C.O.O.M.A.I. une démarche d'audit de la sécurité informatique

Ridha Zarrouk

Comptabilité et stratégie
Chapitre 8 - Stratégie d'audit et contrôle de l'entreprise

C.O.O.M.A.I. une démarche d'audit de la sécurité informatique

Ridha Zarrouk
Université de Rennes I, I.G.R.

INTRODUCTION

Guidées par un souci de productivité et de compétitivité, les entreprises s'informatisent de plus en plus; malheureusement, souvent, dans la précipitation. La sécurité, non génératrice de bénéfices, est reléguée au second plan et traitée au coup par coup.

Une telle attitude est périlleuse. Les risques informatiques sont divers. Leurs conséquences, tant techniques que financières, peuvent compromettre la survie de l'entreprise à défaut d'une réflexion-sécurité à la racine.

Cette réflexion passe à la fois

*) par une sensibilisation des différents acteurs de l'entreprise aux conséquences et aux particularités de ces risques et;

*) par l'élaboration d'une démarche d'audit de la sécurité informatique.

L'auditeur [1] peut jouer un rôle important à la fois en tant que conseiller et en tant qu'utilisateur des informations financières. Il lui appartient de dégager les grandes lignes d'orientation de sa mission tant au niveau du contrôle interne que celui des comptes.

---

1) Il s'agit bien sûr de l'auditeur financier. Nous retenons ce terme dans son sens le plus large. Il désignera l'auditeur interne ainsi que l'auditeur externe chargé d'une mission contractuelle ou légale.

1 BASES DE SENSIBILISATION :

L'appui de la Direction Générale à un projet quelconque est, généralement, interprété par le personnel, à tous les niveaux, comme une autorisation de collaboration. L'auditeur exploitera cette piste tout en élargissant son champ, dans un 2ème temps, aux personnels informatique et utilisateur.

11 sensibilisation de la Direction Générale :

L'accent sera mis sur les spécificités des risques, sur leurs conséquences et éventuellement sur le coût estimé d'un tel projet. Cette présentation sera émaillée de cas réels[2] et de statistiques se rapprochant du contexte de l'entreprise.

111) CARACTERISTIQUES DES RISQUES INFORMATIQUES :

A) DIVERSITE :

Ils vont du simple risque matériel accidentel (incendie, innondation...) à des actes malveillants (vol, sabotage...) passant par des pannes, des erreurs...

B) PARTICULARITES :

(1) Sinistralité en croissance :

types de sinistres	chiffres 1989 [3]		variation 88/89 en %
	nbre	coût	
malveillance	1 800	4,3	+10,2
accidents	11 900	2,5	+ 6,1
erreurs	19 000	1,8	- 2,6
coût total		8,6	+ 5,0

coût en milliard de francs

2) voir CNCC : "Les contrôles dans les entreprises informatisées." Tome 1.

3) ROHEC, C. : "La sécurité informatique en 1990", point de vente n°386 du 15/05/90 p.66.

(2) émergence d'une nouvelle race de criminels : Les délinquants informatiques présentent par rapport aux catégories traditionnelles de la criminologie une personnalité atypique[4]. Ne semblent pas obsédés par l'argent et souvent ne tirent aucun avantage matériel de leurs actes, plaident volontairement coupables si jamais ils sont démasqués. Certains s'empressent même de signaler à leurs victimes les défaillances de leurs systèmes et de se vanter[5].

Leurs mobiles sont d'ordre intellectuel : ils cherchent à montrer leur supériorité sur l'ordinateur et sur les programmeurs qui ont conçus les programmes de sécurité.

(3) clandestinité[4] de la criminalité informatique : une grande partie des fraudes est découverte par hasard.

(4) unicité de compétence[6] : les informaticiens disposent encore d'une grande latitude pour pourvoir au développement et à la maintenance des applications ainsi qu'à la gestion du système malgré l'intérêt qu'accordent les entreprises à la formation des utilisateurs.

La maîtrise des différents aspects informatiques qui les caractérise ainsi que la concentration de la compétence sur quelques personnes représentent une source de risques (appât de gain, défi intellectuel, vengence...), souvent latents.

112) CONSEQUENCES D'UN SINISTRE INFORMATIQUE :

a) conséquences techniques :

Sur ce plan, un sinistre informatique peut :

(1) entrainer une paralysie totale ou partielle du système pour une ± longue durée et/ou;

---

4) BISMUTH, Y.: "Criminalité informatique." EXPERTISES DES SYSTEMES D'INFORMATION, n°111, NOV.88.

5) BELLERET, R.: "Une passion criminelle pour l'informatique." LE MONDE, 2 MARS 1989, p.11.

6) IFACI : "Les principes de la sécurité informatique." CLET 1990.

(2) porter atteinte aux caractères confidentiel, authentique et à l'accessibilité des données.

b) conséquences financières[7] :

Sur le plan financier, il engendre :

(1) des coûts supplémentaires pour remettre en état le système ou assurer la continuité de l'exploitation;

(2) des manques à gagner;

(3) des pertes de fonds.

c) autres :

Un sinistre informatique peut provoquer des conséquences qualitatives difficilement chiffrables (perte de monopole, détérioration de l'image de marque...).

113) SINISTRALITE INFORMATIQUE :

Plusieurs organismes[8] tiennent des statistiques, répertorient des cas de sinistres déclarés et procèdent à une estimation pour se rapprocher de la réalité.

En effet, pour diverses raisons (image de marque...), plusieurs entreprises préfèrent garder secrète l'atteinte qu'ont subie leurs systèmes et ne pas réclamer une réparation ni poursuivre en justice les délinquants.

---

7) J.M.LAMERE les a regroupé dans quatre catégories
1. dommages matériels et annexes
2. frais supplémentaires et pertes d'exploitation
3. pertes de fonds et divers
4. autres pertes
J.M.LAMERE : "La sécurité informatique." Dunod informatique, Bordas 1985.

8) APSAIRD : Assemblée Plénière des Sociétés d'Assurance Incendie et Risques Divers.
CLUSIF : CLUb de la Sécurité Informatique Français.

Dans la mesure du possible, l'auditeur choisira les chiffres ainsi que les cas qui se rapprochent le plus du contexte de l'entreprise (son activité et sa taille, l'importance et l'ancienneté de son centre informatique...); en voici quelques statistiques :

*) 8,6 **milliards de Francs** de pertes financières dues à la sinistralité informatique pour la seule année 1989, soit une progréssion de 5% par rapport à 1988[9]. Chiffre sous-estimé d'après certains experts et assureurs[10].

*) ***44 sinistres de + de 10 millions de*** Francs et ***4 de plus de 100 millions*** ont été recensés en 1989[9].

*) **80 % des entreprises** victimes de sinistres informatiques majeurs disparaissaient dans les cinq années suivantes[10].

*) **8,3% seulement des entreprises** étaient entièrement couvertes par des contrats d'assurance[10].

*) **30,2 % des entreprises** n'ont aucun contrat spécifique à l'informatique[10].

*) **20 % des entreprises interrogées** ne pourraient poursuivre leurs activités que ***quelques heures et 46% quelques jours*** sans l'appui de leurs systèmes informatiques[11].

*) **Une entreprise sur trois, au moins,** a déjà été victime d'un incident sur son système informatique ***entrainant une interruption de service et une perte moyenne de 350 000*** Francs[11].

---

9) ROMEC, C., opcit.

10) LEIGH, F. : "Informatique : couvrez-vous !" SCIENCES ET VIE ECONOMIE, N° 57, JANVIER 1990 p.68-70.

11) Enquête menée par "CABINET ARTHUR YOUNG" auprès de 490 grandes entreprises européennes (le Monde du 18/04/89; p.76 et s.).

114) COUT DE LA SECURITE INFORMATIQUE :

Il se compose de deux éléments :

A) COUT DES ACTIONS CORRECTIVES :

Contrairement à ce que nous pouvons penser, les dépenses en matière de sécurité informatique sont importantes. Malheureusement, parfois, mal positionnées pour permettre d'atteindre un niveau suffisamment cohérent de la sécurité; ce qui laisse penser qu'elles relèvent plutôt d'actions ponctuelles que d'une approche globale d'autant plus que les statistiques de l'APSAIRD de 1986 à 1988 pour un même échantillon montrent une faible amélioration de la note moyenne alors que les notes des différents facteurs de sécurité ont conservé une forte hétérogénéité[12].

L'audit de la sécurité informatique a plus de chance d'aboutir à un meilleur positionnement des dépenses qu'à une importante augmentation de ces dernières.

B) COUT DE LA REALISATION DE L'AUDIT :

Par référence à des cas semblables, l'auditeur estimera ce coût.

*) Si l'audit est réalisé par un auditeur interne, il correspondra aux coûts spécifiques rattachés à ce projet.

*) Si l'audit est réalisé par un auditeur externe, il dépendra, essentiellement de la taille de l'entreprise, de ses équipements informatiques et de leur répartition géographique[13].

---

12) FAURIE,S. : "L'audit informatique : une nécessité tant pour l'entreprise que pour l'auditeur financier." ECONOMIE et COMPTABILITE, n°176, sept.91, p.27.

13) FAURIE estime que "le coût d'un audit de la fonction informatique sera généralement inférieur à 30 000 F, dans une entreprise exploitant un mini-ordinateur et disposant de trois informaticiens." opcit., p.17.

12) SENSIBILISATION DES PERSONNELS INFORMATIQUE ET UTILISATEUR

Fort de l'appui et de l'adhésion de la Direction Générale à son projet, l'auditeur entamera la sensibilisation des personnels informatique et utilisateur.

L'objectif est de s'assurer de leur collaboration. Il insistera sur l'importance qu'il y accorde.

Certains des éléments cités dans le § 11 peuvent être utilisés avec profit. Ils doivent être rapprochés du contexte et de l'activité de chacune des catégories.

121) PERSONNEL INFORMATIQUE :

Lors d'une réunion avec toutes ses catégories (programmeurs, analystes, études, exploitation...), l'auditeur :

*) donnera un aperçu général sur la sinistralité informatique (statistiques, cas réels...);

*) insistera sur l'importance du rôle que joue l'informatique dans la réalisation de l'activité de l'entreprise (degré d'informatisation, rapport temps traitement réel / temps traitement différé...) et sur l'intérêt d'une approche globale de la sécurité informatique;

*) exposera la politique de l'entreprise en matière d'informatisation (passage de certaines applications d'un traitement en temps différé à un traitement en temps réel, informatisation de certaines applications, acquisition de nouveaux matériels...).

Il précisera que son objectif n'est nullement d'évaluer leur performance mais d'apprécier la sécurité du centre.

122) PERSONNEL UTILISATEUR :

L'auditeur organisera des réunions par catégorie homogène d'utilisateurs (facturation, paie, recouvrement...) lors desquels il fournira un aperçu sur la sinistralité informatique en mettant l'accent sur les chiffres ou cas réels proches de l'activité du groupe.

CONCLUSION 1

La sensibilisation des différents acteurs constitue la première condition pour réussir la mise en oeuvre d'une démarche d'audit de la sécurité informatique (objet du 2) notamment dans les PME[14].

Elle se traduit par l'implication et l'appui de la Direction Générale ainsi qu'une collaboration des personnels informatique et utilisateur.

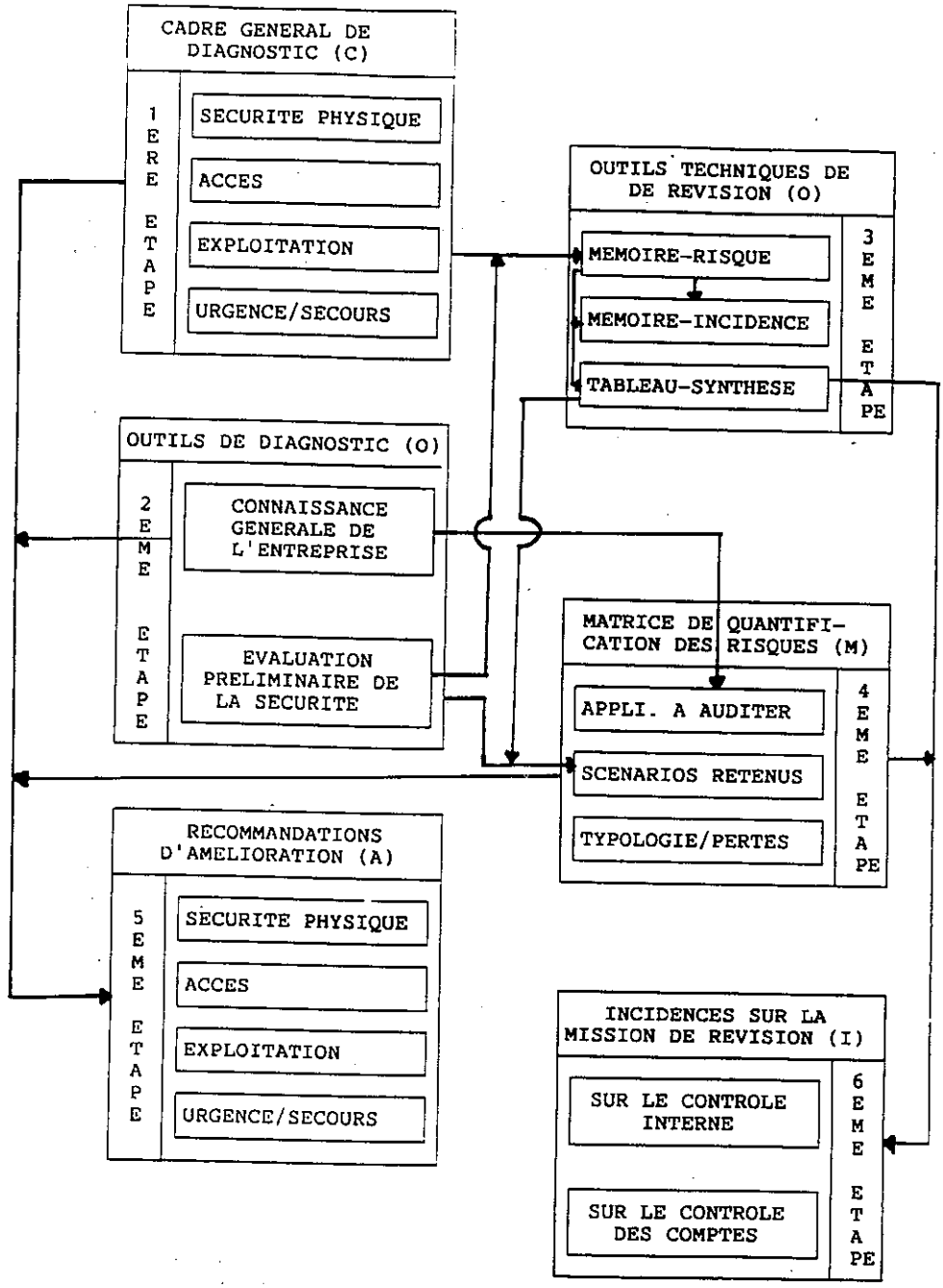
Le temps à lui consacrer doit être conséquent.

Nous pensons que tout désir d'économie à ce niveau ne peut qu'être préjudiciable à la bonne réalisation de l'audit.

La deuxième condition étant une bonne connaissance générale de l'entreprise. Elle prend toute son importance lorsque l'audit est réalisé par un intervenant externe.

---

14) Au niveau des PME, contrairement aux grandes entreprises qui font souvent l'objet d'audits informatiques en raison de leur forme juridique ou de leur organisation (service audit interne...), l'audit de la sécurité informatique est tributaire de la volonté des dirigeants.



NOTRE DEMARCHE D'AUDIT : COOMAI

2 PROPOSITION D'UNE DEMARCHE D'AUDIT [15] DE LA SECURITE INFORMATIQUE (C.O.O.M.A.I.) [16] :

La démarche d'audit[17] que nous proposons intègre à la fois l'aspect quantitatif et qualitatif de l'évaluation. Elle se base sur des Outils Techniques de Révision liés permettant une progression logique avec une synthèse à l'issue de chaque étape et à la base de chaque appréciation. Son objectif est double :

1°) déterminer le coût maximum de la non-sécurité[18]; information importante, à notre avis, pour inciter les responsables à mettre en oeuvre des actions correctives.

2°) jalonner les grandes lignes de la finition de la mission de révision comptable[19].

La décomposition et l'ordonnancement des travaux à effectuer, au niveau de chaque étape, optimisent la durée de leur exécution et facilitent leur mise en oeuvre du fait d'une part implicite d'automatisation.

21) PREMIERE ETAPE : CADRE GENERAL DE DIAGNOSTIC (C)[20] :

Le champ d'investigation est structuré en domaines au sein desquels les éléments vulnérables seront identifiés et les risques ainsi que leurs conséquences probables seront précisés. Nous avons retenu quatre domaines :

*) sécurité physique.
*) accès.
*) exploitation.
*) mesures d'urgence et/ou de secours.

---

15) Elle a fait l'objet d'un mémoire d'expertise comptable soutenu enfévrier 1992.

16) COOMAI : les six premières lettres des six étapes qui composent cette démarche (voir ci-contre).

17) La sensibilisation et la bonne connaissance de l'entreprise constituent des préalables à sa mise en oeuvre.

18) ou de l'insuffisance de la sécurité.

19) que cette mission soit réalisée par un auditeur interne ou externe. Certaines spécificités devront être, cependant, parfois, précisés.

20) voir annexe n°1; ce cadre peut être utilisé, avec profit, lors de la sensibilisation des différents acteurs de l'entreprise.

22) DEUXIEME ETAPE : OUTILS DE DIAGNOSTIC (O) :

Le diagnostic de la sécurité informatique vise :

(1) ***à apprécier*** l'adéquation des mesures envisagées aux menaces probables et;

(2) ***à identifier*** les risques qu'encourt l'entreprise.

Pour ce faire, l'auditeur peut adopter :

*) une ***méthode classique*** à base de questionnaire privilégiant ***l'aspect physique*** de la sécurité;

*) ou une ***méthode faisant appel à des techniques informatiques*** mettant l'accent beaucoup plus sur son ***aspect logique.***

Ces deux méthodes requièrent ***deux niveaux de compétence***. Elles ne sont pas exclusives. Elles sont plutôt complémentaires. L'auditeur doit dans la mesure du possible analyser la sécurité sous ces deux aspects.

221 METHODE CLASSIQUE DE DIAGNOSTIC :
(plutôt aspect physique et général de la protection)

L'auditeur se basera à la fois sur :

*) sa connaissance générale de l'entreprise[21] et;

*) sur un ***questionnaire***[22] qu'il administre aux responsables informatiques. Il doit couvrir tous les domaines concernés par la sécurité.

---

21) pour un auditeur externe il s'agira de toutes les informations qu'il a acquises lors de ses précédentes interventions (dossier permanent, rapports, entretiens non directifs de tous les intervenants : informaticiens, utilisateurs, direction générale, staff...).

22) L'APSAIRO a proposé un questionnaire fermé comportant 74 questions recouvrant 27 facteurs de sécurité. Une note allant de 0 à 4 sera affectée à chaque réponse (OUI = 4, NON = 0). La note obtenue sera ensuite pondérée par un coefficient. Ce questionnaire a été utilisée dans le cadre de la méthode MARION-AP.

Un triple objectif doit être atteint :

1) **DESCRIPTION** : parvenir à une appréhension globale du système (tâches, applications, architecture...);

2) **FCAE** : identifier les Facteurs Clès de l'Activité de l'Entreprise;

3) **FORCES ET FAIBLESSES** : relever les points forts et les points faibles des mesures de sécurité envisagées ou mises en oeuvre.

L'aspect physique de la protection peut être apprécié par *un généraliste* ayant des connaissances en informatique. Il s'agit d'une investigation menée *autour de l'ordinateur* [23].

222 METHODES DE DIAGNOSTIC BASEES SUR DES TECHNIQUES INFORMATIQUES

(plutôt aspect logique de la protection)

L'auditeur peut compléter son diagnostic à l'aide de *l'outil informatique*. Il s'agit, essentiellement, de s'assurer

(1) de la *validité* des mesures de protection des accès logiques;

(2) et de *l'inexistence d'altérations* des programmes.

Il pourra :

*) *utiliser des jeux d'essai;*

*) *simuler des tentatives d'accès illicites* et vérifier l'état de contrôle;

*) *utiliser des progiciels d'interrogation* de fichiers.

L'appréciation de cet aspect nécessite l'intervention *d'un spécialiste*. Il s'agit d'une *investigation à travers l'ordinateur*[23] qui *se justifie, notamment, si certaines réponses au questionnaire laissent présager un certain manque de rigueur* dans les mesures de protection des accès logiques.

---

23) voir CNCC : "Les contrôles dans les entreprises informatisées". Tome III, juillet 81, p.11.

23 TROISIEME ETAPE : OUTILS TECHNIQUES DE REVISION (O) :

L'objectif est de parvenir à une évaluation qualitative de la sécurité informatique à partir d'un traitement progressif des résultats obtenus lors de l'étape précédente.

231 MEMOIRE-RISQUE (MR) : IDENTIFICATION DES RISQUES :

Ces mémoires (voir exemple annexe n°2) ***établis par domaine*** décrivent les procédures de sécurité existantes et visent à identifier les risques probables qui pourraient résulter d'une défaillance de ces procédures.

Ils relatent les ***faiblesses relevées au niveau d'un élément par rapport à un domaine***[24] ***donné*** et présentent les risques probables à partir du diagnostic réalisé préalablement.

232 MEMOIRE-INCIDENCE (MI): IMPACT DES RISQUES IDENTIFIES :

Ces mémoires (voir exemple annexe n°3) reprennent les risques relevés en vue de déterminer leur incidence sur l'intégrité, la disponibilité et la confidentialité. A ce niveau, les risques sans incidences ne seront pas retenus.

A) SUR L'INTEGRITE :

L'intégrité se réfère à l'authenticité, à l'exactitude et à l'exhaustivité des données saisies et sauvegardées. Le MI décrira les conséquences d'une insuffisance des mesures de sécurité sur la fiabilité des résultats fournis par le système.

---

24) Les domaines d'investigation ainsi que les éléments retenus ont été présentés dans le cadre général de diagnostic (annexe n°1).

B) SUR LA DISPONIBILITE :

La disponibilité se réfère à la capacité du système à fournir en permanence les informations nécessaires au bon fonctionnement de l'entreprise. Le MI décrira les conséquences de la défaillance totale ou partielle du système causée par une insuffisance de la sécurité.

C) SUR LA CONFIDENTIALITE :

La confidentialité se réfère à la capacité du système à se prémunir contre l'indiscrétion et le détournement d'informations... Le MI relatera l'impact d'une défaillance des mesures de sécurité sur la confidentialité des informations gardées dans le système.

233 TABLEAU-SYNTHESE (TS) ET EVALUATION QUALITATIVE :

A) TABLEAU-SYNTHESE (TS) (= tableau de bord)

Ce tableau (voir exemple annexe n°4) synthétisera les *deux mémoires précédents*. Il reportera, d'une manière concise, les risques par élément de domaine ainsi que leur impact sur l'intégrité, la disponibilité et la confidentialité. Il permettra :

1°) de déterminer le profil des risques (majeur et mineur). Ce classement s'effectuera en fonction :

*) de leur *impact financier* prévisionnel;
*) de *l'importance stratégique* de l'élément endommagé;
*) et de *la probabilité*[25] *de réalisation* du risque compte tenu de l'état de la sécurité.

2°) de dégager une évaluation qualitative des mesures de sécurité.

---

25) Il s'agit d'une probabilité subjective, voir aussi CNCC : "Les contrôles dans les entreprises informatisées", tome II.

B) PROFIL DES RISQUES :

B1) RISQUES MAJEURS :

Seront qualifiés de majeurs, tous les risques dont la concrétisation aurait un impact important et/ou dont la probabilité de survenance est estimée suffisante pour les retenir en tant que tels. L'entreprise ne peut pas se permettre de les prendre. L'auditeur doit insister sur leur prévention et leur résolution.

B2) RISQUES MINEURS :

Ces risques, pour importants qu'ils soient, ne mettent pas directement en cause l'activité de l'entreprise et/ou la probabilité de leur réalisation peut être estimée négligeable. Ils demandent certes une détection rapide mais ne nécessitent pas, sauf s'il est simple de l'envisager, une prévention. L'auditeur doit prendre en compte ces éléments dans le type d'évaluation et de recommandation qu'il sera amené à effectuer.

C) EVALUATION QUALITATIVE DES MESURES DE SECURITE :

Sur la base du tableau-synthèse *(TS)*, l'auditeur porte un *jugement qualitatif* sur les procédures de la sécurité informatique.

Il s'agit d'une ***appréciation qualitative globale et nullement le résultat d'une moyenne arithmétique*** des forces et faiblesses notées par domaine. Elle doit se baser, essentiellement, sur :

*) l'importance des risques non couverts et;
*) leur profil.

Cette appréciation qualitative sera raffinée par la quantification des risques.

24 QUATRIEME ETAPE : MATRICE DE QUANTIFICATION DES RISQUES (M)

L'auditeur définira un certain nombre de scénarios de sinistre en étroit rapport avec les risques majeurs identifiés et sa connaissance générale de l'entreprise.

La définition du scénario peut, de ce fait, être plus large que celle du risque majeur.

La quantification de leurs conséquences sera effectuée au niveau des fonctions qui constituent les Facteurs Clès de l'Activité de l'Entreprise (FCAE).

Un triple objectif doit être atteint :

1°) décrire les applications à auditer et dégager leurs spécificités;

2°) définir les scénarios retenus et spécifier le cadre de leur quantification (hypothèse, fondements du scénario, conséquences);

3°) estimer le coût maximum de la non-sécurité par scénario et par application à partir de la MQR.

241 A[26] LES APPLICATIONS A AUDITER :

Le choix d'une application doit être guidé par

(1) *son importance* pour la réalisation de l'activité de l'entreprise (FCAE);

EXEMPLE : Cas d'une société de transport routier de marchandises.

la réalisation de son activité se base, essentiellement, sur son personnel et ses véhicules. L'essentiel de ses produits résulte de son activité de transport.

Les applications à la base de la gestion du personnel (paie, gestion social...), de la gestion de son parc de véhicules (carburant, pièces de rechange, entretien...) et facturation sont à retenir.

---

26) A comme Application.

Le calcul d'indicateurs d'importance facilite ce choix :

Indicateur gestion personnel : charges de personnel / charges totales.
Indicateur gestion carburant : achats carburant / charges totales.
Indicateur produit activité transport : produit activité transport/produits totaux

L'informatique fait l'objet de l'étude. Elle est à retenir impérativement.

(2) et l'importance du *rôle* joué par l'informatique en son sein (degrè d'informatisation...)

242 S[27] LES SCENARIOS DE SINISTRE A RETENIR :

Les scénarios de sinistre possibles sont indénombrables[28].

Ceux que choisit de tester l'auditeur doivent avoir, essentiellement, pour ***fondement les risques majeurs*** relevés lors du diagnostic et sa connaissance générale de l'entreprise.

Au niveau de chaque scénario, il définit le cadre de la quantification. Il précisera :

1°) L'hypothèse qui sous-tend le scénario.
2°) les fondements du scénario.
3°) les conséquences probables.

---

27) S comme Scénario.

28) J.M. LAMERE, opcit., distingue deux catégories :

(1) scénarios type 1 :
"Ce sont les scénarios de sinistres qui ne peuvent être directement explicités par les utilisateurs parce qu'ils relèvent de la fonction informatique elle même..." p.163

(2) scénarios type 2 :
"Ce sont les scénarios de sinistres spécifiques aux fonctions concernées : l'informatique ne sert que de moyen au sinistre... On trouve dans ce type essentiellement des sinistres prenant naissance dans la fonction utilisateur." p.164

EXEMPLE : *SINISTRE TOTAL OU PARTIEL TRES GRAVE [incendie, explosion, dégâts des eaux, catastrophes naturelles...]*

A) HYPOTHESE

Nous avons envisagé le cas de la destruction totale ou partielle grave engendrant une indisponibilité pour une longue durée :

*) de la salle-ordinateur;
*) de tout le matériel;
*) des fichiers, programmes et documentation conservés dans le centre;
*) ainsi que de tout le matériel d'environnement.

B) FONDEMENTS DU SCENARIO :

(1) Absence de copies de sauvegarde des fichiers, programmes et documentation à l'extérieur du centre. (MR ...) [29]

(2) Exception faite de la salle-ordinateur, le bâtiment abritant le centre informatique n'est pas équipé d'un système de détection et d'extinction automatique d'incendie et d'eau (MR ...)

(3) Absence de consignes, affichées et testées, à suivre par le personnel en cas d'incendie (MR ...).

(4) Absence de poubelles anti-feu dans la salle-machine et de poubelles métalliques dans le reste du bâtiment (MR ...).

(5) Absence d'unités redondantes (MR ...).

(6) Proximité du centre d'une rue très fréquentée, notamment par les véhicules de la "S" chargés de carburant (MR...).

C) CONSEQUENCES :

Si un tel sinistre se réalisait, la *"S" se trouverait sans fichiers, sans programmes et sans documentation.* En effet, elle ne dispose *pas de copie en dehors du centre.* Tout doit être reconstitué.

Néanmoins, il faut préciser que certains états-utilisateurs sont éparpillés dans les services et peuvent servir comme base de reconstitution.

Il faut préciser, par ailleurs, que la "S" ne possède pas de salle blanche, n'a pas signé de contrat de back-up et *n'existe aucun contrat écrit, même* amical, avec une société disposant d'un matériel compatible lui permettant de traiter ses applications prioritaires pendant quelques heures par jour.

Toutefois, eu égard aux bonnes relations qu'elle entretient avec sa tutelle (la DGTT) ainsi qu'aux services qu'elle lui a rendue lorsque son système est tombé en panne, la "S" pourra recourir au centre de sa tutelle pour réaliser ses

29) MR... fait références aux Mémoires Risques (voir exemple annexe n°2).

applications prioritaires au moins quelques heures par jour. Ce centre est situé à peu près à 30 mn trajet/voiture.

Ayant perdu tous ses fichiers, programmes, documentation et matériels, il est important d'estimer *le délai technique minimum* pour :

a) la reconstitution des fichiers (à partir de la documentation-utilisateur);
b) la reconception de tous les programmes;
c) la mise en état du centre et;
d) la réception du matériel de remplacement;

Ceci afin *d'estimer* pour chaque application à auditer le coût maximum de la non-sécurité.

Selon les entretiens que nous avons menés avec les responsables informatiques de la "S", le délai technique peut être estimé pour la :

a) reconstitution de tous *les fichiers à 6 mois*;
b) reconception de tous les *programmes actuels, avec le même effectif à 3 ans* (la "S" atteindra alors 100% de sa capacité actuelle).
c) remise en état du centre et réception du matériel de remplacement à 12 mois.

Ainsi, *l'hypothèse la plus optimiste est que les applications prioritaires soient parfaitement opérationnelles dans 12 mois (délai de remise en état du centre, reconstitution des fichiers, reconstitution des dossiers d'analyse, jeux d'essai, conception définitive des programmes, réception du matériel...).*

243 LA MATRICE DE QUANTIFICATION DES RISQUES (MQR) :

La quantification des risques revient à estimer le coût maximum de la non-sécurité par scénario au niveau de chaque application.

La synthèse de cette estimation donnera lieu à l'établissement de la MQR (voir modèle ci-dessous).

MATRICE DE QUANTIFICATION DES RISQUES (MQR)

	A1	A2	A3	A4	TOTAL
S1					
S2					
S3					
S4					
TOTAL					

S comme Scénario A comme Application

Elle permettra à l'auditeur de dégager :

1°) le coût maximum de la non-sécurité.
2°) l'application la plus vulnérable.
3°) le (ou les) scénario(s) non confirmé(s)[30].
4°) une appréciation objective qui confortera[31] ou ajustera[32] le jugement préliminaire ± subjectif qu'il a formulé sur la base du Tableau-Synthèse.

25 CINQUIEME ETAPE : RECOMMANDATIONS D'AMELIORATION (A) :

A l'issue de la quantification des risques, l'auditeur rédigera une note[33], à l'intention de la direction générale, dans laquelle il reportera la M.Q.R.[34] et formulera des recommandations, par domaine, relatives à l'absence de certaines mesures de sécurité.

30) les coûts de non-sécurité estimés sont non significatifs.

31) permettra à l'auditeur de justifier ses craintes.

32) *permettra à l'auditeur de nuancer ses craintes.*

33) *Cette note peut être insérée, titre à part, dans la lettre de direction portant sur le contrôle interne ou faire l'objet d'une note spécifique.*

34) *M.Q.R.: Matrice de Quantification des Risques.*

26 SIXIEME ETAPE : INCIDENCES SUR LA MISSION DE REVISION (I) :

Sur la base de la M.Q.R., l'auditeur arrête les **risques majeurs confirmés**[35]. Ils feront l'objet d'un examen approfondi en vue de jalonner les grandes lignes de la finition de sa mission tant sur le plan du contrôle interne que celui des comptes. Seuls seront retenus les aspects pourront avoir un impact sur les états financiers.

Cet examen aboutit à l'établissement de **Mémoires d'Orientation Générale des Travaux (M.O.G.T.)**[36]. Il est important qu'il tienne sur une seule page. Il s'intégrera dans la planification globale de la mission (qu'elle soit légale ou contractuelle), fera partie intégrante du dossier d'audit et donnera lieu à des programmes de travail détaillés dont l'exécution sera confiée aux collaborateurs.

Le budget temps que nécessitera cet examen est faible. Paradoxalement, son résultat est particulièrement important.

Au niveau de cette étape, l'auditeur ne reviendra pas sur l'absence de certaines mesures de sécurité identifiées lors du diagnostic (deuxième étape). Elles ont déja fait l'objet de recommandations[33]. Elles seront reprises dans le rapport général. *Il menera, plutôt, son investigation au niveau de certaines mesures existantes pour apprécier leur adéquation.*

Précisons que l'objectif de cette étape n'est nullement de réaliser cet examen approfondi mais de jalonner ses grandes lignes.

---

35) dont les coûts estimés de non-sécurité sont significatifs. Rappelons que ces risques sont à la base de la définition des scénarios analysés.

36) inspiré du document CNCC intitulé "fiche d'orientation générale des travaux", voir exemple annexe n°5.

261 AU NIVEAU DU CONTROLE INTERNE :

Il s'agit de définir les axes sur lesquels portera l'examen de certaines procédures de contrôle interne par risque majeur confirmé.

262 AU NIVEAU DU CONTROLE DES COMPTES :

L'objectif est de déterminer les postes des états financiers qui feront l'objet d'un examen approfondi.

Il ne s'agit pas d'établir des programmes de travail ni de réaliser l'audit de ces postes mais uniquement de les préciser.

CONCLUSION GENERALE

L'audit de la sécurité informatique est une tâche fonctionnelle. Son coût est indirect. Ses "outputs" sont difficilement quantifiables. Le raisonnement en terme de gain est, donc, inapproprié.

La sensibilisation des différents acteurs de l'entreprise aux conséquences des risques informatiques nous semble plus appropriée. Elle est primordiale dans les PME : l'approche est volontariste. Elle est nécessaire dans les grandes entreprises pour garantir la collaboration des personnels concernés.

L'état de la sécurité informatique a des incidences sur la qualité des états financiers de l'entreprise. Il appartient à l'auditeur d'en déduire l'incidence sur le déroulement de sa mission. Notre démarche (COOMAI) conçue dans cet objectif.

ANNEXE N° 1 : CADRE GENERAL DE DIAGNOSTIC

DOMAINES	ELEMENTS	MENACE/RISQUE	CONSEQUENCES		
			TECHNIQUES	FINANCIERES (cout de...)	AUTRES
SECURITE PHYSIQUE	MATERIEL	VOL	Indisponibilité totale	Remplacement Redressage (n.s.)	
		SABOTAGE	Indisponibilité totale ou partielle	Remplacement ou Réparation Redressage	
		FLEAUX NATURELS	Paralysie complète ou partielle du système	Remise en état du centre Remplacement Centre de remplacement Redressage (n.s.)	
	PROGRAMMES	VOL		Manque à gagner	Divulgation secrets Perte de monopole
		COPIE		Idem	Idem
		DESTRUCTION	Paralysie complète ou partielle du système	Reconception des programmes Réalisation manuelle de traitements Rachat des logiciels décodés Redressage (n.s.)	
		MODIFICATION	Paralysie partielle du système	Détournement de fonds Recherche de la modification. Remplacement du programme Remise en état du système Redressage (n.s.)	Perturbation des services Résultats erronnés
		FLEAUX NATURELS	Cf. matériel	Reconception des programmes Recrut de logiciels Location centre	
	DONNEES	VOL		Manque à gagner	Perte monopole
		CONSULTATION ILLICITE		Manque à gagner Investissement non rentabilisé	Divulgation secrets
		DESTRUCTION	Perte de données	Reconstitution des fichiers	Perturbation des Sces
		FRAUDE		Recherche et correction	Doutes sur les données
		FLEAUX NATURELS	Cf. matériel	Reconstitution des fichiers	
ACCES	PHYSIQUE	VOL	Cf. matériel Cf. données Cf. programmes	Cf. matériel Cf. données Cf. programmes	Cf. matériel Cf. données Cf. programmes
		DESTRUCTION	Idem	Idem	Idem
	LOGIQUE	COPIE ET VOL		Manque à gagner Investissement non rentabilisé	Perte monopole
		CONSULTATION ILLICITE		Poursuite en justice Recherche des fuites	Perte monopole Atteinte confidentialité
		ALTERATION DES DONNEES ET PROGRAMMES	Paralysie partielle du système	Recherche de la modification Détournement de fonds Recherche et correction	Perturbation des Sces Doutes sur les données
EXPLOITATION	RELATIONS UTILISATEURS / INFORMATICIENS	ERREURS DE SAISIE	Indisponibilité des fichiers mis à jour	Recherche et correction Maintenance des programmes Traitements manuels	
		RESULTATS ERRONES	Indisponibilité des fichiers mis à jour	Décisions erronées Recherche et correction	
	PLAN INFORMATIQUE	CONFIGURATION INADAPTEE		Traitement parvisible	Insatisfaction des utilisateurs
MESURES D'URGENCE ET/OU DE SECOURS	PLAN D'EVACUATION A CHAUD	ABSENCE DE PLAN	Paralysie complète ou partielle du système	Remplacement ou réparation Travaux non sauvegardés	
	DUREE DE REPRISE DES TRAITEMENTS	ABSENCE D'ESTIMATION		Services factures plus chers Redressage (n.s.)	Perturbation des Sces Durée de la reprise est plus longue
	REDEMARRAGE	ABSENCE D'ESTIMATION		Coût non transféré à la charge de l'assureur	Mauvaise rédaction du contrat d'assurance

ANNEXE N°2 : MEMOIRE RISQUE

MEMOIRE RISQUE (MR) REF. : MR 1111	SOCIETE : "S" AUTEUR : Z.R. DATE :

DOMAINE : SECURITE PHYSIQUE
ELEMENT : MATERIEL
DIAGNOSTIC : FACTEUR(S) N°304, 305.2, 305.5, 305.8

1°) La salle-ordinateur est équipée de systèmes de détection automatique d'incendie et d'eau reliés à la loge du gardien et d'un système d'extinction automatique des incendies à halon.

2°) Aucun système de détection ni d'extinction automatique d'incendie et d'eau n'existe pour le reste du bâtiment abritant le centre informatique.

3°) Les consignes de sécurité-incendie ne sont pas affichées et testées.

4°) La "S" n'utilise pas de poubelles anti-feu dans la salle-ordinateur ni de poubelles métalliques dans le reste du centre.

5°) Aucune inscription apparante apposée sur le matériel précisant son appartenance à la "S" n'existe
---> gestion physique du matériel non dissuasive.

6°) La "S" ne dispose pas d'unités redondantes.

RISQUES :

VOL : vol de petits matériels.

FLEAUX NATURELS :

1°) Retard dans la détection d'un feu qui se déclare dans le centre informatique en dehors de la salle-ordinateur après les heures de travail. Le feu ne parvient pas à la salle-ordinateur mais atteint les terminaux, l'onduleur, les bureaux du personnel et la salle d'archive.

2°) Inefficacité dans l'application des consignes de sécurité à suivre en cas d'incendie qui se déclare dans la salle-ordinateur pendant les heures de travail. Le personnel pris de panique réagit inefficacement.

3°) Risque qu'un feu se déclare dans la salle-ordinateur La "S" n'utilise pas de poubelles anti feu dans la salle-ordinateur ni de poubelles métalliques dans le reste du centre.

ANNEXE N° 3 : MEMOIRE INCIDENCE

MEMOIRE INCIDENCE (MI) REF. : MI 1211/1	SOCIETE : "S" AUTEUR : Z.R. DATE :

DOMAINE : SECURITE PHYSIQUE
ELEMENT : MATERIEL
RISQUE : VOL

Gestion physique du matériel non dissuasive.

INCICENCES SUR :

L'INTEGRITE : Aucune.

LA DISPONIBILITE : Indisponibilité du matériel dérobé.

LA CONFIDENTIALITE : Aucune.

OBSERVATIONS : Voir, également, accès physique.

ANNEXE N° 4 : TABLEAU SYNTHESE

REF.[1]	INCIDENCES SUR RISQUE / MENACE	L'INTEGRITE	LA DISPONIBILITE	LA CONFIDENTIALITE
	1) D/ SECURITE PHYSIQUE			
	11) E/ MATERIEL			
MI 1211/1	111) VOL	Aucune	petits matériels*	Aucune
MI 1211/1 ;2;3;4	112) FLEAUX NATURELS	fichiers**	éléments périphériques**	consultation illicite involontaire**
	12) E/PROGRAMMES			
MI 1212/1	121) VOL/COPIE	Aucune	Aucune	perte monopole*
MI 1212/2	122) MODIFICATION FRAUDULEUSE	fichiers**	programmes*	Aucune
MI 1212/3	123) FLEAUX NATURELS	Aucune	programmes**	Aucune
	13) E/DONNEES			
MI 1213/1	131) VOL/COPIE CONSULTATION ILLICITE	Aucune	Aucune	perte monopole*
MI 1213/2	132) DESTRUCTION	Aucune	fichiers*	Aucune
MI 1213/3	133) MANIPULATION FRAUDULEUSE	fichiers*	fichiers**	aucune
MI 1213/4	134) FLEAUX NATURELS	Aucune	Aucune	fichiers**
	2) D/ACCES			
	21) E/ACCES PHYSIQUE			
MI 1221/1	211) VOL/DESTRUCTION	Aucune	petits matériels*	perte monopole*
MI 1221/2	212) ACCES FRAUDULEUX	Aucune	fichiers*	perte monopole*
	22) E/ACCES LOGIQUE			
MR 1122	221) COPIE et VOL	Aucune	Aucune	Aucune
MR 1122	222) CONSULTATION ILLICITE	Aucune	Aucune	Aucune
MR 1122	223) ALTERATION	Aucune	Aucune	Aucune

546

	3) D/EXPLOITATION			
	31) E/RELATIONS UTILISATEURS/INFORMATICIENS			
MI 1231/1	311) ERREUR DE SAISIE	fichiers**	fichiers**	Aucune
MI 1231/2	312) RESULTATS ERRONES	fichiers**	fichiers**	Aucune
	4) D/URGENCE/SECOURS			
	41) PLAN D'EVACUATION A CHAUD			
MI 1241/1	411) PERTE MATERIELLE	Aucune	Matériel*	Consultation 111ette inventaire*
MR 1141	412) PERTE DE TEMPS	Aucune	Aucune	Aucune
MR 1141	413) PERTE PROGRAMMES	Aucune	Aucune	Aucune
	42) E/ESTIMATION DE LA DUREE DE REPRISE			
MI 1242	421) CENTRE NON CONTRACTUEL	fichiers*	Aucune	Consultation 111ette inventaire*
MR 1142	422) DELAI DE REPRISE PLUS LONG	Aucune	Aucune	Aucune
	43) E/ESTIMATION DU COUT DE REDEMARRAGE			
MR 1143	431) ASSURANCE	Aucune	Aucune	Aucune
MR 1143	432) CONTRAT D'ASSURANCE	Aucune	Aucune	Aucune

D : comme Domaine E : comme Elément * : risque mineur ** : risque majeur

1) Ces références renvoient à l'annexe n°2

ANNEXE N°5 : M.O.G.T.

MEMOIRE D'ORIENTATION GENERALE DES TRAVAUX (MOGT) REF.: RM 1	SOCIETE : "S" AUTEUR : Z.R. DATE :

1) RISQUE MAJEUR : FLEAUX NATURELS

11) CONSEQUENCES TECHNIQUES : paralysie totale ou partielle du système informatique (matériels, programmes et fichiers) pour une ± longue durée [>=12 mois]

12) CONSEQUENCES FINANCIERES : pertes maximales estimées à ≈ 803 KDT

A1	PAIE	3 KDT
A2	FACTURATION	199,5 KDT
A3	CARBURANT	0,5 KDT
A4	INFORMATIQUE	600 KDT

2) CONTROLE INTERNE :

21 TRAVAUX A EFFECTUER :
211 examen des procédures de secours et/ou d'urgence.
212 examen des clauses du contrat de dépannage.
213 examen des clauses du contrat d'assurance.
214 examen des états utilisateurs (au niveau des applications facturation et paie).

22 OUTILS A UTILISER :
221 examen des documents (manuel de procédures, contrats, recueil de règles, états...)
222 description des règles par les intéressés.

3) CONTROLE DES COMPTES :

31) COMPTES A AUDITER :
311 créditeurs divers : voir si la S.T.M. est en règle vis à vis de l'acquittement de la prime d'assurance.
312 provisions pour risques et dotations aux provisions (relatives à l'assurance informatique).
313 comptes de régularisation actif et passif (respect du principe de la séparation des exercices).

32) OUTILS A UTILISER :
321 confirmation directe; pour le 311 et le 313.
322 évaluation de la provision à constituer; pour le 312.
323 examen de l'échéancier; pour le 313.

4) REFERENCES DES PROGRAMMES DE TRAVAIL :