurs
5.13. Logiciel de relancement des lignes tombées
5.14. Relation entre les identifiants d'utilisateurs et les terminaux
5.15. Back up du matériel et des lignes de communication
5.16. Chute en cascade du réseau

Mesures de sécurité à appliquer Plus "faible"	<u>Domaine de risque moyen</u> 5.17. Problèmes de rapports et de traces 5.18. Participation de l'Audit dans le développement du système 5.19. Etablissement d'un contrôle au point d'entrée 5.20. Etablissement de l'authenticité des données de base 5.21. Documentation du traitement des cas exceptionnels 5.22. Authentification des données 5.23. Authentification des messages 5.24. Sécurité des appels entrants 5.25. Mise à jour de la documentation du système 5.26. Procédures de modification des logiciels de secours 5.27. Restauration des données 5.28. Déconnexion automatique des utilisateurs
Mesures de sécurité à appliquer	<u>Domaine de risque faible</u> 5.29. Compte-rendu des tentatives de violation des mesures de sécurité

Table 5
Table des mesures de sécurité de l'information
Vulnérabilités

Classification des risques	Ressources et équipements	Personnel	Logiciel système	Applications	Communications
ÉLEVÉ Mesures énumérées plus celles de niveaux inférieurs	1.1 1.2 1.3 1.4 1.5 1.6 1.7	2.1 2.2 2.3 2.4 2.5 2.6	3.1 3.2 3.3 3.4 3.5	4.1 4.2 4.3 4.4 4.5 4.6 4.7	5.1 5.8 5.15 5.2 5.9 5.16 5.3 5.10 5.4 5.11 5.5 5.12 5.6 5.13 5.7 5.14
MOYEN Mesures énumérées plus celles de niveaux inférieurs	1.8 1.15 1.9 1.10 1.11 1.12 1.13 1.14	2.7 2.8 2.9 2.10 2.11	3.6 3.13 3.20 3.7 3.14 3.21 3.8 3.15 3.22 3.9 3.16 3.23 3.10 3.17 3.11 3.18 3.12 3.19	4.8 4.15 4.9 4.16 4.10 4.17 4.11 4.18 4.12 4.19 4.13 4.20 4.14	5.17 5.24 5.18 5.25 5.19 5.26 5.20 5.27 5.21 5.28 5.22 5.23
FAIBLE Mesures énumérées	1.16 1.17	2.12 2.19 2.13 2.20 2.14 2.15 2.16 2.17 2.18	3.24 3.25 3.26 3.27	4.21 4.22 4.23 4.24	5.29

Cette grille est destinée à aider les banques dans la mise en œuvre des mesure de sécurité.

ANNEXE VI

La prise en compte de la sécurité dans les applications

- Méthode décrite : ISM[45]

- Autres méthodes possibles : INCAS, MESSIE (cf. ANNEXE IX)

45 ISM : Intégration de la Sécurité dans MELODIC (MELODIC étant la méthode utilisée par la BANQUE DE FRANCE, proche de MERISE +)

EXEMPLE DE PRISE EN COMPTE DE LA SÉCURITÉ
DANS LES DIFFERENTES PHASES DE CONDUITE DES PROJETS INFORMATIQUES

PHASES DE CONCEPTION
Analyse de risques - Etude de mesures - Bilan économique sécurité

LANCEMENT DU PROJET
Identification des éléments stratégiques

ÉTUDE PRÉALABLE
Analyse des risques
Etude des mesures de sécurité
Proposition de **solutions sécurisées**

CONCEPTION D'ENSEMBLE
Propagation de l'étude préalable
Choix d'une **solution sécurisée**

SPÉCIFICATION FONCTIONNELLE
Répartition des responsabilités
Aspects spécifiques de la sécurité

CONCEPTION TECHNIQUE
Risques liés à l'exploitation
Mesures correspondantes
Résumé des mesures

PHASES DE FABRICATION
Contrôle, par les équipes de projet, des mesures prévues

PRÉPARATION DE MISE EN ŒUVRE
Sensibilisation aux risques
Formation sécurité (outils et systèmes)

RÉALISATION ET TESTS
Programmation sécurisée

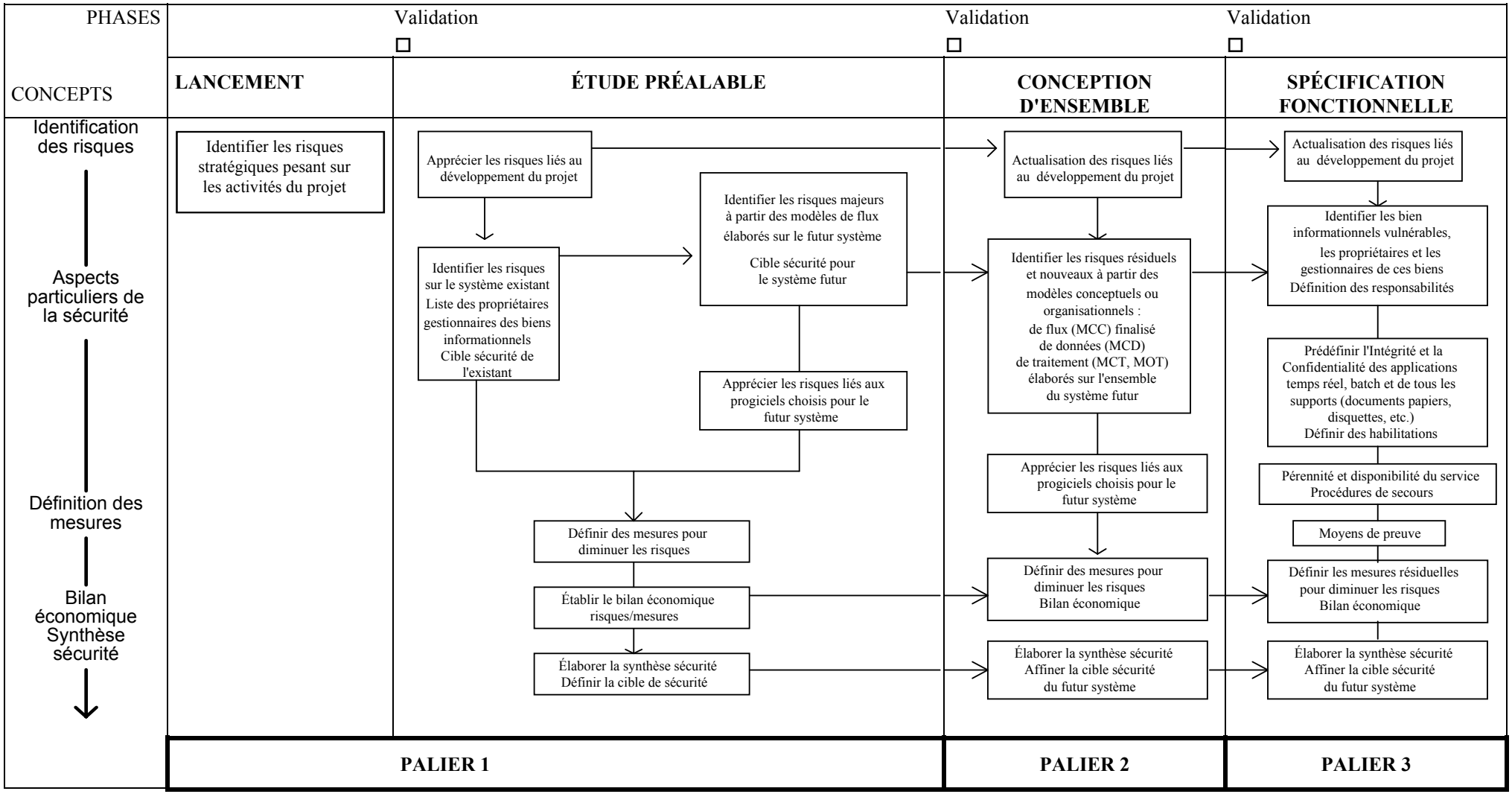
RECETTE
Recette des composants **sécurité**

DÉMARRAGE
Sécurité de fonctionnement

ÉVALUATION
Statut des mesures adoptées
(spécifiques à l'application ou mises en catalogue)

Source : ISM, volet sécurité de la méthode de conduite des projets informatiques à la Banque de France

VUE DE SYNTHÈSE DE LA DÉMARCHE D'INTÉGRATION DE LA SÉCURITÉ DANS LA CONSTRUCTION DES SYSTÈMES D'INFORMATION



LEXIQUE :

MCC-Modèle Conceptuel de Communication, MCD-Modèle Conceptuel des Données, MCT-Modèle Conceptuel des Traitements, MOT-Modèle Organisationnel de Traitement

VUE DE SYNTHÈSE DE LA DÉMARCHE D'INTÉGRATION
DE LA SÉCURITÉ DANS LA CONSTRUCTION DES
SYSTÈMES D'INFORMATION
(suite)

Validation ☐ — FABRICATION — Validation ☐

CONCEPTION TECHNIQUE	RÉALISATION ET TESTS	PRÉPARATION DE LA MISE EN OEUVRE	RECETTE	DÉMARRAGE	ÉVALUATION
Apprécier les risques liés au développement du projet Identifier les risques techniques nouveaux Analyser la propagation des risques techniques identifiés en amont Mesures visant à diminuer les risques techniques Mesures complémentaires de sauvegarde, de secours, d'habilitation aux BD, aux ressources d'exploitation, au réseau Révision éventuelle du bilan économique risques/mesures Synthèse sécurité	Apprécier les risques liés au développement du projet Examen des conditions de réalisation et de test des programmes	Vérification de l'application de la méthode de sécurité dans les phases de conception	Examen des aspects relatifs à la sécurité de l'organisation de la recette	Examen des aspects relatifs à la sécurité du passage à l'exploitation	Examen des aspects relatifs à la sécurité dans la gestion des applications
PALIER 4	**PALIER 5**	**PALIER 6**	**PALIER 7**	**PALIER 8**	**PALIER 9**

ANNEXE VII

EXEMPLE DE CHARTE DE LA SÉCURITÉ DE L'INFORMATION

PRÉAMBULE

La charte de la sécurité de l'information est le document qui établit les attributions et délimite les responsabilités de toutes les unités administratives de l'établissement.

I - DÉFINITION DE LA POLITIQUE DE SÉCURITÉ DE L'INFORMATION

A - Objet de la politique de sécurité

1. Le traitement de l'information qui est au coeur de toutes les activités composant les métiers de la banque, bénéficie de plus en plus de l'automatisation des tâches grâce aux performances sans cesse accrues de l'informatique centralisée ou locale et à l'extension des réseaux de télécommunication.

   L'évolution de ces techniques donne aux services, aux agences et aux personnes physiques ou morales en relation avec la banque, des moyens accrus de traitement et d'accès aux informations.

2. Cependant, le recours croissant à des procédés de stockage magnétique ou numérique de l'information, la généralisation progressive de l'usage de terminaux de saisie ou de consultation, l'extension des réseaux de transport de données ouverts sur l'extérieur sont autant d'accès nouveaux à l'information qui, joints à l'élévation continue du niveau des connaissances en informatique, sont à l'origine de nouveaux risques pour la banque.

3. En effet, les moyens modernes de traitement de l'information ont progressé plus vite que les techniques ou les procédures permettant d'en prévenir le vol, la perte ou la modification non contrôlée.

4. C'est ainsi qu'une prise en compte insuffisante de la sécurité peut générer avec une ampleur nouvelle, des risques informatiques spécifiques. Les erreurs de conception ou d'analyse des projets informatiques, les manipulations défectueuses des matériels et des logiciels, les malveillances de toute nature, le détournement des logiciels ou la divulgation de données confidentielles, enfin l'organisation insuffisante de moyens de sauvegarde et de secours, en sont autant d'exemples.

   Toutefois, les conséquences de tels événements -même affectés de probabilités inégales- sur l'activité, les ressources ou l'image de la banque dans le public, doivent faire l'objet d'une analyse exhaustive.

5. Aucune disposition ne peut garantir en toute certitude l'absence de risques informatiques. De ce fait, l'objet de la politique de sécurité est de contenir ces risques à un niveau acceptable au moyen d'un ensemble de mesures de protection technique et opérationnelle visant à :

   - identifier ou authentifier tout utilisateur des systèmes informatiques[46],
   - assurer l'intégrité des informations stockées ou transportées,
   - respecter la confidentialité des données,
   - rapporter la preuve de toute utilisation des ressources informationnelles ou d'échanges d'information,

[46] quel que soit le constructeur, un système informatique est défini par la loi comme "un ensemble composé d'une ou plusieurs unités de traitement, de mémoires, de logiciels, de données, d'organes d'entrées-sorties et de liaison, qui concourent à un résultat déterminé, cet ensemble étant protégé par des dispositifs de sécurité".

- organiser les moyens de secours en cas de défaillance du service rendu par le système d'information.

B - Domaine de la politique de sécurité

La sécurité de l'information comprend le domaine des fichiers contenus dans les systèmes d'information de l'établissement, mais aussi, plus généralement, l'information orale, écrite sur un support papier ou encore enregistré sur un film vidéo ou sur CD-ROM.

1. Les mesures de sécurité informatique à mettre en œuvre s'appliquent aux données et aux programmes enregistrés dans le système d'information de la banque, en mémoire centrale ou sur les supports en entrée et en sortie de ce système.

2. La sécurité des traitements sur le système d'information couvre le cycle de développement :

   - définition de standards de sécurité dans la conception des applications informatiques,

   - mise au point d'accords formalisés sur les droits d'accès entre le propriétaire d'une information, l'exploitant, le concepteur du logiciel et l'utilisateur,

   - définition de procédures de recette se rapportant aux spécifications de sécurité lors de l'installation ou de la modification des applications informatiques,

   et le cycle d'exploitation :

   - saisie de l'information,
   - conservation sur support magnétique,
   - transfert sur support magnétique ou sur réseau téléinformatique,
   - traitement sur un équipement informatique centralisé ou local,
   - sortie des résultats par affichage sur un écran ou par édition sur un support papier ou magnétique.

3. Les règles de sécurité de l'information s'appliquent :

   - aux services centraux des directions (ou filiales),
   - aux succursales de l'établissement,
   - aux prestataires de services et utilisateurs extérieurs qui interviennent dans le système d'information de la banque.

C - Responsabilité de la politique de sécurité

1. Les dirigeants responsables (Comité de Direction générale de la banque, Directoire...) définissent en liaison avec le RSSI la politique générale de sécurité de l'information.

   Ils se réunissent spécialement sur ce sujet au moins une fois par an en tant que Comité de Sécurité.

2. Le Responsable de la Sécurité des Systèmes d'Information (RSSI), attaché à un niveau hiérarchique élevé, présente les propositions pour décision au Comité de Sécurité, après avoir recueilli l'avis des Directions Opérationnelles concernées.

   Il rend compte au moins une fois par an au Comité de Sécurité de la mise en œuvre de la politique de sécurité.

II - MISE EN ŒUVRE DE LA POLITIQUE DE SÉCURITÉ

La politique générale définie par le Comité de Sécurité est mise en œuvre par les services et les agences.

Toutefois, certaines personnes et certaines unités ont en la matière des responsabilités spécifiques.

A - Responsabilités des services et des agences

1. Chaque unité administrative est responsable, au premier degré, de la sécurité de l'informatique dont elle est propriétaire.

   En conséquence, il lui appartient de définir avec l'appui des services spécialisés :

   - les droits d'accès des utilisateurs sur les informations de son ressort en fonction d'une échelle de confidentialité. En particulier, les accréditations sur ses fichiers des agents chargés de la programmation et de l'exploitation des logiciels doivent être précisées,

   - une échelle des priorités dans le dépannage des applications qu'elle exploite, afin d'organiser les moyens de secours en cas de défaillance du système d'information.

   En outre, les services et les agences (unités locales de base[47]) qui effectuent pour eux-mêmes des tâches de programmation de logiciels sont responsables, au premier degré, de la sécurité de ces développements.

2. Les unités locales appliquent les règles de sécurité et les standards établis par le RSSI avec le concours des responsables sécurité qui sont ses correspondants. Le RSSI effectue (ou fait effectuer) le contrôle de deuxième degré dont il assume la responsabilité vis-à-vis de la Direction générale.

   A cet effet, les unités locales sont tenues de diffuser auprès de tout leur personnel, les instructions qui leur sont adressées.

---

47 Les dénominations et découpages des Directions, services, agences, unités locales varient suivant les établissements. Par "unité locale de base" on entendra l'unité à qui est reconnue une certaine autonomie administrative, technique, financière. Selon les organisations (centralisées/décentralisées), cette unité locale peut être plus ou moins importante.

3. Le chef de chaque unité locale est responsable, au premier degré, du contrôle interne des règles de sécurité de l'information.

   Afin d'éclairer ses choix ou de préciser les modalités d'emploi des procédures ou de produits sécuritaires, il peut solliciter un avis autorisé. Sa demande est adressée au responsable sécurité qui prend conseil le cas échéant auprès du RSSI, ce dernier étant informé de la demande en toute hypothèse.

4. Toute perte ou vol de logiciel, de matériel et de documentation doit être déclaré par le service ou l'agence au RSSI qui évalue les suites à donner et informe le responsable sécurité attaché à l'unité locale à l'origine du constat.

   La suspension du service offert par un produit de sécurité sur un équipement informatique décentralisé[48] fait l'objet d'un compte rendu au gestionnaire local de la sécurité ou à défaut au responsable sécurité du service ou de l'agence.

5. Les incidents relatifs à la sécurité des transferts automatisés de programmes ou de données entre la banque et un tiers doivent être portés à la connaissance du RSSI.

B - Fonction des responsables sécurité et des gestionnaires locaux de sécurité

1. Chaque métier (ou Direction opérationnelle) désigne un ou plusieurs responsables sécurité qui seront les correspondants du RSSI.

   Les agences sont représentées par au moins un responsable sécurité affecté (par exemple) à la Direction du Réseau. En outre, un gestionnaire local de la sécurité est désigné dans chaque agence.

2. Les responsables sécurité sont réunis au minimum trois fois par an. Le RSSI tient le secrétariat de la réunion et informe le Comité de Direction générale des travaux qui y sont menés.

3. Les attributions des responsables sécurité s'exercent dans trois domaines :

   - concourir à la mise au point des normes et des standards de sécurité en référence aux besoins de sécurité des métiers,
   - faciliter la diffusion et l'observation des règles de sécurité dans les services et les agences en apportant aux métiers l'assistance et le conseil dans l'organisation et le choix des techniques de sécurité,
   - valider dans le cadre des développements informatiques, les travaux relatifs à la sécurité des projets.

48 Par exemple micro-ordinateurs de type PC.

4. Lorsque dans un service ou une agence, un outil de sécurité exige la mise en œuvre et le suivi de procédures décentralisées, un Gestionnaire Local de la Sécurité (GLS) y est désigné.

   Les attributions des GLS s'exercent dans trois domaines :

   - gérer les accréditations des utilisateurs sur les fichiers de sécurité par délégation des chefs d'unités locales, propriétaires de l'information,
   - gérer les données et les outils de sécurité[49], notamment dans les échanges de fichiers avec les autres métiers ou avec d'autres établissements,
   - assister les chefs d'unités locales dans le suivi de la sécurité, notamment par le biais des journalisations de sécurité sur les systèmes d'information.

C - Responsabilités des services de l'Organisation et Informatique

1. Les services de l'Organisation et de l'Informatique sont représentés dans tous les projets de sécurité conduits par le RSSI.

2. La Direction de l'Organisation et de l'Informatique (DOI[50]) est responsable, au premier degré, de la sécurité des développements logiciels réalisés par ses services.

   A cet effet, un pôle de compétence sécurité dans les services de l'Organisation et Informatique, apporte aux équipes de projet l'assistance et le conseil nécessaires à l'intégration de la sécurité dans les développements applicatifs.

3. La DOI est responsable de la mise en œuvre des dispositifs de sécurité matériels et logiciels qui protègent les exploitations informatiques gérées par ses services. Elle s'assure de leur fonctionnement régulier.

   La suspension du service offert par un produit de sécurité installé sur un équipement géré par un service de l'O.I. fait l'objet d'un compte rendu au RSSI.

4. L'application -selon une échelle de priorités définie avec les services utilisateurs- des procédures de dépannage des traitements sur les grands systèmes informatiques, sont de la compétence des services de l'Organisation et Informatique.

D - Responsabilités du Service de l'Inspection (ou audit)

1. Ces services sont chargés de contrôler dans les services et les agences le respect des règles de sécurité.

2. En outre, ils sont habilités à prendre l'initiative ou à participer avec un cabinet extérieur à des missions d'audit de la sécurité de l'information.

---

49 Par exemple les clés de chiffrement.

50 Quel que soit le nom qui lui est donné.

E - Responsabilités de la Direction de la Comptabilité (et des autres Directions opérationnelles ayant la charge des valeurs) [POUR MÉMOIRE]

Une cellule spécialisée à la Direction de la Comptabilité gère le stock de cartes à mémoire nécessaire à la sécurité de toutes les applications pourvues de ce dispositif, notamment l'application comptable des agences.

À cet effet,

1. Elle commande et distribue les cartes avec les codes porteurs qui y sont associés.

2. Elle gère le fichier des cartes perdues ou volées.

3. Elle collecte et analyse les cartes hors service.

F - Responsabilités du RSSI

Il met en œuvre les directives du Comité de Direction (ou de Sécurité) et lui rend compte de leur application.

À cet effet, il exécute, avec le concours des unités locales concernées ou éventuellement des sociétés de services, le plan sécurité arrêté par ce Comité.

Ses attributions sont les suivantes :

1. Suivre l'évolution des techniques de sécurité de l'information.

2. Définir des procédures standards de sécurité se rapportant à l'ensemble du traitement de l'information :

    - classification, communication, sauvegarde et destruction des données en fonction de leur sensibilité,
    - protection des données par type de classification,
    - incidence sur la sécurité de l'affectation du personnel[51],
    - classification, identification, authentification des utilisateurs,
    - respect des normes de sécurité dans la mise en œuvre des moyens de secours,
    - définition des normes de sécurité dans le développement des applications.

3. Choisir avec les spécialistes des services de l'O.I. les produits sécuritaires et en définir les règles de gestion.

4. Assumer l'administration centrale des outils de sécurité mis en place dans les services, les agences ou les unités locales.

51 ex. séparation des tâches.

5. Coordonner l'action des responsables sécurité :

    - en entreprenant à leur intention des actions de formation et d'information appropriées au suivi de la sécurité dans les unités administratives de leur ressort,
    - en veillant à leur participation aux groupes sécurité constitués à l'occasion des projets informatiques,
    - en organisant la gestion décentralisée des accréditations sur les fichiers de sécurité.

6. Entreprendre avec l'appui de la Direction de la Communication (ou de la Formation) des actions de sensibilisation de l'ensemble du personnel aux questions de sécurité de l'information.

7. Sensibiliser les chefs de projet, les agents des services de l'Inspection et de l'Audit aux contrôles à effectuer en matière de sécurité de l'information.

8. Saisir les services de l'Inspection et de l'Audit de demandes d'enquêtes.

9. Assurer la cohérence des différents pôles de décision en participant au Comité Technique Informatique (chargé de la cohérence technique des solutions techniques proposées pour les projets présentés par les Directions opérationnelles ou les chefs de projet[52]) et au Groupe chargé au sein de l'établissement de la Stratégie Informatique[53].

52 Maître d'ouvrage (chef de projet utilisateur) et maîtrise d'œuvre (chef de projet informatique).

53 Direction générale + RSSI + Directeur de l'OI + Directeurs opérationnels ou de métiers.

ANNEXE VIII

LE RSSI: RESPONSABLE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION SA FONCTION

Outre les développements contenus dans le Livre blanc lui-même (Chapitre III, paragraphe 2) et dans l'annexe VII précédente (paragraphe II-F), il paraît utile de fournir les quelques renseignements suivants relatifs à :

- son positionnement hiérarchique,
- le profil requis par le candidat à ce poste,
- les qualités nécessaires,
- ses missions.

1. L'importance du poste (son positionnement hiérarchique) :

Elle dépend de la volonté de la Direction générale et de l'importance qu'elle accorde à cette fonction.

Si des rattachements aussi divers qu'à :

- une division du D.O.I.,
- la Direction du D.O.I.,
- l'Inspecteur Général,
- le Président ou Directeur général,

peuvent être trouvés, il est indispensable, pour une meilleure efficacité, qu'un rattachement hiérarchique élevé soit donné.

2. Le profil requis par le candidat RSSI

- Une ancienneté certaine dans l'entreprise (bonne connaissance des métiers).

- Une compétence informatique réelle (il faut parler "d'égal à égal" avec les techniciens).

- Un bon sens de la communication.

3. Les qualités nécessaires ? Être :

- Méthodique
- Rigoureux
- Intègre
- Tenace
- Créatif
- Disponible

4. Les missions du RSSI[54] :

- **Sensibilisation, formation**
- Promotion de la sécurité
- Organisation de la sécurité
- Approche méthodologique de la sécurité
- **Analyse des risques**
- Politique sécurité
- Plan sécurité
- Définition des règles, normes, procédures
- Garant de la cohérence
- Conseils, recommandations, assistance
- **Certification des dispositifs de sécurité**
- Administration de la sécurité
- Gestion des habilitations
- Gestion des clés et secrets
- Gestion des incidents
- **Audit, contrôle du respect des règles**
- Suivi, reporting, tableaux de bord
- Plan de secours (définition, tests, suivi)
- "Correspondant ..."
- **Veille technologique**
- Relations avec les "clubs"
- Interlocuteur sécurité pour l'extérieur
- Relations contractuelles avec les SSII
- **Déontologie informatique**
- etc

54 Les missions qui deviennent aujourd'hui prépondérantes sont repérées en gras.

ANNEXE IX

MÉTHODES UTILISABLES PAR LE RSSI

On trouvera quelque avantage à s'appuyer sur des méthodes pour élaborer puis conduire la mise en place ou l'évolution du schéma directeur de sécurité des systèmes d'information de l'entreprise.

Parmi celles-ci on distingue les méthodes :

- d'analyse des risques (ex : BUDDY[55], CRAMM[56], MARION[57], MELISA[58]...) qui concourent à l'élaboration du plan de sécurité que la direction générale inscrit au plan de charge de l'établissement
- de maîtrise de la conduite des projets informatiques (ex : INCAS[59]...) qui, pour la réalisation d'un niveau de sécurité, respectent des critères d'évaluations établis (ex : TSEC[60], ITSEC/ITSEM[61]).

I - Sommairement les typologies des méthodes citées et qui permettent d'élaborer un plan d'action, sont les suivantes (par ordre alphabétique) :

BUDDY

Sur la base des constats suivants :

- la vulnérabilité d'un système d'information décroît quand le nombre de parades (qui ont une vulnérabilité intrinsèque) augmente sans modifier pour autant la fréquence d'occurrence d'une menace,
- un niveau acceptable de vulnérabilité peut être obtenu par la mise en place de parades.

55 Méthode d'analyse et d'administration de risques - produit de COUNTERMEASURES, INCORPORATED, HOLLYWOOD, MARYLAND, USA

56 CcTA Risk Analysis Management Methodology - évaluation des systèmes d'information du gouvernement Britannique

57 Méthode d'Analyse des risques informatiques et optimisation par niveau - CLUSIF : Club des Utilisateur de la Sécurité Informatique Français

58 Méthode française dont une version est mis à disposition des entreprises civiles

59 INtégration dans le Cycle de développement Applicatif de la Sécurité - CLUSIF

60 Critères d'évaluation de la sécurité des systèmes d'information du département de la défense des Etats Unis d'Amérique - années 80

61 Information Technology Security Evaluation Criteria/Manual - Allemagne, France, Grande-Bretagne, Pays-Bas : Office for Official Publications of the European Communities

La méthode BUDDY est conduite en trois phases :

1. Préparation

- recensement des sites
- préparation d'un questionnaire d'audit pour chaque site

2. Analyse du risque

- analyse des informations collectées par les questionnaires des sites
- analyses des vulnérabilités

3. Gestion du risque

- propositions d'actions correctives, suivies de décisions de la direction
- information aux utilisateurs
- suivi et contrôle de la mise en œuvre des décisions de la direction.

CRAMM

Sur la base des constats suivants :

- un système de traitement de l'information peut être décrit comme un ensemble de biens physiques, de logiciels de traitements et de données,
- un bien *compromis*, *détruit*, *altéré* ou *indisponible* entraîne un dommage mesurable pour l'ensemble du système de traitement,
- chaque groupe de biens a une vulnérabilité selon une probabilité d'occurrence de réalisation des menaces,
- la mise en place de parades peut réduire le niveau de risque pour atteindre un niveau acceptable de vulnérabilité,
- la vulnérabilité d'un système d'information décroît quand le nombre de parades (*qui ont une vulnérabilité intrinsèque*) augmente, sans modifier pour autant la fréquence d'occurrence d'une menace.

La méthode CRAMM est conduite en trois phases :

1. Identification et évaluation des biens

- sur une échelle graduée de 1 à 10, évaluation pour chaque bien des dommages consécutifs à la compromission, l'altération, la destruction ou l'indisponibilité.

2. Estimation des risques

- constitution de groupes de bien vulnérables aux mêmes menaces,
- détermination sur deux échelles graduées : faible, moyen, élevé de la probabilité d'occurrence d'une menace et du niveau de vulnérabilité de chaque lien groupe de biens/menace,

- une échelle graduée de 1 à 5 détermination du niveau de risque de chaque groupe d'objet face à la compromission, l'altération, la destruction, l'indisponibilité,

- validation par la direction.

3. Choix des parades

- coût de réalisation des parades selon les menaces et les biens protégés,
- planification de la mise en place des mesures.

MARION

Cette méthode est déclinée en plusieurs versions spécialisées par domaine technique (ex : Marion MICRO, réseaux) et adaptable au niveau de finesse souhaité dans l'étude (ex : questionnaire de 70 questions à celui de 600). Cette méthode ou des approches voisines est une offre standard des cabinets de conseil.

La méthode MARION est conduite en six étapes :

1. Analyse des risques

- découpage par champ d'automatismes du système d'information,
- découpage typologique sur le triptyque type de risque/fonction/sous-fonction,
- découpage par type de perte,
- détermination du risque maximum.

2. Expression du risque maximum admissible

- définition des ratios pertinents,
- détermination des fourchettes admissibles des ratios par la capacité financière de l'entreprise.

3. Analyse des moyens de la sécurité

- évaluation du niveau de sécurité sur 27 facteurs et représentation graphique du niveau de sécurité global,

- représentation graphique de l'effort à produire pour chaque facteur pour atteindre un niveau acceptable,

- réflexion sur le budget de la sécurité.

4. Évaluation des contraintes

- contraintes techniques, humaines, procédurales, structurelles, budgétaires,
- équilibrage entre les mesures de prévention et de protection.

5. Choix des moyens

- optimisation sous contraintes du choix de protection et de prévention,
- test des hypothèses budgétaires et détermination du coût estimé.

6. Plan de sécurité

- développement des solutions choisies à la cinquième étape pour chaque hypothèse de budget,
- actualisation du calcul des risques de la première étape en fonction de la solution de protection déterminée à la cinquième étape,
- orientation vers le choix optimum,
- transfert de risque à l'assurance.

MELISA

Sur la base des constats suivants :

- les valeurs de l'entreprise peuvent être représentées sur des axes stratégiques (*gradués par niveau de gravité*),
- les ressources vitales et sensibles de l'entreprise matérialisent ses valeurs intrinsèques et ses valeurs de nécessité,
- la destruction, la divulgation, l'altération, l'indisponibilité des ressources sont mesurables sur les axes stratégiques,
- un paramètre unique peut être déterminé à partir du quadruplé : gravité/non-détection/facilité de réalisation/sujet pour exprimer la vulnérabilité de l'entreprise,
- face à chaque scénario de menace existent une ou plusieurs parades qui concourent à réduire la gravité.

La méthode MELISA est conduite en cinq phases :

1. Analyse des enjeux

- définir la cible de l'évaluation,
- analyser les enjeux en définissant les objectifs fonctionnels de la sécurité,
- constitution de la structure organisationnelle qui préside le chantier MELISA.

2. Analyse de l'existant

- réaliser la matrice d'accès entre objet et sujet,
- hiérarchiser les menaces,
- inventorier les mesures de sécurité existantes,
- considérer la situation locale,
- calculer la vulnérabilité effective.

3. Simulation

- calcul de la vulnérabilité résiduelle après mise en œuvre cohérente des parades.

4. Décision, validation, mise en œuvre

- proposer les parades à la structure de décision qui validera un ensemble de mesures,
- planifier la mise en œuvre.

5. Suivi technique et budgétaire

II - Parmi les méthodes de conduite de projet informatique[62], INCAS possède les caractéristiques suivantes :

INCAS

Les mesures à mettre en œuvre dans le cadre de la réalisation d'un projet informatique sont déterminées par les exigences de sécurité analysées sous trois aspects en termes de :

- disponibilité ou continuité de service,
- d'intégrité ou garantie de fiabilité des données,
- confidentialité ou garantie d'inaccessibilité à des informations confidentielles.

La méthode INCAS est conduite en cinq étapes qui accompagnent l'avancement d'un projet (*étude d'initialisation, étude préalable, étude détaillée, réalisation, recette, mise en œuvre*) et prend en compte son cycle de vie (*maintenance*):

1. Évaluation du poids stratégique du projet

- les étapes 2 et 3 sont menées parallèlement

2. Appréciation de la sécurité du système existant

3. Analyse de la sécurité du futur système

4. Proposition des mesures globales et détaillées

5. Synthèse, bilan économique et cible de sécurité

Les critères d'évaluation ITSEC permettent, pour des systèmes ou des produits, de classer ceux-ci par catégorie selon les strates des services de sécurité offerts et réalisés (ex : identification et authentification). Le niveau de service le plus bas est repéré E0 et le plus élevé E6 pour les critères ITSEC. La correspondance entre la classification ITSEC (en Europe) et TCSEC (aux U.S.A.) est la suivante pour chaque niveau :

ITSEC	E0	E1	E2	E3	E4	E5	E6
TCSEC	D	C1	C2	B1	B2	B3	A1

62 On trouvera également en annexe VI un autre exemple de méthode pour aider à la prise en compte de la sécurité dans les applications (méthode ISM -proche de MESSIE- intégration de la sécurité dans MELODIC, méthode dérivée de MERISE, utilisée par la Banque de France).

ANNEXE X

Nouveau questionnaire

Questionnaire 1 : Évaluation des enjeux
Évaluation du Risque Maximal Tolérable *page 255*
Le Dossier d'analyse du Risque Maximal (DSRM[63]) *page 256*

Questionnaire 2 : Évaluation du niveau de sécurité informatique
Informatique centralisée ou départementale *page 259*
Réseau local *page 289*

Questionnaire 3 : Matrices budgétaires, coût de la sécurité, couvertures assurances
Budget informatique
année -1 *page 301*
année -3 *page 303*
note méthodologique *page 305*

Estimation des dépenses consacrées à la sécurité informatique *page 307*

Assurances - grille harmonisée européenne *page 309*

Questionnaire 4
Appréciation de l'efficacité et de la performance opérationnelle de l'informatique *page 311*

Les critères d'appréciation des utilisateurs *page 317*

Coefficients de pondérations

Sites centraux *page 319*

Réseaux locaux *page 323*

63 Dossier de sinistre de risque maximal.

QUESTIONNAIRE 1 : Évaluation des enjeux

1-A LE RISQUE MAXIMAL TOLÉRABLE OU RMT

à servir par la Direction Générale et/ou le Secrétariat Général

RISQUE MAXIMAL TOLÉRABLE

Quel est le montant maximal[64] (en MF) du risque créé par un sinistre informatique que vous estimez pouvoir être supporté par votre établissement sans remettre en cause la continuité de ses opérations ?
(Ce risque maximal tolérable est la limite, nécessairement inférieure aux fonds propres, que vous fixez ; elle sert à compenser les éventuelles pertes liées à un sinistre)

Montant : ____ **MF**

Nom de la personne ayant rempli ce questionnaire	
Fonction	
Téléphone	

[64] Exposer brièvement la méthode d'évaluation

1-B LES DSRM (Dossiers d'Analyse du Risque Maximal)

(fiches à servir par la Direction de l'Informatique)

En paralèlle à l'évaluation du RMT, le chiffrage des principaux risques informatiques de l'établissement suivant des scénarios pré définis permet, par rapprochement, d'établir une cohérence et une vraisemblance entre les déclarations.

Dossier d'Analyse de Risque Maximum - RM en réalisation d'un risque informatique physique maximal	**DSRM**

➔ ***Scénario :*** ***❶ Destruction totale d'un site de production informatique,***
➔ ***Scénario :*** ***❷ Indisponibilité du réseau Télécom ou réseau interne privé (48 heures),***
➔ ***Scénario :*** ***❸ Scénario défini par le chef d'établissement,***

➔ Dans la colonne Évaluation globale, noter les **valeurs de remplacement** -hors indemnité d'assurance- des matériels, locaux, contenus sinistrés **en se limitant à ce qui est directement lié à l'informatique** : fournitures, main d'œuvre, transport, etc.

Nature des pertes	Évaluation globale (kF)	Indemnité assurance
● Dommages matériels		
• Frais de déblaiement et divers après sinistre		
• Matériel[65]		
- Informatique		
- Péri-informatique[66]		
- Télécommunications		
- Gaines et câbles		
- Electrique, électronique		
- Climatisation		
• Logiciels		
• Locaux (ou résident les matériels ci-dessus)		
• Contenu informatique		
- Supports: bandes, disques, ...		
- Fournitures		
- Equipement de bureau et divers		
● Reconstitution d'informations		
- informatique		
- utilisateurs		

[65] En cas de contrat de leasing noter les indemnités restant dues

[66] Modems, écrans, imprimantes

● Frais supplémentaires d'exploitation		
- Coût de transport et de stockage des supports - sauvegarde des documents, etc.- sur le site de secours ou in situ		
- Coûts supplémentaires de Télécommunications		
- Coûts de progiciels supplémentaires, à titre de dépannage.		
- Coûts de maintenance ou de réparations, coûts de sauvetage et nettoyage.		
- Prestations de services -SSII- supplémentaires, personnel intérimaire.		
- Intervention de conseils et spécialistes.		
- Frais supplémentaires de personnels informatiques : déplacements, primes, ...		
- Sous traitance de saisie, d'exploitation .		
- Coût d'usage de matériels et systèmes et services extérieurs, backup ou analogue.		
- Location exceptionnelle de matériels ou locaux.		
- Autres frais incombant directement à l'informatique		
● Pertes financières		
- PE directes (activité)		
- PE indirectes (clientèle)		
- PE intérêts financiers		
- PE divers		
● Pertes de biens et de fonds		
● Préjudices aux tiers		
● Autres pertes		
TOTAL :		

Nom de la personne ayant rempli ces questionnaires	
Fonction	
Téléphone	

QUESTIONNAIRE 2 : Évaluation du niveau de sécurité informatique

2-A INFORMATIQUE CENTRALISÉE ou DÉPARTEMENTALE

❶ Appréciation générale de la sécurité de l'entreprise :

①Facteur 101 - Organisation générale

❍ Organigrammes hiérarchiques et fonctionnels

Question 101-1:
Existe-t-il un organigramme hiérarchique et fonctionnel de l'entreprise, mis à jour régulièrement et proposant une définition des fonctions précisant les attributions -et les restrictions de responsabilité- pour chaque poste ayant une responsabilité décisionnelle ?

Note (0 à 4) :

Observations :

❍ Comité Sécurité

Question 101-2:
Existe-t-il un Comité permanent chargé d'étudier tous les problèmes liés à la sécurité, se réunissant périodiquement et chaque réunion donnant lieu à un compte rendu écrit ?

Note (0 à 4) :

Commentaire :
La composition de ce Comité est importante, il doit inclure les représentants de la DG, de la DI, des utilisateurs, de l'Audit interne et des gestionnaires des couvertures assurances. La périodicité de réunion proposée par MARION est de 4 fois par an.

Observations :

Question 101-3:

Y a-t-il un suivi et un contrôle des recommandations prescrites par le rapport précédemment cité ?

Note (0 à 4) :

❍ *Étude de vulnérabilité*

Question 101-4:

Y a-t-il eu une étude sur la vulnérabilité de l'entreprise face à différents types de risques physiques ou non -pas nécessairement informatiques- dans les 3 dernières années ayant entraîné la mise en place d'un Plan de Sauvegarde ?

Note (0 à 4) :

Commentaire :

La réponse porte à la fois sur l'existence de l'étude, de son ancienneté, de l'existence d'un rapport écrit pour la première partie de la note et la formalisation d'un plan de sauvegarde (à consulter) intégrant les mesures conservatoires et notamment celles financières pour la seconde partie.

Observations :

❍ *Responsable Sécurité*

Question 101-5:

Le Responsable Sécurité dispose-t-il d'un poste spécifique sur l'organigramme avec un rattachement hiérarchique élevé et dispose-t-il d'un budget ?

Note (0 à 4) :

Observations :

②Facteur 102 - Contrôles permanents

❍ *Propriétaire des informations*

Question 102-1:

Existe-t-il un dépositaire ou propriétaire des informations nommément désigné et responsable des règles, procédures et autorisations d'utilisation des informations dont il a la charge ?

Note (0 à 4) :

Observations :

Question 102-2:

A-t-on effectué une classification objective -selon les critères Disponibilité, Intégrité, Confidentialité, Preuve- des informations en fonction de l'impact -risque maximum- qu'un sinistre touchant ces informations aurait sur l'entreprise ?

Note (0 à 4) :

Observations :

❍ *Choix des contrôles non informatiques*

Question 102-3:

Y a-t-il une étude particulière, lors de la conception des applications, sur le choix des contrôles automatisés et utilisateurs en amont et en aval de l'information et si cette étude existe, prend-elle en compte le niveau de classification de chaque information ?

Note (0 à 4) :

Commentaire :

Une telle étude devrait être fondée sur l'analyse des schémas de circulation, de la variabilité des données à traiter et des risques d'erreurs ou de malveillance.

Observations :

❍ ***Qualité des contrôles non informatiques***

Question 102-4:
La mise en place des contrôles utilisateurs fait-elle l'objet de procédures écrites ?

Note (0 à 4) :

Observations :

❍ ***Analyse spécifique des comptes sensibles***

Question 102-5:
Y a-t-il une analyse des comptes comptables sensibles - distincte de celle des Commissaires aux comptes- au moins deux fois par an, les résultats étant consignés par écrit ?

Note (0 à 4) :

Observations :

③Facteur 103 - La réglementation et l'Audit

❍ ***Procédures générales***

Question 103-1:
Existe-t-il un règlement écrit précisant les responsabilités des personnes et la procédure de signature selon le type de document traité ?

Note (0 à 4) :

Commentaire :
Cette question recouvre autant les délégations en matière d'engagements bancaires que la classification des documents d'ordre interne présentant un certain degré stratégique ou confidentiel.

Observations :

Question 103-2:

Tout document comportant des informations stratégiques est-il accompagné à la saisie de pièces justificatives signées par les personnes accréditées ?

Note (0 à 4) :

Observations :

❍ *Archivage et sécurité des documents originaux*

Question 103-3:

A-t-on pris en compte la possibilité de destruction totale d'informations stratégiques - fichiers, programmes, procédures d'exploitation, documentation, etc.- sur support informatique et en a-t-on déduit les procédures systématiques de rétention des documents de base qui pourraient servir à la reconstitution ?

Note (0 à 4) :

Observations :

❍ *Audit informatique*

Question 103-4:

Y a-t-il un audit général (externe ou interne) annuel consacré au moins le tiers du temps au contrôle de l'informatique ?

Note (0 à 4) :

Observations :

④Facteur 201 - Les facteurs socio-économiques

❍ *Aspects socio-économiques*

Question 201-1:

A-t-on le sentiment que le climat social est correct et qu'il n'y a pas à redouter d'action bloquante pour l'exploitation informatique ou d'action interne malveillante ?

Note (0 à 4) :

Commentaire :

Le climat social peut s'apprécier à travers le nombre de jours de grève sur les 3 dernières années, le taux de turn over du personnel et l'action interne malveillante en réponse à l'existence d'un plan social ou de licenciements individuels.

Observations :.

Question 201-2:

A-t-on formalisé un code d'éthique ou de déontologie interne et sensibilise-t-on le personnel sur cette base ?

Note (0 à 4) :

Observations :

❷ Les principes généraux de la sécurité

①Facteur 301 - L'environnement de base

❍ *Sécurité des locaux informatiques*

Question 301-1:
Y a-t-il eu des études contrôlées périodiquement par un organisme spécialisé, sur les dangers présentés par des facteurs extérieurs sur les locaux informatiques avec un suivi des recommandations prescrites ?

Note (0 à 4) :

Observations :

❍ *Protection périphérique*

Question 301-2:
*Dispose-t-on d'un système opérationnel, **cohérent et complet**, de contrôle des accès et de détection des intrusions à la périphérie de tous les bâtiments renfermant des locaux informatiques relié à un poste permanent de surveillance ?*

Note (0 à 4) :

Observations :

❍ *Sécurité des installations*

Question 301-3:
Y a-t-il eu des études, contrôlées périodiquement par un organisme spécialisé, sur les dangers présentés par des facteurs internes au bâtiment renfermant les locaux informatiques ?

Note (0 à 4) :

Observations : Ce thème porte essentiellement sur la sécurité des installations électriques et du câblage

②Facteur 302 - Le contrôle d'accès physique

❍ *Protection et surveillance des salles informatiques*

Question 302-1:

*Y a-t-il un système automatique et **complet** de contrôle d'accès systématique aux salles contenant les ordinateurs (unités centrales et périphériques) ?*

Note (0 à 4) :

Observations :

Question 302-2:

Le système d'accès est-il centralisé avec un traitement automatisé sécurisé et est-il hiérarchisé par type de personnel et de local ?

Note (0 à 4) :

Commentaire :

Le système de gestion des accès doit être sécurisé (gestion des autorisations, planning horaires, traces des accès, ...) et disposer d'une procédure d'accréditation strictement limitative au regard de l'activité de l'individu concerné.

Observations :

③Facteur 303 - La pollution

❍ *La pollution*

Question 303-1:
Les conséquences éventuelles de problèmes liés aux poussières, à la qualité de l'eau, à l'électricité statique et à la qualité de l'air ont-elles été évaluées (études par des organismes spécialisés) et ont-elles fait l'objet de mesures appropriées ?

Note (0 à 4) :

Commentaire :
L'auditeur pourra aborder les problèmes liés à l'environnement immédiat du site étudié : atmosphère aérienne, hygrométrie, électricité statique, dépôt de matières toxiques,.... Il s'attachera à vérifier l'absence de matériels générateurs de poussières de la salle contenant des processeurs.

Observations :

④Facteur 304 - Les consignes de sécurité physique

❍ *Élaboration et tests des consignes*

Question 304-1:
Toutes les consignes de sécurité générale sont-elles correctement affichées et ont-elles fait l'objet de concertation, d'information et de formation ; sont elles testées périodiquement ?

Note (0 à 4) :

Commentaire :
L'auditeur vérifiera que les consignes de sécurité sont correctement affichées, que les consignes des salle informatiques sont spécifiques aux risques liés à la présence de matériels informatiques, différenciées par type de local et par type de risque et sont connues des utilisateurs ; il se fera communiquer des comptes rendus de tests.

Observations :

⑤Facteur 305 - Sécurité spécifique incendie

❍ *Étude spécifique et compartimentage*

Question 305-1:

Pour le bâtiment renfermant les locaux informatiques et pour les locaux informatiques eux-mêmes, y a-t- il eu ***une étude spécifique du risque incendie*** *réalisée par un organisme spécialisé, prenant en compte les problèmes de prévention et de protection (compartimentage des locaux, détection, extinction, etc.) avec un suivi des recommandations prescrites ?*

.

Note (0 à 4) :

Observations :

❍ *Détection automatique salles informatiques*

Question 305-2:

Existe-t-il une installation de détection automatique d'incendie complète pour les salles ordinateurs, composée d'au moins 2 types de détecteurs et ayant fait l'objet d'une déclaration de conformité ?

Note (0 à 4) :

Commentaire :

Voir comptes-rendus de maintenance des installation et rapport de visite des pompiers.

Observations :

❍ *Extinction automatique salles ordinateurs*

Question 305-3:

Les salles ordinateurs sont-elles protégées par une installation d'extinction automatique d'ambiance fonctionnant en permanence (sans débrayage manuel) ?

Note (0 à 4) :

Observations :

⑥Facteur 306 - Sécurité spécifique dégâts des eaux

❍ *Études spécifiques dégâts des eaux*

Question 306-1:

Y a-t-il eu des études, contrôlées périodiquement par un organisme spécialisé, sur les dangers présentés par l'eau sur les salles ordinateurs et de matériels d'environnement (huisserie, toiture, canalisations, etc.) et les recommandations ont-elles été suivies d'effet ?.

Note (0 à 4) :

Observations :

❍ *Évacuation de l'eau*

Question 306-2:

Y a-t- il un système d'évacuation d'eau dans le plancher des salles ordinateurs, naturel (plancher incliné) ou mécanique (pompes) non antinomique avec la sécurité incendie (exemple : étanchéité du local lors de l'utilisation du gaz halon)?

Note (0 à 4) :

Observations :

⑦Facteur 307 - Fiabilité de fonctionnement des matériels informatiques

❍ *Redondance informatique*

Question 307-1:

Y a-t-il une redondance réelle locale des unités centrales des ordinateurs et des organes stratégiques (contrôleurs, frontaux, etc.) qui repose sur un plan de basculement écrit et testé périodiquement ?

Note (0 à 4) :

Observations :

⑧Facteur 308 - Les systèmes et procédures de secours

❍ *Études préliminaires*

Question 308-1:

A-t-on réalisé une étude préliminaire, du type MARION AP, qui permette de classer les applications dans l'ordre décroissant des pertes ou préjudices qui surviendraient après un sinistre physique (total ou partiel), d'une panne grave ou d'une grève ?

Note (0 à 4) :

Commentaire :

Afin de procéder au choix du degré de couverture des moyens de secours (sauvetage exhaustif ou partiel), a-t-on effectué les études permettant d'isoler le noyau des applications stratégiques au plan fonctionnel et au plan de l'exploitation (planification, procédures cataloguées, sauvegardes des fichiers).

Observations :

Question 308-2:

Dans le cas ou l'on vise un sauvetage exhaustif de toutes les applications, a-t-on étudié les besoins globaux (matériels et logiciels), la planification de la charge ainsi que les contraintes techniques et organisationnelles ?

Note (0 à 4) :

Observations :

❍ ***Plan de secours***

Question 308-3:

Existe-t-il un plan de secours reprenant l'exploitation éventuellement en mode dégradé et/ou éclaté (sur plusieurs sites) ainsi que des documents permettant le mise en oeuvre rapide des procédures de sauvetage ?

Note (0 à 4) :

Commentaire :

Le plan de secours doit inclure :

- ❍ la liste des médias et documents à protéger et à emporter en cas de sinistre,
- ❍ les procédures de reprise manuelles temporaires dans les services utilisateurs,
- ❍ les procédures de liaison avec les entités extérieures à l'entreprise,
- ❍ la gestion des ressources humaines,
- ❍ la réservation du site de secours,
- ❍ la restauration du système d'exploitation, du réseau et des fichiers,
- ❍ la relance primaire des applications,
- ❍ les processus post-reprise (commande de matériels, reconstitution du site, ...),
- ❍ les processus et planning de retour à la normale.

Observations :

Question 308-4:

Le plan de secours est-il remis à jour (évolutions matérielles et logicielles, configuration réseau...) et sauvegardé périodiquement ?

Note (0 à 4) :

Commentaire :

Le plan de secours doit pouvoir, au moins pour les applications stratégiques, être mis en œuvre à tout moment.

Observations :

❍ *Back up*

Question 308-5:

Existe-t-il une solution de back-up :

- *soit sur un site de secours strictement réservé au site étudié (salle redondante),*
- *soit par un système de secours contractuel avec un façonnier spécialisé incluant les règles de priorité d'utilisation, le mode de réservation, les délais de mise à disposition et les plages horaires de fonctionnement,*
- *soit un système de secours interne à l'entreprise ?*

Note (0 à 4) :

Commentaire :

Le différentes solutions à analyser n'ont pas la même valeur de sécurité :

- la solution de la salle redondante offre le maximum de sécurité si son niveau technique est maintenu "parallèle" au site de référence,
- la solution contractuelle chez un façonnier doit faire l'objet d'une analyse détaillée au niveau des engagements contractuels,

dans tous les cas, la disponibilité des moyens et leur adéquation aux choix stratégiques doit être vérifiée.

Observations :.

❍ *Réseau*

Question 308-6:

En cas de reprise du réseau, a-t-on effectué une étude spécifique, tenant compte de la sécurité sur le choix des liaisons entre le site de secours et le site étudié ?

Note (0 à 4) :

Observations :

❍ ***Tests***

Question 308-7:
La solution de secours est-elle complètement testée au moins 2 fois par an ?
Note (0 à 4) :

Observations :

⑨Facteur 309 - Les protocoles utilisateurs-informaticiens

❍ ***Micro-informatique : choix et règles***

Question 309-1:
La Direction informatique réalise-t-elle les choix techniques en matière de micro-informatique ?
Note (0 à 4) :

Commentaire :
Les choix recouvrent les architectures techniques (réseau local, connexion main-frame,...), approvisionnements en matériels, les systèmes d'exploitation (intégration) et les progiciels utilisateurs (compatibilité ascendante).
L'auditeur s'attachera à relever la cohérence de la politique d'attribution de matériels micro-informatique et l'intégration des choix dans un politique à long terme tenant compte des standards des méthodes de développement et des capacités d'intégration dans une architecture de traitement répartie.

Observations :

Question 309-2:

La Direction de l'informatique propose-t-elle :

- ❍ *des moyens centraux de sauvegarde,*
- ❍ *des moyens de détection et de lutte contre le sabotage immatériel (virus) ?*

Note (0 à 4) :

Observations :

Question 309-3:

Existe-t-il un système de contrôle et de restriction des accès pour les micros connectés ou connectables (portables) ?

Note (0 à 4) :

Observations :

❍ ***Intégration de la sécurité***

Question 309-4:

Les Comités Informatiques ou Sécurité font-ils obligation qu'il y ait un chapitre sûreté des systèmes d'information dans chaque document (avant-projet, cahier des charges, dossier applicatif) relatif à une étude informatique ?

Note (0 à 4) :

Observations :

①⓪Facteur 310 - Le personnel informatique

❍ *Définition de fonctions, responsabilité, qualité*

Question 310-1:

Le Règlement intérieur précise-t-il les obligations et les responsabilités du personnel quant à l'utilisation, la conservation et l'archivage des biens en fonction de niveaux de classification ainsi que les limites du secret professionnel avec les modalités de sa protection ?

Note (0 à 4) :

Observations :

①①Facteur 311 - Les plans informatiques et de sécurité

❍ Plan de sécurité

Question 311-1:

Existe-t-il un plan de sécurité des systèmes d'information remis à jour chaque année incluant : une évaluation quantitative des risques, une définition des risques intolérables (en liaison avec les utilisateurs), les moyens de sécurité existants, ceux à mettre en oeuvre, le planning et les priorités, un budget annuel de la sécurité, les règles de sécurité et le tableau des responsabilités, une étude spécifique pour l'infocentre et les moyens autonomes libres ou connectés ?

Note (0 à 4) :

Observations :

❹ La sécurité des matériels et logiciels de base

①Facteur 401 - Le contrôle des accès logiques

❍ Système de contrôle des accès logiques

Question 401-1:

Y a-t-il et utilise-t-on un système ou progiciel de contrôle d'accès dont le choix a reposé sur une analyse préalable des besoins et d'une étude fonctionnelle comparative des différents produits ?

Note (0 à 4) :

Observations :

Question 401-2:

Y a-t-il une analyse et un outil de suivi et de contrôle (tableau de bord, trace d'audit) permettant de mémoriser et de suivre les accès aux ressources (au moins les fichiers et les données par type d'accès et d'utilisateur) ?

Note (0 à 4) :

Observations :

Question 401-3:

Le système de contrôle d'accès prend-il en compte tous les accès locaux ou à distance sans aucune exception (y compris les accès vidéotex, la télémaintenance, les portables, etc.) ?

Note (0 à 4) :

Observations :

Question 401-4:

Y a-t-il une identification et une authentification pour chaque utilisateur (mot de passe, clé ou carte personnelle,...) ?

Note (0 à 4) :

Observations :

Question 401-5:

Y a-t-il une journalisation et un suivi quotidien des tentatives infructueuses de connexions?

Note (0 à 4) :

Observations :

② Facteur 402 - La sécurité des télécommunications

❍ *Sécurité du réseau*

Question 402-1:

*Lors de l'étude préalable sur le choix du réseau, a-t-on pris en compte le **choix du type** (liaisons spécialisées, réseau commuté, Transpac, Transmic, etc.) et le **mode dégradé** (maillage du réseau, redondance des points d'accès, etc.) ?*

Note (0 à 4) :

Observations :

Question 402-1-1:

*La liaison primaire (raccordement au réseau) est-elle **doublée** (raccordement à deux centraux différents) et est-elle sécurisé (chemin de câble interne à l'entreprise protégé) ?*

Le réseau est-il géré par au moins 2 unités frontales situées dans des locaux séparés et protégés ?

Note (0 à 4) :

Observations :

Question 402-1-2:

*Dans le cas d'utilisation du RTC, **la table des numéros d'appel est-elle protégée** et existe-t-il une procédure de rappel de l'appelant ?*

Note (0 à 4) :

Observations :

❍ ***Surveillance des lignes et transmissions stratégiques***

Question 402-1-3:

Utilise-t-on pour les données sensibles échangées interentreprises (EDI) un ***protocole normalisé*** *incluant la protection des informations de bout en bout (EDIFAC, ETEBAC, ATLAS, etc.) ?*

Note (0 à 4) :

Observations :

Question 402-2:

Les transactions stratégiques ne peuvent-elles être effectuées qu'à partir de terminaux placés dans des locaux à accès contrôlé et/ou disposant d'un système spécifique de sécurité d'accès logique (mot de passe de certification, lecteur de carte à mémoire, etc.) ?

Note (0 à 4) :

Observations :

Question 402-3:

Les virements et opérations financières télématiques, les transferts d'informations "confidentielles" pour l'entreprise sont-ils uniquement supportés par un réseau professionnel spécifique -type SWIFT - avec, pour les opérations financières, une gestion des oppositions en cours ?

Note (0 à 4) :

Observations :

Question 402-4:
Pour les transactions stratégiques, utilise-t-on :
un système de chiffrement (algorithme connu et déclaré),
un procédé de signature numérique et de scellement ?

Note (0 à 4) :

Observations :

③ Facteur 403 - La protection des données

❍ *Administration de bases de données*

Question 403-1:
Existe-t-il un administrateur des bases de données responsable de la mise en place, des modifications et de la surveillance de la structure des bases ?

Note (0 à 4) :

Observations :

❍ *Journalisation et sécurité des MAJ*

Question 403-2:
Toutes les mises-à-jour sont elles journalisées (exemple: utilisation d'un journal after), avec des procédures spécifiques de sécurité pour la conservation des supports et la restauration ?

Note (0 à 4) :

Observations :

❍ ***Accounting et suivi des accès***

Question 403-3:

Existe-t-il un "accounting" journalier des accès de tous les utilisateurs (consultation, MAJ) par application et par programme aux différents fichiers et éléments des bases de données contrôlé systématiquement par l'administrateur et donnant lieu à la tenue à jour systématique d'un journal de bord ?

Note (0 à 4) :

Observations :

❍ ***Chiffrement***

Question 403-4:

Utilise-t-on des techniques de chiffrement pour le stockage des fichiers et des archivages de données stratégiques ?

Note (0 à 4) :

Observations :

❺ La sécurité de l'exploitation

①Facteur 501 - Archivage-Désarchivage

❍ ***Procédures d'archivage***

Question 501-1-1:

Existe-t-il des procédures écrites concernant l'archivage/désarchivage (stockage et utilisation) spécifique à chaque type de support et tenant compte de la classification des informations ?

Note (0 à 4) :

Observations :

❍ ***Gestion des supports***

Question 501-1-2:

Existe-t-il un responsable de la gestion des supports utilisant un inventaire permanent avec compte-rendu périodique des entrées et sorties ?

Note (0 à 4) :

Observations :

❍ ***Transfert sécurisé des supports informatiques***

Question 501-2

En cas de transfert de données stratégiques sur support informatique, existe-t-il une procédure utilisant des conteneurs haute sécurité et des convoyeurs accrédités par l'entreprise ?

Note (0 à 4) :

Observations :

②Facteur 503 - Les sauvegardes

❍ ***Plan de sauvegarde***

Question 503-1

A-t-il été effectué une étude spécifique pour chaque fichier en fonction de ses caractéristiques (taux de mise à jour, périodicité d'utilisation, classification des informations, importance stratégique) et cette étude a-t-elle entériné la mise en place de règles strictes et détaillées par fichier, consignées dans un Plan de sauvegarde remis à jour systématiquement après chaque création ou modification d'application ?

Note (0 à 4) :

Observations :

❍ ***Procédures de sauvegarde***

Question 503-2

Réalise-t-on périodiquement ou de manière impromptue une relecture (échantillon cyclique) des sauvegardes des fichiers stratégiques en fonction de la périodicité de mise à jour, de la classification des contenus et de la qualité des supports ?

Note (0 à 4) :

Observations :

❍ ***Procédures de reprise et de restauration***

Question 503-3

Existe-t-il des procédures de reprise automatique des applications en cas d'interruption accidentelle de l'exploitation, notamment :

- procédures de reprise à chaud (points de reprise ou check point programmés et utilisation du journal image-avant)

- procédures de reprise à froid,

consignées dans un document écrit ?

Note (0 à 4) :

Observations :

②Facteur 504 - Le suivi de l'exploitation

❍ ***Procédures de recette en exploitation***

Question 504-1

Existe-t-il une procédure de mise en place et de validation de toute nouvelle application ou version du logiciel de base mise en exploitation qui précise la mise à disposition systématique au secteur d'exploitation :

- d'une documentation complète (présentation de l'application, JCL de tests, mécanismes et règles de sécurité, règles de sauvegarde des fichiers, etc.) ?

- des programmes objets (et éventuellement des sources) ?

Note (0 à 4) :

Observations :

❍ ***Lutte contre les sabotages immatériels***

Question 504-2

Dispose-t-on de procédures et de moyens de prévention, de protection et de détection de sabotages immatériels (bombes logiques, virus, ...) ?

Note (0 à 4) :

Observations : Ces mesures doivent être mises en action avant chaque chargement de fichiers en provenance de l'extérieur.

❻ La sécurité des études et réalisations

①Facteur 601 - Les procédures de recettes

❍ ***Procédures de recettes et de révisions***

Question 601-1

Existe-t-il des procédures de révision (protocoles de recette) appliquées systématiquement, avant la mise en exploitation, pour toute création ou maintenance d'une application s'appuyant sur un document cosigné par l'utilisateur et le chef de projet informatique ?

Note (0 à 4) :

Observations :

❍ ***Protocole de recette***

Question 601-2:

Le protocole de recette inclut-il :

- une présentation "études" de l'application pour l'exploitation,
- les jeux d'essais,
- les mécanismes de sécurité (droits d'accès, points de reprise),
- le dossier d'exploitation et les règles générales de sécurité à l'exploitation (y compris les règles de confidentialité),
- le régime de sauvegardes,
- le mode dégradé éventuel,
- des estimations en volumétrie (temps CPU, volumes fichiers,...).

Note (0 à 4) :

Observations :

Question 601-3

Le dossier utilisateur inclut-il le partage des responsabilités utilisateurs-informaticiens (contrôles, validations) et un dossier spécifique dans le cas des applications mettant en jeu des moyens autonomes connectés à l'ordinateur central ?

Note (0 à 4) :

Observations :

②Facteur 602 - Les méthodes de développement

❍ ***Méthodologies***

Question 602-1

La méthode de conduite de projet permet-elle d'intégrer les aspects sécurité à chaque phase d'avancement des projets (schéma directeur, étude préalable, étude détaillée) et permet-elle de définir une classification stratégique des données (pérennité, intégrité, confidentialité) objective en fonction de l'impact (risque maximum) qu'un sinistre touchant ces données aurait sur l'entreprise ?

Note (0 à 4) :

Observations :

❍ ***Documentation des applications***

Question 602-2

Existe-t-il une documentation par application opérationnelle structurée, claire et tenue à jour incluant :

- les schémas d'intégration (liaisons inter-applications),

- les schémas de circulation de l'information accompagnés de la liste des contrôles effectués,

- des tableaux croisés fichiers/programmes et données/programmes,

- les options organiques (ordinogrammes, dessins et chaînes, maquettes TP et états) ?

Note (0 à 4) :

Observations :

③Facteur 603 - Les contrôles programmés

❍ ***Poids stratégique des données***

Question 603-1

Y a-t-il eu au moment de l'étude préalable, une étude quantitative des conséquences d'accident, d'erreur ou d'action volontairement malveillante menée avec les utilisateurs et ayant permis le classement des données en fonction de leur "poids stratégique" ?

Note (0 à 4) :

Observations :

❍ ***Contrôles programmés***

Question 603-2

Chaque chef de projet a-t-il pour instruction, lorsqu'il élabore des contrôles sur des données stratégiques dans un programme de vérifier que ces contrôles soient reproduits dans tous les programmes utilisant cette donnée ?

Note (0 à 4) :

Observations :

Question 603-3

Pour les données stratégiques a-t-on conçu :

- des contrôles de base (cadrage, limite de valeur),

- des contrôles de vraisemblance directe (fourchette),

- des contrôles de vraisemblance indirecte (ratios),

- des contrôles de cohérence (évolution et comparaison par rapport à des données antérieures ou une base statistique) ?

Note (0 à 4) :

Observations :

Nom de la personne ayant rempli ce questionnaire	
Fonction	
Téléphone	

2-B RÉSEAU LOCAL

①Facteur 301 Environnement de base

❍ *Sécurité physique de base*

Question 301-A-1

*Dispose-t-on d'un **inventaire à jour** de tous les équipements (serveurs, stations, modems, multiplexeurs, concentrateurs, ponts, passerelles, etc.) avec leur emplacement et leurs connexions ?*

Note (0 à 4) :

Observations :

Question 301-B

*Les stations de travail sont-elles **dépourvues de lecteurs de disquettes** (ou l'accès en est-il physiquement interdit) ?*

Note (0 à 4) :

Observations :

②Facteur 302 Les contrôles d'accès physiques

Question 302-A

*Les serveurs sont-ils **sécurisés physiquement** et disposés dans des pièces fermées à accès contrôlé ?*

Note (0 à 4) :

Observations :

Question 302-B

Les bureaux renfermant des petits matériels et des supports informatiques ferment-ils à clé et sont-ils effectivement fermés à clé ?

Note (0 à 4) :

Observations :

③Facteur 307 Fiabilité de fonctionnement des matériels informatiques

❍ *Qualité du système*

Question 307-A

*Le choix de la configuration a-t-il reposé sur une **étude comparative** des caractéristiques en matière de sécurité menée par la direction informatique pour des raisons de **cohérence** (maintenabilité, portabilité, compatibilité, évolutivité, fiabilité, contrôle d'accès) ?*

Note (0 à 4) :

Observations :

④Facteur 308 - Les systèmes et procédures de secours

❍ *Plan de secours*

Question 308-3:

Existe-t-il un plan de secours reprenant l'exploitation éventuellement en mode dégradé et/ou éclaté (sur plusieurs sites) ainsi que des documents permettant le mise en oeuvre rapide des procédures de sauvetage ?

Note (0 à 4) :

Commentaire :

Le plan de secours doit inclure :

- ❍ la liste des médias et documents à protéger et à emporter en cas de sinistre,
- ❍ les procédures de reprise manuelles temporaires dans les services utilisateurs,
- ❍ les procédures de liaison avec les entités extérieures à l'entreprise,
- ❍ la gestion des ressources humaines,
- ❍ la réservation du site de secours,
- ❍ la restauration du système d'exploitation, du réseau et des fichiers,
- ❍ la relance primaire des applications,
- ❍ les processus post-reprise (commande de matériels, reconstitution du site...),
- ❍ les processus et planning de retour à la normale.

Observations :

Question 308-4:

Le plan de secours est-il remis à jour (évolutions matérielles et logicielles, configuration réseau,...) et sauvegardé périodiquement ?

Note (0 à 4) :

Commentaire :

Le plan de secours doit pouvoir, au moins pour les applications stratégiques, être mis en oeuvre à tout moment.

Observations :

❍ *Back up*

Question 308-5:

Existe-t-il une solution de back-up :

- *soit sur un site de secours strictement réservé au site étudié (salle redondante),*
- *soit par un système de secours contractuel avec un façonnier spécialisé incluant les règles de priorité d'utilisation, le mode de réservation, les délais de mise à disposition et les plages horaires de fonctionnement,*
- *soit un système de secours interne à l'entreprise ?*

Note (0 à 4) :

Commentaire :

Le différentes solutions à analyser n'ont pas la même valeur de sécurité :

- la solution de la salle redondante offre le maximum de sécurité si son niveau technique est maintenu "parallèle" au site de référence,
- la solution contractuelle chez un façonnier doit faire l'objet d'une analyse détaillée au niveau des engagements contractuels,

dans tous les cas, la disponibilité des moyens et leur adéquation aux choix stratégiques doit être vérifiée.

Observations :.

❍ *Réseau*

Question 308-6:

En cas de reprise du réseau, a-t-on effectué une étude spécifique, tenant compte de la sécurité sur le choix des liaisons entre le site de secours et le site étudié ?

Note (0 à 4) :

Observations :

Tests

Question 308-7:
La solution de secours est-elle complètement testée au moins 2 fois par an ?
Note (0 à 4) :

Observations :

⑤Facteur 309 - Cohérence des systèmes

Question 309-A

*Assure-t-on la **cohérence des systèmes répartis** les uns par rapport aux autres (matériels, logiciels de base, langages, progiciels, réseaux, etc.) ainsi que la cohérence et la compatibilité des systèmes répartis avec l'informatique centrale ?*

Note (0 à 4) :

Observations :

⑤Facteur 310 - Le personnel

Question 310-A

*Existe-t-il une sensibilisation et une information de l'ensemble des utilisateurs aux **problèmes de sécurité** et en particulier a-t-on réalisé un **guide de sécurité micro** ?*

Note (0 à 4) :

Observations :

⑥Facteur 311 - Plan de sécurité

❍ Plan de sécurité

Question 311-A

Le plan de sécurité des systèmes d'information couvre-t-il le domaine des micros (stand alone, fixes et portables) et les LAN (serveurs, ST, etc.) : analyse des vulnérabilités et des menaces, solutions, organisation de la sécurité ?

Note (0 à 4) :

Observations :

❍ *Architecture du réseau local*

Question 311-B

Le choix de supports, de topologie, de systèmes sont-ils adaptés au contexte d'utilisation ?

Note (0 à 4) :

Commentaires :

- Sauf si le LAN est peu étendu (< 1000 m), on devrait éliminer les supports de type paire torsadée,
- Si l'on a retenu une topologie en anneau (exemple Token Ring), on devrait limiter le nombre de noeuds actifs (< 250 sur fibre optique et <100 sur autre supports) et intégrer les risques de coupures,
- Si l'on recherche une grande disponibilité et si les noeuds sont peu éloignés on pourrait retenir une topologie en étoile (exemples: Starian, Arcnet, Novell Netware),
- Si l'on a retenu une topologie en bus (exemples: Ethernet, Arcnet, Token Bus), on doit tenir compte des risques de coupures et des extensions possibles (topologie arbre).

Observations :

⑦Facteur 401 - La sécurité logique de base

❍ *Contrôle d'accès*

Question 401-A

*Y a-t-il notamment un système d'**identification et d'authentification** par mot de passe - non trivial et à renouvellement contrôlé- pour chaque utilisateur ?*

Note (0 à 4) :

Observations :

⑧Facteur 402 - La sécurité des communications

Question 402-A

L'accès aux fonctions de communication *est-il restreint et soumis à une* ***procédure spécifique de contrôle d'accès*** *?*

Note (0 à 4) :

Observations :

Question 402-B

Toutes les fonctions d'exploitation du réseau (protocole local et protocoles d'interface) sont-elles gérées uniquement sur une ***console dédiée*** *et par le* ***seul administrateur*** *LAN ?*

Note (0 à 4) :

Observations :

Question 402-C

Toutes les communications, sans exception, transitent-elles ***obligatoirement*** *par le serveur ?*

Note (0 à 4) :

Observations :

Question 403-A

*Les **données confidentielles** stockées sont-elles **chiffrées** (ceci inclut les fichiers de mots de passe, de profils utilisateurs, d'audit, de pointeurs, etc.) ?*

Note (0 à 4) :

Observations :

⑨Facteur 501 - Archivage-Désarchivage

Question -501 A

*Existe-t-il des locaux et/ou armoires et/ou coffrets de sécurité permettant de **stocker les disquettes** micro dans des conditions de sécurité acceptables ?*

Note (0 à 4) :

Observations :

Question -501 B

*Les **disquettes originales** de progiciels (ainsi que les contrats de licence) sont elles stockées dans une armoire de sécurité ?*

Note (0 à 4) :

Observations :

①⓪Facteur 502 - Transfert classique de données

Question -502 A

*Existe-t-il des règles particulières pour les logiciels et les informations résidentes sur les **micros portables** hors de l'entreprise (interdiction de sortie de certaines données ou progiciels, et/ou chiffrement en cas de sortie) ?*

Note (0 à 4) :

Observations :

①①Facteur 503 - Sauvegardes

Question -503 A

*Y a-t-il au moins **une sauvegarde systématique** (périodicité adaptée à une reconstitution raisonnable) de l'ensemble des informations ?*

Note (0 à 4) :

Observations :

Question -503 B

Ces sauvegardes sont-elles à 2 niveaux, dont le second est stocké dans un local éloigné du local considéré et correctement protégé ?

Note (0 à 4) :

Observations :

Question -503 C

*Existe-t-il un système centralisé (serveur dédié) de sauvegarde ou, à défaut, existe-t-il un responsable chargé d'organiser et **de contrôler** les règles de sauvegardes ?*

Note (0 à 4) :

Observations :

①②Facteur 504 - Sécurité Générale

Question -504 A

*A-t-on défini des règles de **journalisation systématique** et sécuritaire, le contrôle étant centralisé et réalisé par l'administrateur LAN ?*

Note (0 à 4) :

Commentaires: Conserve-t-on et analyse-t-on les journaux (logs) qui reprendront notamment les informations suivantes :

- essais infructueux de log on,
- essais d'opérations non autorisées,
- arrêts intempestifs, délibérés ou accidentels,
- changement dans les fonctions de sécurité, changement de paramètres systèmes,
- trace des connexions, déconnexions,
- accès aux ressources stratégiques.

Question -504 B

*Les utilisateurs connaissent-ils les symptômes **des virus informatiques** et en déduisent-ils des prescriptions de détection et des mesures d'éradication ?*

Note (0 à 4) :

Observations :

①③Facteur 602 - Méthodes d'analyse-programmation

Question -602 A

*Chaque projet développé dans l'environnement micro est-il soumis au **strict respect** des **normes méthodologiques** (cahier des charges, programmation, protocole de recette,...) élaborées par la Direction des Systèmes d'Information ?*

Note (0 à 4) :

Observations :

Nom de la personne ayant rempli ce questionnaire	
Fonction	
Téléphone	

QUESTIONNAIRE 3 : Évaluation du coût de l'informatique

BUDGET INFORMATIQUE Année A-1

	Montants (kF)	Sous-totaux	Total (KF)
Frais de personnel permanent			
Études			
Exploitation			
Systèmes-Réseaux			
Administration			
Intérimaires			
Études			
Exploitation			
Infogérance, FM, SSII, ...			
Études			
Exploitation			
Systèmes-Réseaux			
Consultants			
Formation [67]			
Sécurité[68]			
Matériels			
Ordinateurs centraux			
Location simple			
Leasing			
Amortissements annuels			
Maintenance			
Ordinateurs départementaux			
Location simple			
Leasing			
Amortissements annuels			
Maintenance			

[67] en nombre de jours agents

[68] Cf. Note méthodologique

Micro-informatique			
Locations simples			
Leasing			
Amortissements annuels			
Maintenance			
Logiciels			
Locations			
Achats			
Amortissements annuels			
Maintenance			
Locaux professionnels[69]			
Achats et consultation de fichiers externes			
Télécommunications			
Automates, DAB - GAB			
Autres charges (à préciser)			
Refacturation de prestations (à déduire)			
TOTAL GÉNÉRAL			

[69] Surface occupée * valeur locative au m2

BUDGET INFORMATIQUE Année A-3

	Montants (kF)	Sous-totaux	Total (KF)
Frais de personnel permanent			
Études			
Exploitation			
Systèmes-Réseaux			
Administration			
Intérimaires			
Études			
Exploitation			
Infogérance, F.M., SSII			
Études			
Exploitation			
Systèmes-Réseaux			
Consultants			
Formation[70]			
Sécurité[71]			
Matériels			
Ordinateurs centraux			
Location simple			
Leasing			
Amortissements annuels			
Maintenance			
Ordinateurs départementaux			
Location simple			
Leasing			
Amortissements annuels			
Maintenance			

[70] en nombre de jours agents

[71] Cf. Note méthodologique

Micro-informatique			
Locations simples			
Leasing			
Amortissements annuels			
Maintenance			
Logiciels			
Locations			
Achats			
Amortissements annuels			
Maintenance			
Locaux professionnels[72]			
Achats et consultation de fichiers externes			
Télécommunications			
Automates, DAB - GAB			
Autres charges (à préciser)			
Refacturation de prestations (à déduire)			
TOTAL GÉNÉRAL			

Nom de la personne ayant rempli ce questionnaire	
Fonction	
Téléphone	

[72] Surface occupée * valeur locative au m2

BUDGET INFORMATIQUE - NOTE MÉTHODOLOGIQUE

❶ **L'établissement servira un tableau pour l'année A-1 et un tableau pour l'année A-3.**

❷ **Tous les montants seront servis Hors Taxes.**

❸ **Tous les postes budgétaires doivent strictement se rattacher à l'activité informatique liée à l'exploitation bancaire.**

Intérimaires : Tout personnel externe utilisé dans l'entreprise.

Consultants :
Facturation de travaux d'études générales (Audit, Organisation, Architectures techniques, choix stratégiques...) confiés à des cabinets spécialisés.

Formation :
Formation professionnelle des seuls agents de la Direction des Systèmes d'Information.
Cet indicateur est apprécié en nombre de jours/agents et en kF.

Sécurité :
Total du tableau -Dépenses consacrées à la sécurité informatique-.

Matériels :
Cet ensemble de postes doit recenser l'ensemble des matériels : informatique de production, informatique d'études et de développement, informatique décentralisée (réseaux locaux, ordinateurs départementaux, et systèmes déportés en agences).

Logiciels :
Ensemble des logiciels (système, exploitation, programmation...).

Locaux professionnels :
Valeur locative annuelle des surfaces utilisées par la Direction de l'Organisation et de l'Informatique pour l'informatique centralisée.

Télécommunications :
Facturation annuelle des frais liés à l'utilisation ou à la réservation (abonnements) des liaisons spécialisées.

Refacturation de prestations :
Ce montant déductible correspond aux factures émises en contrepartie de prestations de services informatiques à des entreprises externes à l'établissement de crédit.

Estimation des dépenses consacrées à la sécurité informatique

Type de dépense	Montant A-3 (en KF)	Montant A-1 (en KF)
ORGANISATION, AUDITS (poste de RSI, audits externes et internes)		
SÉCURITÉ PHYSIQUE (Environnement de base, contrôle des accès, détection et lutte contre la pollution, sécurité incendie, dégâts des eaux)		
PLANS ET MOYENS DE SECOURS (Back-up interne ou contractuel)		
SÉCURITÉ DES ACCÈS LOGIQUES (progiciels de contrôle d'accès : investissement, maintenance et gestion)		
SÉCURITÉ DES TÉLÉCOMMUNICATIONS (progiciels sécurité, coût de la redondance des unités de télécommunications et du maillage du réseau)		
SÉCURITÉ D'EXPLOITATION (Archivage, sécurisation des transferts de données, sauvegardes, outils d'automatisation, ...)		
SÉCURITÉ DES ÉTUDES ET RÉALISATIONS (coût de l'intégration de la sécurité dans les différentes phases de conduite de projet et dans les applications)		
AUTRES (à préciser)		
TOTAL		

Nom de la personne ayant rempli ce questionnaire	
Fonction	
Téléphone	

ASSURANCES : Grille harmonisée européenne[73]

Indiquer dans les cases des colonnes C1 à C6 les risques couverts et non couverts

Conséquences / Type de risques	Matériel C1	Non-Matériel C2	Frais supplémentaires et pertes d'exploitation C3	Pertes de patrimoine C4	Responsabilité civile C5	Divers C 6	PRIME ANNUELLE (kF)	FRANCHISE (kF)
ACCIDENTS								
A1 - Physiques (Incendie, Explosion, Dégâts des eaux, Pollution, etc.)								
A2 - Pannes								
A3 - Force majeure (événements naturels)								
A4 - Pertes de services essentiels (Télécom, électricité, eau, etc.)								
A5 - Autres								
ERREURS								
E1 - Erreurs d'utilisation								
E2 - Erreurs de conception et de réalisation								
MALVEILLANCE								
M1 - Vol (physique)								
M2 - Fraude								
M3 - Sabotage (physique)								
M4 - Attaque logique								
M5 - Divulgation								
M6 - Autres								

[73] Source CLUSIF

Nom de la personne ayant rempli ce questionnaire	
Fonction	
Téléphone	

QUESTIONNAIRE 4-A Appréciation de l'efficacité et de la performance opérationnelle de l'informatique

La Direction Informatique

Les effectifs

Servir le tableau de répartition fonctionnelle des effectifs suivant:
(Les personnels permanents, contractuels ou temporaires seront totalisés en nombre de jours agents)

Secteurs d'activités	Nombre (jours agents)
Études :	
Organisation :	
Analyse-programmation	
Système	
Micro-informatique	
Exploitation :	
Plateau	
Réseau	
Maintenance :	
Main-frames	
Réseau	
Micro-informatique	
TOTAL :	

Le rattachement hiérarchique

La Direction de l'Informatique est-elle directement rattachée à :

☐ la Direction Générale,
☐ la Direction Financière,
☐ la Direction Administrative,
☐ au Secrétariat Général,
☐ Autre (précisez) :_____.

Le Plan informatique

Année de réalisation du schéma directeur : 19 . .

Horizon du schéma directeur : 3ans 5 ans >5ans

Domaines couverts par le schéma directeur :
(Répondre **O**ui, **N**on ou **S**ans objet)

- ☐ Matériels de l'informatique centralisée,
- ☐ Informatique décentralisée (départementaux),
- ☐ Micro-informatique,
- ☐ Télécommunications,
- ☐ Méthodes et outils (AGL...),
- ☐ Infocentre,
- ☐ Télématique (Videotex, Audiotex, Internet...),
- ☐ Gestion des ressources humaines,
- ☐ Budgets,
- ☐ Plan de sécurité,
- ☐ Informatique de pilotage (tableaux de bord, OAD...),
- ☐ Autres (précisez) :_____.

Existe-t-il un Plan informatique formalisé ? ☐

Le Plan informatique est-il révisé annuellement ? ☐

Le Plan est-il contrôlé par un Comité de pilotage ? ☐

S'il existe un Comité de pilotage est-il composé du :

- ☐ Directeur Informatique,
- ☐ Directeur Général,
- ☐ Directeur Financier,
- ☐ Directeur Informatique,
- ☐ Directeur Commercial,
- ☐ Secrétaire général,
- ☐ Responsable Inspection,
- ☐ Responsable sécurité,
- ☐ Représentant(s) d'utilisateurs.

Les méthodes de développement :

Utilisez-vous **systématiquement** une méthode de développement ? ☐ **O/N**

Si oui, laquelle ?

- ☐ MERISE,
- ☐ AXIAL,
- ☐ SDMS,
- ☐ Autre (précisez) :_____.

Les outils de développement :

Utilisez-vous **systématiquement** des outils de développement ? ☐ **O/N**

Si oui, lesquels ?

- ☐ L4G,
- ☐ AGL,
- ☐ Générateur de code,
- ☐ outil de maquettage,
- ☐ Autres (précisez) :_____.

Le niveau de centralisation :

(Parts, exprimées en pourcentages, résidentes sur des systèmes informatiques centralisés)

⇨ Matériels : _____ %

⇨ Données : _____ %

⇨ Développements : _____ %

Les solutions informatiques

Quelle est la part des solutions informatiques (hors bureautique classique) apportées à travers :

(Évaluer en %)

⇨ Informatique classique : _____ %

⇨ Infocentre : _____ %

⇨ Micro-informatique : _____ %

L'informatique stratégique

Les cibles stratégiques :

Quels sont par ordre d'importance relative les cibles définies comme stratégiques de votre informatique (avantages concurrentiels par réduction des coûts, croissance et innovation, relations clientèle, maîtrise interne, produits de substitution, nouveaux entrants, etc.) ?

① _____

② _____

③ _____

④ _____

⑤ _____

Les choix technologiques :

Classez hiérarchiquement par ordre décroissant d'importance (1 pour le premier) les technologies de l'information :

- ❍ Autoroutes de l'information,
- ❍ Échanges de Données Informatisées (EDI),
- ❍ Liaisons PC-Mainframes, développements client-serveur,
- ❍ Internet, Minitel, videotex, audiotex,
- ❍ Messageries électroniques,
- ❍ Systèmes experts, I.A.,
- ❍ Autres (précisez) :_____

_____

Assistance extérieure

Quel est le budget annuel moyen (sur les 3 dernières années) consacré aux :

- ● Cabinets de consultants (Etudes) : _____ KF
- ● S.S.I.I. (Réalisations, ingénierie) : _____ KF
- ● S.S.I.I. (Facilities management) : _____ KF

Nom de la personne ayant rempli ce questionnaire	
Fonction	
Téléphone	

QUESTIONNAIRE 4-B Les critères d'appréciation des utilisateurs

Ce questionnaire pourra être reproduit et distribué à une série d'utilisateurs "privilégiés" du système d'information responsables de la mise en œuvre de décisions stratégiques. (Responsables de la trésorerie, de la salle de marchés, des secteurs opérationnels de l'activité guichet ou crédit...)

Notez de 0 à 10 votre appréciation du sujet suivant, en traduisant votre sentiment vis à vis du système informatique que vous utilisez :

❶ **Le système d'information :**

- **Fiabilité** : _____
- **Ergonomie, convivialité** : _____
- **Adéquation aux besoins** : _____
- **Sécurité** : _____
- **Intégration** : _____

❷ **Les équipes informatiques :**

- **Réactivité** : _____
- **Respect des délais et des budgets** : _____
- **Capacité à imaginer et gérer le changement** : _____
- **Facilité de communication** : _____
- **Compétence** : _____

Nom	
Qualité/Fonction	
Téléphone	

TABLE DES PONDÉRATIONS : Sites centraux

	FACTEURS DE SÉCURITÉ	Sites	Cumuls	Cumuls
	APPRÉCIATION GÉNÉRALE DE LA SÉCURITÉ DE L'ENTREPRISE			**125**
101	***Organisation générale***		30	
	Organigrammes hiérarchiques et fonctionnels	6,5		
	Comité sécurité	10		
	Étude vulnérabilité	6,5		
	Responsable sécurité	7		
102	***Contrôles permanents***		50	
	Propriétaire des informations	17		
	Choix des contrôles non informatiques	10		
	Qualité des contrôles non informatiques	13		
	Analyse spécifique des comptes sensibles	10		
103	***Réglementation et Audit***		45	
	Procédures générales	21		
	Archivage et sécurité des documents originaux	13		
	Audit informatique	11		
	FACTEURS SOCIO-ÉCONOMIQUES			**10**
201	***Facteurs socio-économiques***		10	
	Aspects socio-économiques	10		
	PRINCIPES GÉNÉRAUX DE LA SÉCURITÉ			**335**
301	***Environnement de base***		40	
	Sécurité des locaux informatiques	16		
	Protection périphérique	12		
	Sécurité des installations	12		
302	***Contrôle d'accès physique***		35	
	Protection et surveillance des salles informatiques	35		
303	***Pollution***		10	
	Les facteurs de pollution	10		
304	***Consignes de sécurité physique***		10	
	Élaboration et tests de consignes	10		
305	***Sécurité Incendie***		40	
	Étude spécifique et compartimentage	14		
	Détection automatique salles informatiques	13		
	Extinction automatique salles ordinateurs	13		

306	***Dégâts des eaux***		10	
	Étude spécifique	6		
	Évacuation de l'eau	4		
307	***Fiabilité de fonctionnement des matériels informatiques***		35	
	Redondance informatique	35		
308	***Systèmes et procédures de secours***		75	
	Études préliminaires	23		
	Plan de secours	22		
	Back-up	11		
	Réseau	8		
	Tests	11		
309	***Protocoles utilisateurs informaticiens***		30	
	Micro-informatique : choix et règles	15		
	Intégration de la sécurité dans les phases études	15		
310	***Personnel Informatique***		30	
	Déontologie	30		
311	***Plan de Sécurité***		20	
	Plan de sécurité	20		
	SÉCURITÉ DES MATÉRIELS ET LOGICIELS DE BASE			**155**
401	***Contrôle des accès logiques***		60	
	Système de contrôle des accès logiques	60		
402	***Sécurité des télécommunications***		70	
	Sécurité du réseau	28		
	Surveillance des lignes et transmissions stratégiques	42		
403	***Protection des données***		25	
	Administration des bases de données	9		
	Journalisation et sécurité des mises à jour	6		
	Accounting et suivi des accès	6		
	Chiffrement	4		
	SÉCURITÉ D'EXPLOITATION			**160**
501	***Archivage-Désarchivage***		20	
	Procédures d'archivage	10		
	Gestion des supports	10		
502	***Transfert sécurisé des supports***		15	
	Transfert sécurisé des supports	15		
503	***Sauvegardes***		80	

	Plan de sauvegarde	27		
	Procédures de sauvegarde	27		
	Procédures de reprise et de restauration	26		
504	***Suivi de l'exploitation***		45	
	Procédures de recette en exploitation	30		
	Lutte contre les sabotages immatériels	15		
	SÉCURITÉ DES ÉTUDES ET RÉALISATIONS			**150**
601	***Les procédures de recettes***		10	
	Les procédures de recettes et de révisions	4		
	Le protocole de recette	6		
602	***Méthodes Analyse-Programmation***		50	
	Méthodologies	25		
	Documentation des applications	25		
603	***Contrôles Programmés***		90	
	Poids stratégique des données	40		
	Contrôles programmés	50		
			935	**935**

TABLE DES PONDÉRATIONS : Réseaux locaux

	FACTEURS DE SÉCURITÉ	R.L.	Cumuls	Cumuls
	PRINCIPES GÉNÉRAUX DE LA SÉCURITÉ			**265**
301	***Environnement de base***		40	
	Sécurité physique de base	40		
302	***Contrôle d'accès physique***		35	
	Protection et surveillance des matériels informatiques	35		
307	***Fiabilité de fonctionnement des matériels informatiques***		35	
	Qualité du système	35		
308	***Systèmes et procédures de secours***		75	
	Plan de secours	25		
	Back-up	18		
	Réseau	15		
	Tests	17		
309	***Cohérence des systèmes***		30	
	Cohérence des systèmes	30		
310	***Personnel Informatique***		30	
	Guide de sécurité micro	30		
311	***Plan de sécurité***		20	
	Plan de sécurité	10		
	Architecture du réseau local	10		
	SÉCURITÉ DES MATÉRIELS ET LOGICIELS DE BASE			**155**
401	***Sécurité logique de base***		60	
	Système de contrôle des accès logiques	60		
402	***Sécurité des télécommunications***		70	
	Sécurité des communications	70		
403	***Protection des données***		25	
	Chiffrement	25		
	SÉCURITÉ D'EXPLOITATION			**145**
501	***Archivage-Désarchivage***		10	
	Procédures d'archivage_désarchivage	10		
502	***Transfert sécurisé des supports***		10	
	Transfert sécurisé des supports	10		
503	***Sauvegardes***		80	
	Procédures de sauvegarde	80		
504	***Sécurité générale***		45	
	Règles de journalisations	30		
	Lutte contre les sabotages immatériels	15		

	SÉCURITÉ DES ÉTUDES ET RÉALISATIONS			**50**
602	***Méthodes Analyse-Programmation***		50	
	Méthodologies	30		
	Documentation des applications	20		
			615	**615**

ANNEXE XI

RENSEIGNEMENTS PRATIQUES

- Bibliographie

- Adresses utiles

- Glossaire

BIBLIOGRAPHIE

- À la poursuite de dark avenger	DUNOD
- Antivirus mode d'emploi	SYBEX
- Comment protéger votre micro	MASON
- Danger pirates informatiques	CCC PLON
- Délinquance assistée par ordinateur	DUNOD
- Dossiers techniques du Clusif	CLUSIF Notamment : - La gamme méthodologique MARION (référence CLUSIF n° M-90.01) - La méthode MARION (présentation) (réf. M-90.02) - La méthode MARION 1994 (réf. M-94.01) - Les projets prioritaires post-schéma directeur (réf. M-92.01) - INCAS (présentation) (réf. M-92.03) - AROME (présentation) (réf. M-91.01) - MESSEDI 1994 (réf. M-94.03) - Méthode d'audit des réseaux locaux (réf. M-94.04) - Introduction à la sécurité informatique pour les petits et moyens systèmes (réf. TR-90.01) - Code d'éthique des métiers de la sécurité informatique (réf. D-91.02) - Les aspects humains de la sécurité informatique (réf. D-88.02)
- Droit de l'informatique	X Linant de Bellefonds et A Hollande Masson
- ITSEC : Information Technology Security Evaluation Criteria	Luxembourg: Office for official publications of the european communities
- La fraude informatique	Champy 2-903089-31-4
- Le nid du coucou	ALBIN MICHEL
- Numéro spécial	BANQUE STRATEGIE n° 103 (février/mars 1994)
- Les infections informatiques	CLUSIF
- Les principes de la sécurité informatique. Guide d'audit de l'IFACI	IFACI. CLET Editeur 27 bld de Port-Royal 75013 Paris (1990)
- Les virus, méthodes et techniques de sécurité	DUNOD
- PROTECTION DES SYSTÈMES D'INFORMATION Qualité et sécurité informatique	Les référentiels Dunod DUNOD SA RCS Paris B 316 053 628 15, rue Gossin 92543 Montrouge CEDEX
- Recueil des conférences SECURICOM 94	M.C.I 6, rue de l'Isly 75008 Paris
- Risks in computer and telecommunication systems	BRI/BIS (juillet 1989)

- Secure Computing (ex Virus News International)	+ 44 792 324 000
- Security and reliability in electronic systems for payment	BRI/BIS (1982 ; 1985)
- Sécurité informatique et virus	EYROLLES
- SOS données	DUNOD
- TRIBUNIX	Bulletin de liaison de l'association française des utilisateurs d'unix et des systèmes ouverts E-MAIL : tribunix@afuu.fr
- Virus Bulletin	Contact France (1) 43 74 42 24
- Virus, la maladie des ordinateurs, Micro-application	Burger 1989, 2-86899-186-6

ADRESSES UTILES

AFCET	Association française des sciences et technologies de l'information et des systèmes (ex Association française pour la cybernétique économique et technique) 156, boulevard Pereire 75017 Paris
AFIN	Association française des informaticiens[74] 54, rue Saint Lazare 75009 Paris
AFNOR	Association Française de Normalisation Tour Europe 92049 Paris la Défense
AFUU	Association Française des Utilisateurs d'Unix et des systèmes ouverts 11, rue Carnot 94270 Le Kremlin-Bicêtre
APP	Agence pour la protection des programmes 119, rue de Flandre 75019 Paris
CCETT	Centre commun d'études de télédiffusion et de télécommunication 4, rue du Clos Courtel 35512 Cesson Sévigne
CFONB	18, rue la Fayette 75009 Paris
CIGREF	Club informatique des grandes entreprises françaises 21, avenue de Messine 75008 Paris
CLUSIF	Club de la sécurité informatique française 26, boulevard Haussmann 75009 Paris. Association loi de 1901
CNIL	Commission nationale informatique liberté 21, rue saint Guillaume 75007
DISSI	Délégation Interministérielle pour la Sécurité des Systèmes d'Information 3, Avenue Octave Gréard 75007 Paris
FORUM	Forum des Compétences 34 boulevard Haussmann 75009 Paris Tél. : 43.44.29.29 ; Fax : 43.44.30.44
SAFICO	Service des Autorisations Financières et Commerciales 42, rue de Clichy 75436 Paris CEDEX 09 (demande de licence d'exportation de moyens de cryptologie)

74 Association en sommeil.

SCSSI	Service Central de la Sécurité des Systèmes d'Information 18, rue Docteur Zamenhof 92131 ISSY-LES-MOULINEAUX CEDEX (déclaration de fourniture ou d'utilisation de moyens de cryptologie)

GLOSSAIRE

APSAD
Assemblée Plénière des Sociétés d'Assurance Dommages

Classification
Attribution, à un élément du système d'information, d'un niveau de sécurité pour chacun des facteurs Disponibilité (D), Intégrité (I), Confidentialité (C) et Possibilité de contrôle et de preuve (P)

CLUSIF
Club des Utilisateurs de la Sécurité de l'Information en France

Confidentialité (C)
Propriété qui assure la tenue secrète des informations avec accès aux seules entités autorisées.

CPI
Chef de Projet Informatique, responsable du projet pour la maîtrise d'œuvre.

CPU
Chef de Projet Utilisateur, responsable du projet pour la maîtrise d'ouvrage.

Critique
Niveau d'un risque qui entraînerait des pertes financières, commerciales et organisationnelles importantes, voire inacceptables, ou des préjudices majeurs d'ordre judiciaire, et qui obligerait à prévoir des mesures de sécurité.

DICP
Facteurs de risques : Disponibilité, Intégrité, Confidentialité, Possibilité de contrôle et de preuve.

Disponibilité (D)
Aptitude des systèmes à remplir une fonction dans des conditions pré définies d'horaires, de délais, de performances.

Faible
Niveau d'un risque qui n'entraînerait pas de pertes importantes, et que l'on pourrait assumer.

GLS
Gestionnaire Local de la Sécurité
Les GLS sont spécialisés dans un domaine technique, par exemple : grands systèmes (IBM, autres), OMF (ordinateurs multi-fonctions), micro-informatique.

INCAS
Intégration, dans la Conception des Applications, de la Sécurité.

Intégrité (I)
Propriété qui assure que des informations sont identiques en deux points, dans le temps et dans l'espace.

ITSEC
Information Technology Security Evaluation Criteria

MARION

Méthode d'Analyse des Risques Informatiques Organisée par Niveaux (CLUSIF)

MELISA
Autre méthode d'analyse du risque (CF6)

Menace
Relation entre, d'une part, un événement d'origine naturelle, accidentelle ou volontaire et, d'autre part, un élément du système d'information susceptible d'en subir les atteintes.

MESSIE
Méthode destinée aux Etudes pour la prise en compte de la Sûreté -sécurité + qualité- dans les Systèmes d'Information de l'Entreprise

Mesure de prévention
Mesure de sécurité qui agit sur la probabilité d'un sinistre
Exemples de mesures de prévention : organisation, qualité, contrôle des accès, chiffrement.

Mesure de protection
Mesure de sécurité qui agit sur l'impact d'un sinistre
Exemples de mesures de protection : scellement, backup, audit.

Mesure de sécurité non standard
Mesure de sécurité qui ne figure pas dans le Guide de sécurité de l'information de l'établissement.

Modèle sécurisé
Modèle (MCC, MCT, MCD...) dont on a analysé les risques, auxquels on ajoute une classification sous forme "DnInCnPn". Les noms des entités comportant des risques majeurs sont libellés en italique.

Contrôle et preuve (P)
Faculté de vérifier le bon déroulement d'une fonction.
Non répudiation : impossibilité pour une entité de nier avoir reçu ou émis un message.

PSOI
Pôle de compétence Sécurité de l'OI (ou DSI)

Risque informatique
Probabilité d'atteinte au système d'information, selon un certain impact et avec des conséquences plus ou moins importantes.

Risque majeur
Risque de niveau sensible, critique ou stratégique.

RSM
Responsable Sécurité du Métier

RSSI
Responsable de la Sécurité des Systèmes d'Information

SCSSI
Service Central de la Sécurité des Systèmes d'Information (À la Défense Nationale)

SDSI
Service de Sécurité de l'Information ; peut être le nom de la petite équipe qui travaille directement sous les ordres du RSSI.

Sécuriser un modèle
Analyser les risques concernant les entités représentées par un modèle.

Sensible
Niveau d'un risque qui entraînerait des pertes financières, commerciales et organisationnelles significatives, ou des préjudices mineurs d'ordre judiciaire, et qui obligerait à prévoir des mesures de sécurité.

SGBD
Système de Gestion de Bases de Données

Stratégique
Niveau d'un risque qui entraînerait la perte d'une activité de la Banque, ou des poursuites judiciaires à l'encontre d'un haut responsable de la Banque, et qui obligerait à prévoir des mesures de sécurité.

Tâche ISM
Unité de travail visant à traiter l'une des fonctions d'ISM : analyse de risques, étude de mesures de sécurité, bilan économique sécurité, etc.

TCSEC
Trusted Computer Security Evaluation Criteria

Valorisation des risques
Évaluation du coût d'un scénario de risque, en kF, en mois/hommes, ou sous forme qualitative.

Vulnérabilité
État des éléments du système d'information soumis à des menaces

Vulnérable
Appellation globale s'appliquant aux risques de niveau sensible, critique ou stratégique.

ANNEXE XII

LISTE DES PARTICIPANTS

Ont participé au groupe de travail et apporté une contribution active à la rédaction de cet ouvrage :

M. Patrick BRUGUIER	Banque de France / Contrôle Général - RSI
M. Alain DEQUIER	Banque de France / Secrétariat général de la Commission bancaire - SIGD
M. Jean-Rémi FANGET	Banque de France / Inspection générale - Cabinet
M. Pierre-Yves THORAVAL[75]	Banque de France / Secrétariat général de la Commission bancaire - Direction de la Surveillance générale et de l'analyse du système bancaire

Forum des Compétences

M. Michel BOURGOGNE	Crédit Lyonnais
M. François GAUDICHEAU	Banque Hervet
M. Wilfrid GHIDALIA	Forum des Compétences / Live
M. Bernard LOISELEUR	Lyonnaise de Banque
M. Bertrand de LA RENAUDIE	Banque Indosuez
M. Claude VOISIN	Société Générale

75 Coordinateur du projet.

TABLE DES MATIÈRES

page

PRÉAMBULE **5**

Historique 5

Raisons de ce Livre blanc 5

Philosophie : "a best practice paper" 5

Mini-questionnaire destiné aux responsables 7

I - CONSTATS **9**

1. L'informatique : une menace spécifique pour les banques 9
2. Une menace financière réelle 10
3. Quelques exemples concrets des menaces dues aux systèmes d'information 12

II - LES OUTILS DE MESURE DU RISQUE **15**

1. Un exemple : l'enquête menée par le SGCB en 1992 15
   a. une enquête pour servir de base de référence 15
   b. un impératif : sensibiliser au plus haut niveau 15
   c. un mini-questionnaire : soixante-cinq questions pour cerner la sécurité 16
   d. évaluer les contraintes (budgétaires, d'assurances) 19
   e. apprécier la satisfaction des utilisateurs et le niveau d'efficacité/qualité de l'informatique 19
   f. conclusion : au total, une sécurité informatique globalement satisfaisante, mais perfectible 20
2. Une méthode formalisée de mesure du risque : quelques conseils 21
   a. connaître ses risques 21
   b. classer ses informations en fonction des quatre facteurs de sécurité DICP 23
   c. évaluer son risque maximal tolérable (RMT) 25
   d. classer ses informations entre stratégiques et non-stratégiques (échelle d'évaluation de l'impact des risques) 26
   e. mesurer ses faiblesses (mini-questionnaire MARION) 28
   f. comment arbitrer entre les priorités ? 28

III - LES PARADES POSSIBLES **33**

Les trois niveaux de réponse 33

1. Niveau 1 : réduire les faiblesses découvertes 33
2. Niveau 2 : passer d'une réponse "coup par coup" à une réponse organisée 33
   a. désigner un RSSI, faire un SDSSI 33
   b. les cinq conditions de sa réussite 34
3. Niveau 3 : agir en prévision des risques nouveaux 35

IV - RECOMMANDATIONS ("best of") **37**

1. pour les RSSI 38
2. pour les dirigeants responsables 39
3. Les points de sécurité les plus importants 40

CONCLUSION **41**

Le risque informatique est une des composantes du risque global de la banque. 41

Il doit donc être mesuré, surveillé, géré, réduit au mieux. 41

La Direction générale en est, elle aussi, in fine, responsable. 41

Ceci est faisable. 41

Il est fortement suggéré aux établissements de crédit de s'inspirer des recommandations contenues dans ce Livre blanc. 42

Transformer la diminution du risque en arme commerciale. 42

Vers un "rating du niveau de sécurité informatique" ? 42

La constellation du risque bancaire 43

LISTE DES ANNEXES

ANNEXE I :	Lettre envoyée par le Secrétaire général de la Commission bancaire aux Présidents des Etablissements de crédit	49
ANNEXE II :	Textes réglementaires	53
ANNEXE III :	Questionnaire simplifié (mini-Marion) ; matrice de pondération et tableaux de résultats	59
ANNEXE IV :	Fiches-conseils ; 36 fiches-conseils, par types de risques, classées par ordre alphabétique.	103
ANNEXE V :	Les risques, les facteurs de sécurité et les méthodes d'analyse du risque (un exemple)	217
ANNEXE VI :	La prise en compte de la sécurité dans les applications	233
ANNEXE VII :	Exemple de charte de la sécurité de l'information	237
ANNEXE VIII :	Le RSSI : responsable de la sécurité des systèmes d'information ; sa fonction	245
ANNEXE IX :	Méthodes utilisables par le RSSI	247
ANNEXE X :	Nouveau questionnaire	253
ANNEXE XI :	Renseignements pratiques	325
	- éléments bibliographiques	327
	- adresses utiles	329
	- glossaire	331
ANNEXE XII :	Liste des participants au groupe de travail sur le Livre blanc	335

Directeur de la publication :

Jean-Louis Butsch
Secrétaire général de la Commission bancaire

_____

Réalisation : Atelier de reprographie du SGCB
et SMI Banque de France

Dépôt légal : 1er trimestre 1996

ISBN 2-9505164-6-7

Prix TTC : 150 F