CESAG Centre Africain d'études Supérieures en Gestion

Institut Supérieur de Comptabilité, de Banque et de Finance (ISCBF)

Master Professionnel en Audit et Contrôle de Gestion (MPACG)

Promotion 4
(2010-2011)

Mémoire de fin d'étude

THEME

L'évaluation de la maitrise des risques liés au réseau informatique : Cas de la Banque pour le Commerce et l'Industrie du MALI (BCI-Mali SA)

Présenté par :
KONE Aziz Abdoulaye

Dirigé par :
M. Samba N'DIAYE
Enseignant associé
En systèmes d'informations et en informatique

Octobre 2011

Dédicaces

A la mémoire de mes grands-parents maternels, j'aurais aimé qu'ils voient leur petit-fils grandir.

A mes grands-parents paternels, que leurs bénédictions m'accompagnent.

A mes très chers parents qui ont toujours été là pour moi, et qui m'ont donné un magnifique modèle de labeur et de persévérance. J'espère qu'ils trouveront dans ce travail toute ma reconnaissance et tout mon amour.

A mes sœurs bien-aimées : Assista et Awa.

A mes tantes et à mes oncles.

A mes cousins et cousines.

A mes amis : Idrissa, Laye, Ahmadou.

Je dédie ce mémoire.

Puisse le Seigneur les récompenser de leurs efforts, leurs apports et nous guider.

Remerciements

Au très Miséricordieux.

Je ne saurai commencer ces remerciements sans tendre la main à Mme YAPI Bernadette, ses enfants : Claire, Yannick et Landry, et Nabou ; leur proximité a été une source d'assurance indéniable. Puisse Dieu vous bénir.

A M. & Mme DJERMA ainsi qu'à leurs enfants, ils ont été ma seconde famille, puisse leurs enfants marcher sur vos pas.

Je remercie chaleureusement M. Samba N'DIAYE, mon directeur de mémoire, sans qui ce travail n'aurait eu un aboutissement.

A M. Adama Moulaye SIDIBE et à tout le personnel de la Banque pour le Commerce et l'Industrie particulièrement au département d'audit, je ne saurai exprimer la nostalgie que je ressens depuis la fin du stage. Je leur suis reconnaissant pour le climat de travail, vos conseils et votre ouverture.

A M. SYLLA Dolele dont les qualités ont su faire naitre en moi une impulsion allant jusqu'à la rédaction d'un mémoire sur les risques informatiques.

A M. YAZI Moussa et tout l'institut ISCBF, leur rigueur a été une source de motivation et d'abnégation.

Je remercie affectueusement les membres de mon groupe de travail Mauly Des-Lor, Leïla, Serge, Oda Marième, Rachad, Kader. L'expérience fut gratifiante à leurs côtés ; Puisse Dieu rendre éternels ces liens que nous avons créés.

Au CESAG, un environnement inoubliable.

Liste des sigles et abréviations

AES : Advanced Encryption Security

BCEAO : Banque Centrale des Etats de l'Afrique de l'Ouest

CLUSIF : Club de la Sécurité de l'Information Français

CNIL : Commission Nationale de l'Informatique et des Libertés

COBIT : Control Objectives for Informations and Related Technologies

COCO : Criteria On Control Committee

DES : Data Encryption Security

DNS : Domain Name Service

EBIOS : Expression des besoins et Identification des Objectifs de Sécurité

EDM : Energie Du Mali

FTP : File Transfer Protocol

HTTP : HyperText Transfer Protocol

IP : Internet Protocol

ISO : International Standard Organization

LAN : Local Area Network

MAN : Metropolitain Area Network

MEHARI : Méthode Harmonisée d'Analyse des Risques

OCTAVE : Operationally Critical Threat, Asset and Vulnerability Evaluation

OSI : Open Systems Interconnections

PAT : Performance Acceleration Technology

SOTELMA : Société des Télécommunications du Mali

SSII : Société de Service en Ingénierie Informatique

TCP : Transmission Control Protocol

UEMOA : Union Economique et Monétaire Ouest-Africaine

WAN : Wide Area Network

Liste des figures et tableaux

Tableaux

Figures

Liste des annexes

Table des matières

INTRODUCTION GENERALE

Jusqu'à un passé récent, les ressources humaines, matérielles et financières ont toujours été perçues comme les capitaux les plus importants. Leur synergie est indispensable au bon fonctionnement des entreprises et renseigne ses acteurs sur la voie qu'elles empruntent en lui permettant de prendre des décisions. De ce fait, l'information dont elles sont l'un des conducteurs principaux, se présente comme l'épine dorsale de l'entreprise. En effet, les entités n'ont aucune vie sans information. Elle est en amont et en aval des activités des organisations. Les états financiers, les indicateurs de performance, les rapports, les contrats, les messages, les discussions, etc. sont autant d'éléments constitutifs de l'information au sein des entreprises et dans notre quotidien. Ces entités sont des greniers d'informations. Elle peut être définie comme un ensemble de signaux en vue de la diffusion et de la communication de données, dans tous les domaines, par un individu, par des groupes d'individus ou des entités agissant ou rétroagissant ainsi sur leur environnement et dont le but est de déclencher éventuellement des processus dialectiques alimentant l'échange. La gestion de l'information s'avère être au sein des structures tout un système, à l'instar des implications que nécessite la gestion financière ou humaine, tant sa portée et son importance sont prépondérantes.

En 2003, quand le géant Enron déposait la clé sous les paillassons, des mesures ont été entreprises pour endiguer l'expansion de la production de données inexactes, voire frauduleuses. La loi Sarbannes Oxley (SOX), rentrée en vigueur en Juillet 2002, aux Etats Unis, a durci le ton sur la nécessité de la gouvernance des systèmes d'informations, surtout financiers. Cette notion, incluse dans la gouvernance de l'entreprise, a pris de l'ampleur du fait d'une volonté première de voir nos entités plus transparentes et plus saines. Ces éléments ont pollué nôtre quotidien à la suite des nombreux dérapages des entreprises dans le monde. La mise en œuvre de la gouvernance dans l'entreprise permet de garantir un processus durable et efficace de création de valeurs conforme à l'ensemble des parties-prenantes internes et externes. Elle met en relief une nécessité de respecter les règlements légaux, les statuts internes et les principes éthiques. Ainsi, la gouvernance du système d'informations a pour dessein de s'assurer que celui-ci réponde bien, aujourd'hui et demain, aux attentes des différentes parties prenantes : utilisateurs et clients, financés et financeurs, concepteurs et techniciens. Selon ANGOT (1996 :210) : « un SI (système d'information) est un réseau complexe de relations structurées où interviennent hommes, machines et procédures qui a pour but d'engendrer des flux ordonnés d'informations pertinentes provenant de différentes sources et destinées à servir de base aux décisions ». Fort de cela,

d'aucuns diront que les gagnants dans la vie d'aujourd'hui seront ceux qui portent un regard attentif sur la manière dont l'information circule au sein de leurs entreprises.

Au sein des systèmes d'informations, sont incluses les technologies de l'information qui concourent au bon traitement de l'information. Les réseaux dans ce champ, occupent une place de choix car ils permettent de relier les matériels informatiques. En effet, l'homme, en tant qu'être communiquant, a rapidement compris l'intérêt qu'il pouvait y avoir à relier les ordinateurs entre eux afin de pouvoir échanger des informations. De nos jours, c'est entre plusieurs ordinateurs que l'information est échangée et plus avec l'internet. Ainsi, il est rare d'observer une entité sans réseau informatique pour la facilitation de son fonctionnement et généralement du fait de la nécessité de l'environnement qui le lui impose. Chaque entreprise utilise et stocke de plus en plus d'informations sous forme numérique : e-mails, propositions commerciales, factures, processus de production, comptabilité... même la téléphonie s'est informatisée. Dans le souci d'accompagner les entités dans la quête perpétuelle de la qualité, des « best practices » sont édictés notamment le COBIT « Control Objectives for Information and Related technology » qui communique sur les meilleures dispositions à adopter en matière de gestion des technologies de l'information.

Néanmoins, selon les résultats de la 11ème édition de la plus grande enquête mondiale sur la sécurité de l'information réalisée par le cabinet PricewaterhouseCoopers en 2010 (12 800 entreprises et organisations interrogées dans le monde), les pertes financières liées aux incidents de sécurité informatique ont doublé. La séduction mondiale de l'internet en parallèle avec la cybercriminalité accroit les probabilités d'incidents sur les systèmes informatiques des entreprises, en particulier leur réseau, et par ricochet sur leurs systèmes d'informations qui sont ouverts aux partenaires, fournisseurs et clients. En concourant à une atteinte plus prompte des objectifs, ces outils sont très menacés à cause des possibilités d'accès aux ressources informationnels qu'ils offrent. Dès lors que deux matériels sont reliés, il y'a la naissance d'un risque, plus avec l'internet. Nous ne sommes pas en marge des menaces qui planent sur les vulnérabilités des réseaux vu la croissance du volume de nos transactions avec l'extérieur, la recrudescence des malversations, la faible importance apportée à la sécurité des informations et l'excroissance de la cybercriminalité. Leur importance au regard de l'inexistence de la certitude sécuritaire absolue alerte les sociétés où qu'elles soient. En Afrique et particulièrement dans la sous-région, nos entreprises sont beaucoup influencées par ce qui se passe en occident.

En Afrique de l'Ouest, les banques sont les institutions les plus avancées dans la prise en compte de l'importance des systèmes d'informations. Même si, encore parmi elles, certaines tardent à le faire, il y' a un effort à souligner. Cette longueur d'avance sur les autres acteurs de l'économie est imputable à la technologie qu'elles utilisent et à la concurrence qu'impose leur secteur. Effectivement, au Mali, la gestion des systèmes d'informations est perçue généralement comme l'apanage des grandes entités. Ce constat est perceptible auprès des acteurs de la Banque pour le Commerce et l'Industrie (BCI) mais les dirigeants imputent cela à la jeunesse de l'entité, âgée d'à peine 4 années.

Elle dispose, à l'instar de ses consœurs, d'un réseau local, indispensable à son fonctionnement qui regroupe tous les postes de travail de la banque. L'internet étant primordial à ces activités, tous y ont accès sans restriction. Elle a à son actif une plateforme ouverte aux partenaires et accessible via l'internet, accédant aux applications internes de la banque sans toutefois que ces dernières aient été connectées au web. Néanmoins, comme toute banque, elle n'a pas été épargnée par des dysfonctionnements internes du réseau local ayant entraîné une perturbation des activités même si elle n'a pas encore été victime d'attaques externes.

La banque prend en compte toutes ces possibilités d'attaques sans qu'il ait encore eu une évaluation du dispositif de maîtrise des risques liés au réseau informatique ; par conséquent aucun référentiel exposant les risques dont l'entreprise peut être sujette n'est à disposition. Cette constatation n'est pas seulement relative à la BCI car de nombreuses autres banques de la place sont dans la même situation. Ceci est attribuable au faible volume des activités de la banque comparée aux banques occidentales, aux décisions de leurs dirigeants, au milieu économique et aux politiques en vigueur tant au niveau Etatique qu'au niveau des entités elles-mêmes.

Toutefois, les donnes changeant, les environnements évoluant ainsi que les mentalités, la prise en compte de l'importance de la gestion des systèmes d'informations prend forme, en particulier celui du réseau local. Géré d'habitude, comme un paramètre purement informatique, la perception est en voie d'être révolue quoique les ressources n'accompagnent pas véritablement ce fait. Au sein de la BCI, le département audit marque un point d'honneur à vulgariser la prise en considération dans les faits et écrits de l'évaluation des risques liés aux systèmes d'informations tandis qu'il n'y en a pas encore eu. La mise en exergue des incidents antérieurs survenus sur le réseau de certaines institu-

tions occidentales alertent plus d'un sur la nécessité de porter un œil attentif sur ce service tant utilisé et c'est le moyen le plus usité sous nos cieux pour rappeler l'importance d'un actif.

Les intérêts de la mise en place des réseaux sont multiples, que ce soit pour une entreprise ou un particulier. Aujourd'hui, avec internet, on assiste à une unification des réseaux, par ricochet une transversalité et une ouverture au public des systèmes d'informations en partie ou en totalité de certaines firmes. À mesure que les entreprises se développent, elles sont de plus en plus dépendantes des technologies réseau pour assurer leur rentabilité. Les réseaux informatiques n'ont jamais été aussi précieux pour l'activité des entreprises et, en même temps, aussi difficiles à protéger. Certaines attaques virales de grande envergure telles que MyDoom[1] ou Blaster[2] nous ont rappelé combien la sécurité informatique reste un sujet d'actualité. D'autres chiffres, souvent en rapport avec nos propres agissements en l'occurrence des velléités de malversation via le réseau informatique de l'entreprise, corroborent ces dires car :

- « en Europe, 61% des entreprises considèrent les logiciels espions comme un problème de sécurité majeur tandis que la moitié d'entre elles les perçoivent comme résolus après éradication du réseau et que, 44% analysent le réseau chaque semaine pour traquer les menaces.

- Le centre de coordination du CERT (Computer Emergency Response System) de l'université Carnegie Mellon a enregistré 3784 failles de sécurité en 2003. Ce centre a également déclaré que la plupart des intrusions résultaient d'une exploitation de vulnérabilités connues, d'erreurs de configuration ou d'attaques et pour lesquelles il existait des contre-mesures.

[1] Mydoom : Virus qui se propage par email et KaZaA. Il se présente sous la forme d'un message dont le titre est aléatoire, accompagné d'un fichier joint dont l'extension est .BAT, .CMD,.EXE, .PIF, .SCR ou .ZIP et dont l'icône est faussement souvent celle d'un simple fichier texte. Si ce fichier est exécuté, le virus s'envoie aux contacts dont les adresses figurent dans le carnet d'adresses Windows et divers autres fichiers, installe une backdoor et se copie sous divers noms aguicheurs dans le répertoire partagé via KaZaA.

[2] Blaster : Premier virus ciblant les ordinateurs vulnérables à la faille RPC de Microsoft. Si une machine connectée à Internet n'est pas à jour dans ses correctifs, Blaster l'infecte via le port 135 TCP puis scanne le réseau à la recherche de nouvelles machines vulnérables. Il est par ailleurs programmé pour lancer une attaque par déni de service contre le site WindowsUpdate à partir du 16/08/03, afin de tenter d'empêcher les retardataires de télécharger le correctif nécessaire à leur système. La mise à jour des ordinateurs sous Windows NT, 2000, XP et 2003 est urgente et impérative.

- Aux Etats-Unis, 85% des entreprises ont été frappées par des virus en 2002.
- En 1999, des sociétés figurant parmi les 1000 premières au monde (classement Fortune) ont perdu 45 milliards de dollars US en raison de vol d'informations et ont subi en moyenne 67 attaques.
- 35 % des responsables informatique d'entreprises espionnent leurs collègues et utilisent leurs mots de passe pour connaître jusqu'à leurs salaires, selon la société américaine Cyber-Ark.
- "Avec un taux de 78 %, le Sénégal est le deuxième pays d'Afrique de l'Ouest et du centre, derrière le Cameroun avec 83%, en matière de piratage informatique" selon, Youssry, directeur général de Microsoft Afrique de l'Ouest et du Centre. ». LIVRE BLANC LANDESK (2005 :3)

Et plus cela progressera, plus les réseaux perdront encore en fiabilité, mais leur mise en place reste encore prépondérante tandis que nos entreprises ne sont pas en marge de ces maux, qui commencent à s'installer sous nos cieux. En effet, dès lors qu'ils font partie du noyau de traitement de l'information dans l'entreprise, il est primordial de s'interroger sur l'efficacité des dispositions prises par les entités en vue de maîtriser les risques déductibles des réseaux et leurs impacts sur les systèmes d'informations. Cependant, il est important de s'interroger sur les origines potentielles de ces aléas.

Plusieurs vulnérabilités relatives au réseau informatique peuvent être exploitées par des menaces réalistes au sein de la banque. Nous pouvons énumérer :

- des pannes ou une obsolescence ou une inadéquation des matériels usités,
- un contrôle à distance des ordinateurs,
- de mauvaises manipulations,
- des erreurs de paramétrage,
- une absence ou une inefficacité de la maintenance des réseaux,
- une prise en compte insuffisante de l'audit de la maintenance du réseau par le service d'audit interne,

- une absence ou une inadéquate ou une insuffisante politique de sécurité informatique du réseau,
- une carence dans la maîtrise des risques informatiques liés au réseau.

Une palette de corollaires peut résulter de ces causes à savoir :

- des détournements d'argent,
- des pertes liées à l'indisponibilité du SI,
- des pertes d'images et de crédibilité,
- des vols d'informations confidentielles,
- la mise en cause de la responsabilité juridique et contractuelle.

Ainsi les pertes financières ne sont pas que les résultantes des causes précitées. Celles évoquées sont autant importantes que les finances car elles peuvent avoir des envergures incommensurables.

Afin d'appréhender les évènements susceptibles de dégrader les réseaux informatiques, moult moyens peuvent être mis en œuvre parmi lesquels :

- Définir et réviser la politique informatique.
- Définir une politique de maîtrise des risques liés au réseau informatique.
- Effectuer la maintenance des réseaux informatiques, de façon préventive, surtout.
- Effectuer des missions d'audit du réseau informatique.
- Evaluer la maîtrise des risques potentiellement déductibles de ce réseau.

Il serait judicieux de mettre en œuvre selon les cas, ces solutions sur la base de ce qui se fait de mieux à travers le monde, c'est-à-dire conformément aux meilleures pratiques, aux normes et référentiels en technologie de l'information. Toutefois, ces solutions ne sont efficaces que si l'institution, elle-même, est consciente que son réseau, au même titre que ses autres actifs, peut engendrer des risques et qu'elle se doit de les identifier, de mettre en œuvre ce qui est nécessaire pour les parer. Cela nous amène à retenir que dans la bataille contre les obstacles, la maîtrise des risques liés au réseau informatique est plus qu'importante de par ce qu'elle implique.

Partant de cela, nôtre interrogation majeure est la suivante : quelle est l'efficacité de la maîtrise des risques liés au réseau informatique en place au sein de la banque ?

Cela nous amène à étudier différentes questions à savoir :

- Comment évaluer le contrôle interne du réseau informatique ?
- Quels sont les risques liés au réseau informatique ?
- Quelle organisation mettre en place pour le contrôle interne du réseau informatique ?
- Quelles sont les sécurités logiques et physiques indispensables pour un réseau sécurisé ?
- Quels sont les politiques et dispositifs de maîtrise des risques liés au réseau informatique de la structure ?
- Quel est l'outil de mesure de la maîtrise des risques liés au réseau informatique en place ?

Les solutions à ces questions découleront de l'évaluation de la maîtrise des risques liés au réseau informatique : cas de la Banque pour le Commerce et l'Industrie du Mali. Elle aura pour objectif principal d'apprécier l'efficacité de la maîtrise des risques liés au réseau informatique en place et plus concrètement :

- Evaluer le contrôle interne pour en tirer les forces et les faiblesses ;
- Proposer une cartographie des risques liés au réseau informatique ;
- Garantir que les données sont bien celles que l'on croit être (l'intégrité) ;
- Assurer que seules les personnes autorisées aient accès aux ressources échangées (la confidentialité);
- Maintenir le bon fonctionnement du réseau informatique (la disponibilité) ;
- Garantir qu'une transaction au niveau du réseau ne peut être niée (la non répudiation,) ;
- Assurer que seules les personnes autorisées au niveau du réseau aient accès aux ressources (l'authentification,) ;
- Garantir la séparation en le système d'information et les accès à internet.

Dans notre traité, nous ne nous étendrons que sur la sécurité logique du réseau informatique en place en écartant donc la sécurité physique traitant des protections anti-incendie, systèmes antivol, secours électrique. Après une analyse théorique du sujet à partir d'écrits et d'expériences, nous énoncerons le modèle d'analyse que nous emploierons dans cette étude, et pour finir présenter nos expériences et résultats tirés de l'évaluation pratique que nous mènerons

Ce sujet se présente à l'entreprise comme un recueil de solutions expérimentables dans leur recherche quotidienne de qualité et de perfectionnement. Elle contribue modestement à la maîtrise des risques auxquels la banque est exposée à travers son réseau informatique en mettant en exergue, les aléas auxquels elle est confrontée et les bonnes pratiques en matière de gestion de ces risques. Il se présente comme un tremplin vers une spécialisation en audit informatique et une occasion de mettre en relief nos acquis sur les concepts théoriques en matière de maîtrise des risques.

Au CESAG, elle apporte sa participation au renflouement d'une bibliothèque qui a servi et continuera de servir. Pour les lecteurs, elle constitue une source d'informations permettant de renforcer les capacités de recherche et d'analyse des questions d'intérêt des réseaux informatiques en général et en particulier, l'évaluation des risques liés au réseau informatique et à la dédramatisation d'un sujet, originellement associé aux informaticiens uniquement.

CADRE THEORIQUE

Introduction à la partie

Jacques ATTALI dans les trois mondes (pour une théorie de l'après crise) dit qu'une théorie est vraie si elle est énonçable selon les règles de la logique formelle et si ses conséquences sont vérifiables par tout observateur. L'évaluation de la maîtrise des risques est certes un travail très pratique mais dont les fondements sont soutenus par des théories établies par des professionnels et qui ont été expérimentés pour aboutir à plusieurs méthodes d'évaluation. Il ne s'agira pas dans cette partie de faire un étalage des relatifs à notre étude mais plutôt de rendre accessible et compréhensible ce travail à toute personne rentrant en sa possession. De ce fait, la partie qui suivra mettra un point d'honneur à poser les jalons de ce qui nous aidera à évaluer la maitrise des risques du réseau informatique tout en explicitant les aspects prépondérants et les avis émis ou expériences vécues dans le domaine.

La gestion des risques liés au réseau informatique nécessite l'utilisation d'outils de gestion adéquats qui permettent à l'entreprise d'atteindre les objectifs qu'elle s'est assignée. L'un des outils utilisés dans ce cadre est la cartographie des risques. Nous consacrerons donc cette partie aux risques liés au réseau informatique, à un aperçu des méthodes usitées en la matière par les experts, puis à la méthodologie que nous emploierons pour dérouler l'évaluation, objet de notre étude.

Chapitre 1 : Administration d'un réseau informatique

Introduction

Au fil des années, les ordinateurs sont devenus indispensables au fonctionnement des entreprises. En outre, une nécessité de les relier afin d'en former un tout s'est accrue en vue d'améliorer la disponibilité et la transmission de l'information. Il suffit de relier plusieurs PC (Personnal computer) entre eux et vous obtenez la structure rudimentaire d'un réseau local (Local Area Network ou LAN). Toutefois cette structure peut être complexifiée par son agrandissement jusqu'à obtenir des « Metropolitan Area Network » (MAN) lorsqu'on se situe dans le cadre d'une liaison entre les villes et lorsque les distances qui séparent les sites sont importantes, on parle de réseau étendu (Wide Area Network : WAN).

Pour les besoins de son entreprise, le réseau usité est appelé l'intranet. Le mot intranet est devenu familier depuis une décennie bien qu'il renferme différentes interprétations. Le paradigme intranet correspond au système d'informations de l'entreprise utilisant les applicatifs d'Internet. L'intranet désigne aussi l'infrastructure de l'entreprise pour réaliser ses communications internes. L'extranet renvoie à l'infrastructure externe de l'entreprise, utilisée par les personnes ayant un accès à l'intranet depuis l'extérieur.

Dans cette étude, nous nous limiterons au réseau Ethernet, en lieu et place de sa consœur Token Ring. Il est nécessaire de préciser que les deux se valent en termes de performance, même si, à débit égal, la dernière citée a un léger avantage. Toutefois, Ethernet détient plus de 85% du marché et a toujours été techniquement en avance sur Token-Ring. Partant de cela, si l'on doit alors créer soi-même un réseau à partir de rien, autant se lancer dans Ethernet : c'est plus simple et cela coûte moins cher.

Avec les réseaux, nous rentrons donc de plein pied dans la société de l'information. Pour les besoins de ce travail, nous n'évoquerons pas le réseau dans ses profondeurs techniques, néanmoins des énoncés seront faits sur des notions indispensables à la compréhension des explications qui seront avancées.

1.1.Réseau d'entreprise

Les réseaux d'entreprise ont utilisé des technologies variées au cours du temps. L'explosion et le succès commercial d'internet, associés à une demande pressante d'interconnexion et d'interopérabilité par des protocoles les plus ouverts possibles, ont contribué à l'arrivée massive de la technologie Internet et de ses composants. En effet, suivant MONTAGNON (2001 :15), parmi les services qui peuvent être demandés à un réseau d'entreprise et donc à l'environnement intranet, on trouve :

- la mobilité, qui permet à un client de se déplacer simplement tout en conservant l'accès personnel à son système d'information ;
- l'archivage des informations, qui représente la richesse disponible en ligne sur un intranet. Les entrepôts de données ou « datawarehouses », qui rassemblent les bases de données et permettent de s'adapter à la demande, voire de la prédire ;
- le multimédia, qui permet d'intégrer, aussi bien au niveau du transport que du stockage, des informations de différentes natures ;
- le télétravail et le travail coopératif, qui permettent de gérer le déplacement physique de la personne qui travaille sans pour autant diminuer son efficacité et qui lui procurent la possibilité de coopérer avec d'autres personnes dans le but d'obtenir un résultat de meilleure qualité.

Les maîtres mots sont dès lors : qualité de service et performance du réseau. Pourtant, l'atteinte de ces objectifs devient contraignante lorsque le réseau se complexifie avec la jonction de la téléphonie aux données informatiques. C'est ce que les réseaux d'entreprise d'aujourd'hui, essentiellement bâti sur une technologie Ethernet et associée à des réseaux VLAN (Virtual Local Network), ont la charge d'exécuter.

Le réseau simple d'entreprise connecté à Internet est composé de commutateurs Ethernet et de routeurs IP (Internet Protocol). SANDOVAL (1996 :20) ajoute que les principales techniques fondamentales d'Ethernet peuvent être résumées à l'aide de quelques phrases qui suivent :

- Ethernet est devenu un réseau universel, dans le sens où des interfaces ont été développées pour les types de machines (du plus petit portable jusqu'au mainframe).
- La distance maximale entre deux stations reliées à un même réseau est de 4 km.
- Il est possible de relier jusqu'à 1024 machines sur un réseau Ethernet.

- Il est possible de retirer une machine du réseau sans perturber le fonctionnement de l'ensemble.
- Le débit global est de 1 à 10 Mbit/s en mode série (soit environ 10^6 caractères par seconde), sur l'ensemble du réseau, cette capacité étant partagée entre toutes les stations. Avec les dernières évolutions, ce débit peut être multiplié par 10 (soit 100 Mbit/sec).
- Il permet de faibles délais d'attente à l'émission en situation normale.
- Ethernet emploie une méthode d'accès distribuée entre tous les équipements connectés. Toutes les stations sont égales vis-à-vis du réseau, et il n'y a donc pas de station maîtresse qui contrôlerait le réseau.
- Le mode de transmission est de type bidirectionnel à l'alternat, c'est-à-dire que les signaux transitent dans les deux sens mais pas simultanément. Ethernet est conforme au modèle OSI[3] défini par l'organisme de normalisation ISO[4].

Le fonctionnement logique d'un réseau Ethernet peut quant à lui peut être résumé comme suit, selon TANEMBAUM (2002 :65) :

- Il s'appuie sur une méthode d'accès équitable et distribuée, dans laquelle chaque équipement, est toujours capable de décider seul s'il peut équiper le média par son émission.
- Il véhicule les données à l'intérieur de paquets (ou trames) émis sur le média. La longueur de ces trames est nécessairement comprise entre 64 et 1518 octets (avec un champ de données de 46 à 1500 octets).
- Il requiert une interface pour l'ordinateur à connecter, celle-ci gérant les fonctions MAC (Medium Access Control) propres à Ethernet.

Toutefois, la technologie Ethernet comporte des limites en termes de trafic et d'efficacité. Un réseau de quelques centaines de machines réellement actives et prétendant chacune à une part de la bande passante de plusieurs pourcents, doit être considéré comme un grand réseau. Il pourra être sujet à des pics de charge faisant généralement chuté les performances des communications, liés à des taux d'erreur et de collision importants.

[3] OSI : Open Source Information
[4] ISO: International Standard Organization

1.2. Pilotage du réseau informatique

Après la mise en activité du réseau c'est-à-dire son installation et sa mise en marche, survient l'aspect de son suivi. En effet, plus le réseau est important, plus la probabilité qu'une panne survienne à un endroit ou un autre est importante. En outre, plus il est important, plus il est difficile à gérer. Il convient donc de se doter d'outils qui simplifient sa gestion et qui diminuent le nombre de potentielles pannes. Nous irons quelques fois plus loin en parlant de la gestion du réseau, notion qui englobe plusieurs variantes aussi importantes les unes que les autres.

1.1.1. Définition de la gestion d'un réseau

D'après PUJOLLE (2008 :753) et SIMONI & AL (1997 ; 30), nous dirons donc que la gestion du réseau se résume à l'ensemble des actions qui concourent au bon fonctionnement du réseau et de ses composants, à sa configuration, à la prise en charge des pannes et de la sécurité, à la comptabilité et la recherche de performance. Après un survol de l'administration du réseau dans une entreprise, qu'en est-il de l'acteur en charge de cette fonction ?

1.2.2. Activités d'un administrateur réseau

Suivant LIMONCELLI (2007 :87), des intérêts antinomiques mais légitimes sont à gérer dans une entreprise. En effet, l'employeur souhaite protéger les intérêts de son entreprise en protégeant la fuite des informations stratégiques, en prévenant l'apparition de virus ou encore en empêchant la circulation de contenus illicites notamment racistes ou pornographiques sur le réseau. Cela passe par la sécurisation de son réseau. A l'inverse, nombre de salariés revendiquent le droit à une vie privée sur leur lieu de travail qui se matérialise par une connexion à Internet à des fins personnelles. Toujours selon le même auteur, cette opportunité est pour eux la contrepartie de la porosité entre la sphère professionnelle et la sphère privée intensifiée par l'utilisation des nouvelles technologies. Afin d'encadrer et de limiter un usage excessif de l'Internet sur le lieu de travail, l'employeur dispose au titre de son pouvoir de direction d'un droit de contrôle et de surveillance sur ses

salariés. Mais ce pouvoir reconnu à l'employeur ne doit pas méconnaître les principes du droit à la vie privée et du secret des correspondances.

En effet, en France, la Commission Nationale de l'Informatique et des Libertés (CNIL) a reconnu au salarié le droit à une vie privée au travail en soulignant qu'il était à la fois irréaliste et disproportionné d'interdire strictement une utilisation d'Internet à des fins personnelles.[5] Subséquemment et en accord avec LIMONCELLI (2007 :95), l'administrateur réseau est au carrefour de ses deux logiques. En effet, il est la personne en charge d'assurer à la fois la sécurité du réseau, à la demande de son autorité hiérarchique qui voit en lui un moyen de faire face aux situations périlleuses, et la sécurité des données professionnelles et personnelles des salariés. Il prévient l'intrusion de virus, veille à l'utilisation optimale du réseau et assure la sécurité des données de l'entreprise. Ses principales activités peuvent être déclinées comme suit :

- « Il identifie les facteurs de qualité de service, définit les outils d'analyse des performances ainsi que les méthodes et les règles de gestion du réseau. Il étudie, préconise et supervise l'implantation des matériels et logiciels correspondants.
- Il suit et analyse les performances de ces systèmes, s'assure du traitement des incidents ou anomalies (diagnostic et résolution) en pilotant les interventions.
- Il décide des procédures à mettre en œuvre afin de garantir la continuité du fonctionnement (plans de secours des réseaux).
- Pour veiller à une bonne gestion économique des moyens de communication dont il a la charge, il a une vue d'ensemble des équipements et des systèmes de communication utilisés par son entreprise.
- En relation avec les fournisseurs, il assure une veille technologique sur les produits matériels et logiciels de son domaine. »[6]

Dans certains pays, selon les législations, il lui est conféré l'obligation d'assurer la sécurité des traitements informatiques. Aussi, s'engage t'il, vis-à-vis des personnes concernées, à prendre toutes les précautions utiles afin de préserver la sécurité des informations et notamment d'empêcher qu'elles ne soient déformées, endommagées ou communiquées à des tiers non-autorisés.

[5] Rapport du 5 février 2002 de la CNIL concernant la « Cyber surveillance sur les lieux de travail »
[6] Extrait du référentiel des métiers du GET

1.2.3. Compétences nécessaires d'un administrateur réseau

« Comme l'ingénieur réseau, l'administrateur réseau travaille pour des entreprises où les réseaux atteignent un haut niveau de complexité et de contrainte, qu'il soit directement employé par l'entreprise ou détaché par une SSII (Société de Service en Ingénierie Informatique) », FORAY (2007 :55). Chez un opérateur, il travaille dans les équipes de supervision du réseau ou, en se spécialisant sur certains équipements, dans des équipes de support technique.[7]

Il doit posséder des connaissances très pointues en réseaux et télécom, ouvertes sur d'autres disciplines et avoir des connaissances spécifiques des techniques utilisées par l'entreprise. Ce métier demande de la curiosité technique, des capacités d'analyse et de la rigueur. Il suppose une bonne autonomie et une réactivité face aux problèmes techniques. De bonnes capacités relationnelles et le sens du service sont également importants. Bien que proposé parfois à un débutant, c'est un métier qui nécessite le plus souvent plusieurs années d'expériences pour maîtriser à la fois l'expertise technique et les aspects gestion.[8]

1.2.4. Limites de l'administrateur réseau

En accord avec FOUQUET (2000 : 75), l'administrateur réseau, appelé aussi gestionnaire des ressources ou superviseur, bien que possédant des attributs qui autorisent à mener des actions dans le cadre de sa mission, doit respecter certains domaines et aspects relevant de la vie privée ou de sa position hiérarchique. Ainsi, certaines règles érigées en mode de contrôle guideront ces actions.

Un contrôle loyal : la démarche de l'administrateur doit être impartiale et sincère. Il doit agir dans le cadre de ses fonctions et son action ne doit pas découler d'une initiative personnelle ou d'un ordre hiérarchique mais d'une nécessité justifiée par des impératifs de sécurité. Il appartient à l'administrateur d'agir dans le respect de la vie privée des salariés.

Un contrôle transparent : la démarche de l'administrateur doit se faire dans une logique de transparence vis à vis des salariés. Ces derniers doivent être informés par l'employeur de la mise en place d'un dispositif de contrôle soit en le spécifiant dans le con-

---

[7] Extrait de www.institut-telecom.fr
[8] Extrait du référentiel des métiers du GET

trat de travail soit au moyen d'une charte informatique. [9]Le comité d'entreprise, ou à défaut les délégués du personnel, devra avoir été informé et consulté préalablement pour la mise en place d'un tel dispositif de contrôle. [10]

Un contrôle proportionné : le contrôle qu'il soit effectué par le supérieur hiérarchique en vertu de son pouvoir hiérarchique ou par l'administrateur réseau dans le cadre de sa fonction doit être proportionnel au but recherché.[11] « Il appartient à l'administrateur d'utiliser les moyens permettant de remplir sa mission sans aller au-delà. Il n'y a pas lieu pour l'administrateur réseau de contrôler le contenu même des messages émis ou reçus si le seul contrôle du volume des pièces jointes ou des extensions des fichiers joints lui permet de vérifier l'utilisation optimale du réseau. Son action doit s'inscrire dans une logique cohérente », (FOUQUET, 2000 : 75).

1.2.5. Techniques d'administration du réseau informatique

Dans ce volet, nous nous limiterons aux observations du trafic sur le réseau. En effet, le réseau peut présenter un dysfonctionnement et que, malgré toutes les investigations, le problème n'ait toujours pas été identifié. Il ne reste plus qu'à l'ausculter, c'est-à-dire observer les données qui y circulent. Même lorsque le réseau semble bien fonctionner, il n'est pas inutile d'y jeter un coup d'œil car bien souvent des erreurs (collisions, paquets corrompus, flux non identifié, trafic censé ne pas être présent sur ce segment, etc.) se produisent. Ces erreurs ne sont alors pas perceptibles, mais peuvent le devenir sous certaines conditions, par exemple lorsque la charge réseau augmente. Une maintenance préventive permet donc d'éviter le pire.

L'analyseur réseau est l'outil tout indiqué pour ce type de situation. C'est un logiciel capable de décoder idéalement tous les protocoles existants, du niveau 2 au niveau de

---

[9] Article L.121-8-1 du Code du Travail Français : « aucune information concernant personnellement un salarié ou un candidat ne peut être collectée par un dispositif qui n'a pas été porté préalablement à sa connaissance ».

[10] Article L 432-2 du Code du travail Français: « le comité d'entreprise est informé et consulté préalablement à tout projet important d'instruction de nouvelles technologies, lorsque celles-ci sont susceptibles d'avoir des conséquences sur les conditions de travail du personnel »

[11] Art L 120-2 du Code du Travail Français: « nul ne peut apporter au droit des personnes et aux libertés individuelles et collectives des restrictions qui ne seraient pas proportionnées au but recherché »

session. Il fonctionne de concert avec une carte réseau, de préférence haut de gamme. Il permet :

- « de capturer toutes les trames qui circulent sur un segment Ethernet ;
- d'analyser le contenu de toutes les couches réseau, de la trame aux données applicatives en passant par le paquet IP ;
- de déterminer si des erreurs se produisent (collision, erreur de transmission, etc.) et quelle proportion ;
- de connaître les temps de réponse précis », SMONI & ZNATY (1997 :55).

Dans le champ de l'administration du réseau, s'inscrit une autre composante à savoir la sécurité du réseau. Le réseau avec accès à internet ou de par les agissements des utilisateurs internes, est une cible potentielle. A cet effet, les lignes prochaines seront consacrées au volet sécuritaire du réseau.

1.3. Sécurité du réseau informatique

En concordance avec PUJOLLE (2008 :869), avec un peu de sens commun et de vigilance, il est possible d'éviter des dégâts éventuels, en bloquant les agresseurs potentiels. Soulignons, en outre, que la sécurité ne consiste pas à protéger l'ordinateur d'une agression mais à protéger l'information qui y circule. Avant d'aborder les développements propres à la sécurité dans le cadre de l'intranet, nous présenterons certaines remarques d'ordre plus général concernant les problèmes de défaillances et les fraudes, les menaces venant de l'intérieur de l'organisation et les mesures de sécurité classiques qui s'imposent en particulier, les firewalls ou pare-feux.

1.3.1. Définition de la sécurité du réseau informatique

La sécurité est une fonction incontournable des réseaux. Puisqu'on ne voit pas son correspondant directement, il faut l'authentifier. Puisqu'on ne sait pas par où passent les données, il faut les chiffrer. Puisqu'on ne sait pas si quelqu'un ne va pas modifier les informations émises, il faut vérifier leur intégrité. Nous pourrions ajouter une longue suite de requêtes du même genre qui doivent être prises en charge par les réseaux.

Selon PUJOLLE (2008 :870), la sécurité du réseau peut être définie en s'appuyant sur les thèmes clés qu'elle englobe à savoir :

- l'authentification, permettant de s'assurer de l'identité pour connaître l'origine des opérations ;
- la confidentialité, qui a pour but d'éviter toute divulgation d'informations ;
- l'intégrité, pour interdire ou connaître les modifications et se préserver des pertes d'informations ;
- la disponibilité, qui permet d'assurer un service en toute circonstance.

En complément de ces quatre thèmes peut être ajoutée la notion de non-répudiation. Elle a pour but de s'assurer, en toutes circonstances, de l'origine d'une communication ou d'un transfert d'informations. Pour cela, elle reprend un concept familier de notre vie quotidienne, la signature, ici sous forme électronique.

1.3.2. Objets de sécurité du réseau informatique

Inutile de se préoccuper de sécurité sans avoir défini ce qui était à protéger : en d'autres termes toute organisation désireuse de protéger ses systèmes et ses réseaux doit déterminer son périmètre de sécurité. Le périmètre de sécurité, au sein de l'univers physique, délimite l'intérieur et l'extérieur, mais sa définition doit aussi englober (ou pas) les entités immatérielles qui peuplent les ordinateurs et les réseaux, essentiellement les logiciels et en particulier les systèmes d'exploitation.

Conformément à BLOCH & WOLFHUGEL (2003 :10), la notion de périmètre de sécurité, ainsi que le signalait déjà l'alinéa précédent, devient de plus en plus fragile au fur et à mesure que les frontières entre l'extérieur et l'intérieur de l'entreprise ainsi qu'entre les pays deviennent plus floues et plus poreuses. Interviennent ici des considérations topographiques : les ordinateurs portables entrent et sortent des locaux et des réseaux internes pour aller se faire contaminer à l'extérieur ; mais aussi des considérations logiques : quelles sont les lois et les règles qui peuvent s'appliquer à un serveur hébergé aux États-Unis, qui appartient à une entreprise française et qui sert des clients brésiliens et canadiens? Question phare qui retient toujours l'attention des législateurs.

La sécurité d'un réseau repose avant tout sur la sécurité des équipements ou systèmes réseau qui le composent. Cette dernière, d'après LLORENS (2006 :221), concerne les trois domaines principaux suivants :

- Sécurité physique. Il s'agit de la protection des équipements réseau face aux menaces de feu, d'inondation, de panne de courant, etc. Des équipements de protection tels qu'extincteurs, onduleurs, etc., permettent de se protéger de ces menaces.
- Sécurité du système d'exploitation (operating system). Il s'agit de se prémunir des faiblesses de sécurité ou des bogues du système d'exploitation qui s'exécutent sur l'équipement réseau. Seuls des tests de non-régression et de sécurité permettent de détecter certaines de ces faiblesses.
- Sécurité logique. Il s'agit de se prémunir des faiblesses de configuration de l'équipement ou du système réseau. Seules des règles de configuration sécurisées permettent de se prémunir contre ce type d'erreur.

La sécurité du système d'exploitation est difficile à maîtriser, du fait que ce dernier est généralement propriétaire et que les sources ne sont pas disponibles. En revanche, la sécurité physique et la sécurité logique des équipements réseau et des systèmes sont des axes majeurs de la politique de sécurité réseau, dont on parlera ultérieurement.

1.3.3. Attaques et vulnérabilités sur le réseau informatique

LLORENS (2006 :24) dresse un panorama des attaques sur le réseau selon la typologie suivante :

- les attaques réseaux ;
- Les attaques systèmes réseaux ;
- Les attaques indirectes réseaux ;

1.3.3.1. Les attaques réseaux

Les attaques réseaux sont aujourd'hui si nombreuses qu'il serait illusoire de prétendre les décrire toutes. Il est cependant possible de dresser une typologie des faiblesses de sécurité afin de mieux appréhender ces attaques, qui ont pour point commun d'exploiter des faiblesses de sécurité.

Les attaques réseau peuvent être lancées directement ou indirectement. En procédant à une classification de ces différentes attaques, nous obtenons, LLORENS (2006 :26) :

- attaques permettant de dévoiler le réseau ;
- attaques permettant d'écouter le trafic réseaux ;
- attaques permettant d'utiliser des accès distants Wifi ;
- attaque permettant d'interférer avec une station réseau ;
- attaque permettant de modifier le routage réseau ;
- attaque permettant de mettre le réseau en déni de service;
- autres formes d'attaque.
    - « L'accès physique aux équipements réseau permet de prendre la main en tant qu'administrateur sur pratiquement tous les systèmes actuels.
    - La copie des configurations des équipements réseau est une attaque redoutable, qui permet au pirate de reconstituer tout le réseau logique ainsi que les protections mises en place.
    - L'écoute électronique pour récolte d'information peut permettre de mener des attaques ciblées. Les diverses techniques d'écoute disponibles actuellement permettent d'écouter n'importe quel type de média.
    - Le vol de secret se rencontre plus fréquemment dans l'ingénierie sociale. Par exemple, l'agresseur entre en contact avec la personne qu'il veut usurper en se faisant passer pour un technicien en intervention bloqué dans son travail par une demande d'authentification ou une permission trop forte. Pour peu qu'il soit convaincant, l'agresseur peut obtenir les couples compte/mot de passe ou permissions qu'il désire, voire directement ceux de l'administrateur système. Une variante de cette attaque consiste à obtenir un compte privilégié créé directement par un administrateur trouvant cette procédure plus sécurisée. », NORTHCUTT & NOVAK (2004 :45).

1.3.3.2. Les attaques systèmes réseaux

D'après CALE & TOUITOU (2007 :75), la prise de contrôle d'un système par un pirate est beaucoup plus nuisible dans l'absolu pour l'entreprise, car le pirate peut dès lors installer des outils dévastateurs sur le système pénétré. Entre le moment où le pirate peut examiner un système cible et celui où il réussit à le pénétrer, un certain nombre d'étapes

doivent être franchies. Le pirate doit d'abord découvrir les services réseau offerts par le système, puis estimer l'attrait de chacun d'eux en termes de possibilités de pénétration (risque intrinsèque du service, vulnérabilités, etc.) et enfin faire le choix de ceux qui présentent la meilleure chance de pénétrer le système le plus discrètement possible. Les différents types d'attaques sont :

- Attaques permettant d'identifier les services réseaux.
- Attaques permettant de pénétrer le système.
- Exploitation des faiblesses ou vulnérabilités.

Les techniques d'attaques des systèmes réseau sont nombreuses et variées. La publication de programmes permettant d'exploiter les vulnérabilités des systèmes ne renforce évidemment pas la sécurité de ces systèmes et met gratuitement à la disposition des pirates des outils redoutables. La pénétration de tels systèmes peut mettre en péril la sécurité de l'ensemble du réseau et de ses services. Si les serveurs DNS (Domain Name Service) d'un opérateur de télécommunications venaient à être indisponibles, par exemple, le réseau entier et ses services pourraient s'en trouver paralysés.

1.3.3.3. Les attaques indirectes réseaux

Le présent point traite des autres types d'attaques susceptibles d'impacter le réseau de manière indirecte en provoquant des phénomènes de saturation ou de congestion du réseau. Ces autres formes d'attaques réseau s'appuient principalement sur les faiblesses des applications. Ainsi nous distinguons, conformément à LLORENS (2006 :67) :

- attaque par virus : on peut qualifier de virus tout programme, sous quelque forme que ce soit, capable de se reproduire par lui-même. Les virus ont pour caractéristique commune une volonté de nuire. Cette volonté peut prendre la forme d'une routine, ou programme, qui, une fois activée, use de tous les moyens à sa disposition pour empoisonner la vie de l'utilisateur. « Les virus ont donc un degré de nuisance variable. Quel que soit ce dernier, ils doivent être éradiqués, car ils font peser une menace constante sur les systèmes informatiques. Il existe différents types de virus, dont le comportement, la mise en place ou la capacité d'être détectés sont extrêmement variables. »[12]

[12] Extrait de CLUSIF, les virus informatiques (2005 :10)

- Attaques par relais : les attaques par relais peuvent impacter le réseau ainsi que les services réseau. Un relais peut être un système de messagerie fondé sur le protocole SMTP (Simple Mail Transfer Protocol) ou un système de résolution de noms de domaine à l'aide du protocole DNS.

1.3.4. Politique de sécurité du réseau informatique

Elle est constituée d'une suite de règles et de principes répondant aux besoins de sécurité de l'entreprise et dont le management est le support numéro 1 pour une bonne intégration au sein de l'entreprise. Son objectif est de protéger les éléments critiques de l'entreprise afin d'assurer sa pérennité en cas d'incident de sécurité. La définition d'une politique de sécurité réseau n'est pas un exercice de style mais une démarche de toute l'entreprise visant à protéger son personnel et ses biens d'éventuels incidents de sécurité dommageables pour son activité. En cela, selon FERRERO (1995 :45), elle fait intégralement partie de la démarche sécuritaire de l'entreprise et s'étend à de nombreux domaines, notamment les suivants :

- audit des éléments physiques, techniques et logiques constituant le système d'information de l'entreprise ;
- sensibilisation des responsables de l'entreprise et du personnel aux incidents de sécurité et aux risques associés ;
- formation du personnel utilisant les moyens informatiques du système d'information ;
- structuration et protection des locaux abritant les systèmes informatiques et les équipements de télécommunications, incluant le réseau et les matériels ;
- ingénierie et maîtrise d'œuvre des projets, incluant les contraintes de sécurité dès la phase de conception ;
- gestion du système d'information de l'entreprise lui permettant de suivre et d'appliquer les recommandations de sécurité des procédures opérationnelles ;
- définition du cadre juridique et réglementaire de l'entreprise à l'égard de la politique de sécurité et aux actes de malveillance, 80 % des actes malveillants provenant de l'intérieur de l'entreprise ;
- classification des informations de l'entreprise selon différents niveaux de confidentialité et de criticité.

Avant de définir une politique de sécurité réseau, il est essentiel d'en connaître les principes génériques. Différents organismes officiels se penchent depuis plusieurs années sur cette question mais nous n'évoquerons que que la norme ISO 17799 d'ISO. La norme ISO 17799 est issue de la norme anglaise BS 7799 créée en 1995 et révisée en 1999. Cette norme constitue un code de bonnes pratiques pour la gestion de la sécurité de l'information. Elle fait l'objet en Grande-Bretagne d'un schéma de certification, qui permet aux entreprises anglaises d'être référencées. Un client qui opère avec ces entreprises a ainsi la garantie que ses informations sont gérées de manière plus ou moins sécurisée, car un certain nombre de mesures techniques ou non techniques ont été mises en place. À cette norme s'ajoutent d'autres en cours de révision ou non, notamment les suivantes :

- BS 7799 (code de pratiques pour la gestion de la sécurité de l'information) et BS 7799- 2 (système de management de la sécurité de l'information) ;
- ISO 27005(gestion de la sécurité des systèmes d'information) ;
- ISO 13335 (système de management de la sécurité de l'information) ;
- ISO 19011 (audit des systèmes de management de la qualité).

Et le COBIT 4.1 (Control Objectives of Information technologies) qui est aussi un répertoire de « best practices » traitant de la gouvernance et la gestion des technologies de l'information.

Toutefois, le fait de définir une politique de sécurité ne signifie pas nécessairement qu'elle soit implémentée ni, si elle est implémentée, qu'elle le soit toujours demain.

1.3.5. Mécanismes de défenses du réseau informatique

L'ISO s'est attachée à prendre toutes les mesures nécessaires à la sécurité des données durant leur transmission. Ces travaux ont donné naissance à un standard d'architecture international, ISO 7498-2 (OSI Basic Reference- Model-Part 2: Security Architecture). Cette architecture est très utile pour tous ceux qui veulent implémenter des éléments de sécurité dans un réseau car elle décrit en détail les grandes fonctionnalités et leur emplacement par rapport au modèle de référence. Trois grands concepts ont été définis :

- Les fonctions de sécurité, qui sont déterminées par les actions pouvant compromettre la sécurité d'un établissement.

- Les mécanismes de sécurité, qui définissent les algorithmes à mettre en œuvre.
- Les services de sécurité, qui représentent les logiciels et les matériels mettant en œuvre des mécanismes dans le but de mettre à la disposition des utilisateurs les fonctions de sécurité dont ils ont besoin.

Dans cette section, nous évoquerons les certificats de sécurité ainsi que de l'algorithme de chiffrement.

- Les certificats

« Une difficulté qui s'impose à la station d'un réseau qui communique avec beaucoup d'interlocuteurs consiste à se rappeler de toutes les clés publiques dont elle a besoin pour récupérer les clés secrètes de session. Pour cela, il faut utiliser un service sécurisé et fiable, qui délivre des certificats. Un organisme offrant un service de gestion de clés publiques est une autorité de certification, appelée tiers de confiance », PUJOLLE (2008 :875).

- Les algorithmes de chiffrement

D'après PUJOLLE (2008 :872), les plus classiques utilisés sont DES (Data Encryption Standard) et 3 DES. Le chiffrement est la méthode suivie pour que l'information ne puisse pas être lue par une autre personne que le destinataire. Toutefois, les techniques de chiffrement utilisées sont à priori violables, mais il faudrait pour une cela utiliser une machine extrêmement puissante et la faire tourner pendant plusieurs années. Nous avons aussi AES (Advanced Encryption Standard) qui se présente aujourd'hui comme le remplaçant des standards précités.

1.3.6. Architecture du dispositif de défense du réseau

Dans cette partie, nous parlons essentiellement des firewalls en ayant un aperçu sur leur architecture, leur mode de fonctionnement et d'autres aspects. Un pare-feu ou coupe-feu ou encore firewall est comme son nom l'indique, un équipement dont l'objectif est de séparer le monde extérieur du monde intérieur à protéger. Son rôle est de ne laisser entrer que les paquets dont l'entreprise est sûre qu'ils ne posent pas de problème. Toute la question est alors de savoir comment reconnaître les paquets à accepter et à refuser. Il est possible de travailler de deux façons :

- interdire tous les paquets sauf ceux d'une liste prédéterminée ;

- accepter tous les paquets sauf ceux d'une liste prédéterminée.

Selon MONTAIGNER (2004 : 464), le firewall se charge en général d'accomplir les fonctions ci-dessous :

- protection active contre les attaques ;
- détection d'intrusion ;
- filtrage des paquets IP sur la base des adresses et des ports source et destination ;
- filtrage des commandes applicatives (http, FTP, DNS, etc.) ;
- authentification des utilisateurs, permettant ainsi de filtrer les accès aux sessions par utilisateurs et non plus sur la base des adresses IP sources ;
- chiffrement et intégrité des données à l'aide du protocole IPsec ;
- décontamination anti-virus, le plus souvent avec un serveur dédié à cette tâche ;
- filtrage des composants actis (ActiveX, applet Java, Java Scripts).

Conclusion

Les politiques édictées, la gestion clarifiée, les attaques identifiées et les mécanismes déterminés, l'entreprise doit savoir détecter les risques que son réseau et elle encourent ainsi que les méthodes de maîtrise de ceux-ci. Tels sont les volets que nous aborderons au chapitre suivant.

Chapitre 2 : Dispositif et évaluation de la maîtrise des risques liés au réseau informatique

Introduction

La valeur de l'organisation est maximisée d'une part lorsque la direction élabore une stratégie et fixe des objectifs afin de parvenir à un équilibre optimal entre les ambitions de croissance, de rendement et les risques associés, et d'autre part lorsqu'elle déploie les ressources adaptées permettant d'atteindre ces objectifs. En effet, l'entreprise dans cet environnement fort concurrentiel, doit avoir un œil attentif et rigoureux sur ces dispositifs de contrôle interne lui permettant de créer la plus value en particulier, ce qui concerne notre étude, celui du réseau informatique. En outre, les risques qui chevauchent les sentiers de la réussite doivent être connus et les méthodes d'appréhension de ceux-ci édictées et appliquées. Dès lors, nous rentrons dans le cadre du management des risques qui offre la possibilité d'apporter une réponse efficace aux risques et opportunités auxquelles l'organisation fait face, renforçant de facto la capacité de création de valeur de l'organisation. Aussi, une fois le dispositif mis en place, son évaluation permanente s'impose, de même que l'identification et l'évaluation des risques qu'il doit annihiler.

2.1. Dispositif de maîtrise des risques

Le Larousse 2012 définit le dispositif tel qu'un ensemble de mesures prises, de moyens mis en œuvre pour une intervention précise ; laquelle intervention est ici, la maîtrise des risques. Au cours des dernières années, l'augmentation des risques dans l'économie et la fréquence des défaillances d'entreprise ont mis en évidence la nécessité de disposer d'outils de pilotage et de contrôle de plus en plus efficace. En effet, l'incertitude étant une donnée intrinsèque à la vie de toute organisation, il convient de mettre en place en amont ce qui endiguera ces risques mais aussi un enchaînement itératif et continu d'actions visant, en aval, à manager ces risques, qui qu'on le veuille ou non, émaillent la vie de nos entités.

2.1.1. Notion de risque

Les organisations opèrent dans un environnement dans lequel des facteurs tels que la mondialisation, la technologie, les restructurations, l'évolution des marchés, la concurrence et la règlementation engendrent des incertitudes. L'incertitude est liée à l'incapacité pour l'entité de déterminer précisément quels évènements pourraient survenir et quels en sont les probabilités d'occurrence et l'impact. L'incertitude résulte également des choix stratégiques. Elle est fortement liée à la notion de valeur et peut revêtir des risques comme des opportunités.

2.1.1.1. Définition du risque

La survenance d'un évènement d'origine interne ou externe peut avoir des répercussions sur l'atteinte des objectifs. Les évènements peuvent avoir un impact négatif ou positif ou les deux simultanément. Les évènements ayant un impact négatif constituent les risques.

L'IFACI[13] & al (2005 :23) définit le risque comme : « la possibilité qu'un évènement survienne et nuise à l'atteinte d'objectifs ». Nous rajouterons que le risque est la menace qu'un évènement, une action ou une situation affecte la capacité de l'entreprise à atteindre ces objectifs d'activité, de sauvegarde du patrimoine et/où à maximiser sa performance. Effectivement, les évènements ayant un impact négatif, tels que des pannes, des incendies, des virus, empêcheront la création de valeur et/ou provoqueront une destruction de la valeur existante.

2.1.1.2. Typologie générale des risques

La typologie demeure une convention de regroupement des risques propre à chaque entreprise. Elle évolue progressivement en tenant compte des modalités pratiques de son application sur le terrain. Nous évoquerons, ici, conformément à MOREAU (2002 :75), trois grands niveaux de risques décomposables comme suit:

---

[13] IFACI : Institut Français de l'Audit Interne

- Le risque humain :
    - le risque de gestion des carrières et des compétences ;
    - le risque d'éthique ;
    - le risque social.
- Le risque organisationnel et de traitement :
    - le risque opératoire ;
    - le risque technique et de sécurité ;
    - le risque de management ;
    - le risque légal, règlementaire et judiciaire ;
    - le risque lié aux menaces externes.
- Le risque lié aux systèmes d'informations :
    - le risque lié à la technologie et aux systèmes informatiques (hardware, logiciel, réseau) ;
    - le risque lié à la gestion de l'information.

L'avant-dernier point est celui qui rentre dans le cadre de notre étude et que nous détaillerons au prochain paragraphe. Néanmoins, LAFITTE (2003 :96-97) propose une autre typologie fondée sur le caractère du risque. Ainsi, il distingue :

- Les risques purs qui sont inhérents à l'activité de l'entreprise, avec une occurrence brutale et se traduisant par une perte. Parmi les risques informatiques, l'incendie d'un ordinateur rentre dans cette catégorie.
- Les risques spéculatifs correspondent à un choix délibéré de l'entreprise et a donc une occurrence prévisible pouvant ou non se traduire par une perte.
- Les risques obligatoires qui font l'objet d'une obligation d'assurance.
- Les risques facultatifs non astreints à une couverture obligatoire.
- Les risques anticipés sont ceux qui sont identifiés en tant que tel par l'entreprise et vis-à-vis desquels l'entreprise prend des mesures conservatoires.
- Les risques subis sont des risques identifiés ou non mais contre lesquels l'entreprise ne prend pas de mesures particulières de sauvegarde.

Nous retiendrons, que cette typologie peut s'insérer dans la première citée en mettant en exergue une classification par nature c'est-à-dire lié à un domaine bien précis et par caractère.

2.1.1.3. Les risques spécifiques au réseau informatique

Divers épisodes médiatiques ont éveillé les esprits sur les risques informatiques qu'encourent les entreprises, sans forcément attribuer à chaque risque la part qu'il mérite. Les risques liés au réseau informatique sont les suivants (CALE & TOUITOU, 2007 : 43-82) :

- Les malwares : terme générique qui désigne l'ensemble des programmes malveillants qui peuvent être utilisés par des pirates afin de commettre leurs méfaits :
    - les virus ;
    - les vers ;
    - le cheval de troie ;
    - back door ;
    - logiciels espions.
- Les spams qui désignent l'envoi massif de courriers publicitaires dans les boîtes aux lettres électroniques de personnes qui n'ont pas exprimé le souhait de les recevoir.
- Les facteurs humains : « la plus grande menace de la sécurité informatique d'une entreprise n'est pas le virus, la faille de sécurité non corrigée ou un firewall mal installé, en fait, la plus grande menace pourrait être vous. »[14]
    - Erreurs humaines ;
    - atteinte à la disponibilité ;
    - compromission de l'information ;
    - usurpation d'identité ;
    - le déni de service.

Toutefois ces risques peuvent être liés soit au caractère physique du réseau tel que les incendies ou au caractère logique comme les vers. Nos développements futurs seront articulés autour de l'aspect logique dont les risques liés au réseau sont essentiellement d'origine humaine :

- soit lorsque les informaticiens ou les utilisateurs créent eux-mêmes des situations illogiques, voire dangereuses ;
- soit sous le feu d'attaques externes criminelles.

[14] Extrait de vulnerabilité.com

L'entité ayant connaissance des risques qu'elle court, des actions doivent être orchestrées pour soit prémunir l'entreprise, soit guérir lorsque le mal est déjà présent.

2.1.1.4. Définition d'un service de sécurité

« Un service de sécurité est une réponse à une besoin de sécurité, exprimée en termes génériques et fonctionnels décrivant la finalité du service, généralement en référence à certains types de menaces », MEHARI-DIAGNOSTIC (2010 :6). Un service de sécurité décrit donc une fonction de sécurité ; laquelle est indépendante des mécanismes et solutions concrètes permettant la réalisation effective du service.

Un mécanisme sera donc une manière particulière d'assurer, totalement ou partiellement, la fonction du service ou du sous-service. Il peut s'agir de procédure spécifique, d'algorithme, de technologie, etc. Partant de cela, la solution de sécurité sera perçue comme la réalisation concrète d'un mécanisme de sécurité et comprend les matériels et logiciels nécessaires à son déploiement, les procédures de déploiement et de support opérationnel ainsi que les structures organisationnelles nécessaires.

2.1.2. Le dispositif de contrôle interne

Les dirigeants d'entreprises ont pour préoccupation constante de mieux maîtriser les activités dont ils ont la responsabilité. Des systèmes de contrôle interne sont mis en place afin de détecter, en temps voulu, tout dérapage par rapport aux objectifs de rentabilité visés par l'entreprise, et de limiter les aléas. Ces dispositifs permettent aux dirigeants de freiner l'évolution rapide de l'environnement économique concurrentiel, des besoins et des priorités des clients, et de procéder à temps aux adaptations nécessaires à la croissance de l'activité. Se référant à COOPERS & LYBRAND (2000 :14) : « Le contrôle interne est un processus mis en œuvre par la direction générale, la hiérarchie, le personnel d'une entreprise et destiné à fournir une assurance raisonnable quant à la réalisation d'objectifs entrant dans les catégories suivantes :

- réalisation et optimisation des opérations ;
- fiabilité des informations financières ;

- conformité aux lois et règlementations en vigueur. »

2.1.2.1. Dispositif de maîtrise des risques relatifs au réseau informatique

Toute personne dans l'entreprise, du conseil d'administration aux vigiles, a un rôle à jouer dans la gestion des risques. Le personnel est un facteur clé pour la réussite et chaque personne doit comprendre la mission de l'organisation, et doit adhérer aux valeurs énoncées pour que les procédures de maitrise des risques aboutissent.

LLORENS & AL (2006 :337) soulignent que le contrôle interne de la sécurité du réseau informatique porte sur les analyses suivantes :

- Analyse de la configuration des équipements réseau (routeurs, commutateurs, services réseau critiques, comme DNS, NTP, etc.).
- Analyse de la configuration des systèmes d'information qui sont hébergés par le réseau, généralement des serveurs ou des stations de travail.
- Utilisation d'équipements de sécurité chargés de faire de l'écoute passive du réseau et analyse de leurs journaux d'activité ou messages.

Avant d'aborder les questions d'analyses comme le démontre LLORENS, faisons cas des parades techniques et organisationnelles que l'entreprise met en place afin de repousser les négations de son réseau, (CALE & TOUITOU, 2007 :85-168) :

- Parades techniques :
    - firewall ;
    - serveurs relais ;
    - protection contre les codes malicieux et le spam ;
    - anti-spam ;
    - système de prévention et de détection contre les intrusions ;
    - logiciel d'audit ;
    - réseau privé virtuel ;
    - protection de l'information par cryptographie ;
    - gestion des identités et des autorisations ;
    - contrôle d'admission réseau.
- Parades organisationnelles :
    - politique de sécurité ;

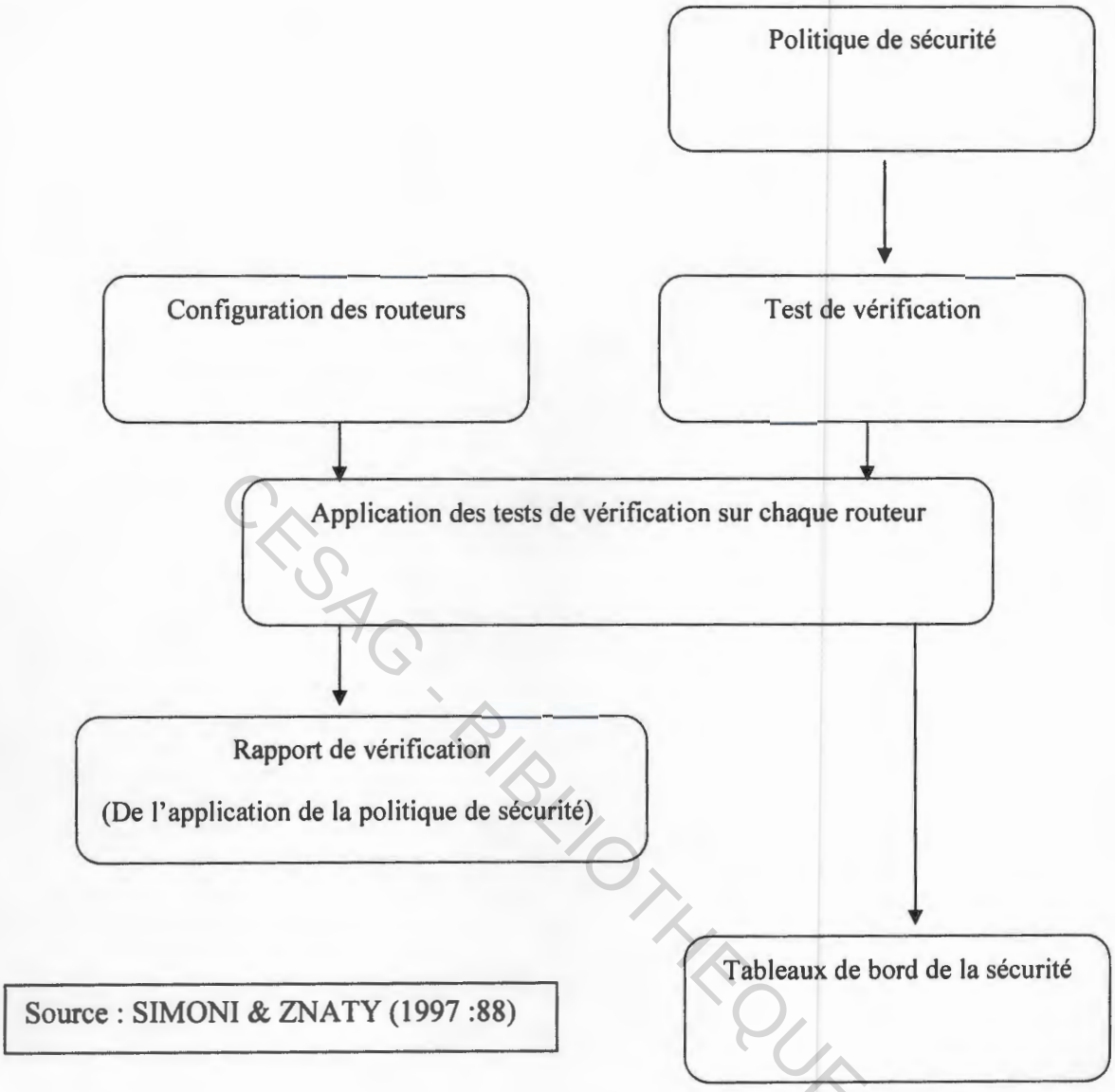
- gestion des risques ;
- traitement des risques ;
- veille technologique règlementaire.

Le contrôle du système contrôle interne doit être effectué régulièrement, une fois par jour, par semaine ou par mois, et automatisé au maximum afin de gagner du temps pour l'analyse des données. Il doit tenir compte des évolutions de la politique de sécurité, mais également de celle des architectures, des services réseau, des systèmes d'information et des risques. Toutefois, il est toujours difficile d'observer un contrôle interne optimal en tout point compte tenu de ces diverses évolutions.

2.1.2.2. Analyse de la configuration des équipements du réseau

La configuration des équipements réseau (commutateurs, routeurs, pare-feux, etc.) représente la sécurité logique du réseau. « Cette sécurité logique se traduit par des règles de configuration précises réalisées sur ces équipements, telles que la configuration des règles de filtrage d'un pare-feu, d'un routeur, etc. Toutes ces règles représentent l'implémentation de la politique de sécurité réseau », (LLORENS, 2006 :361).

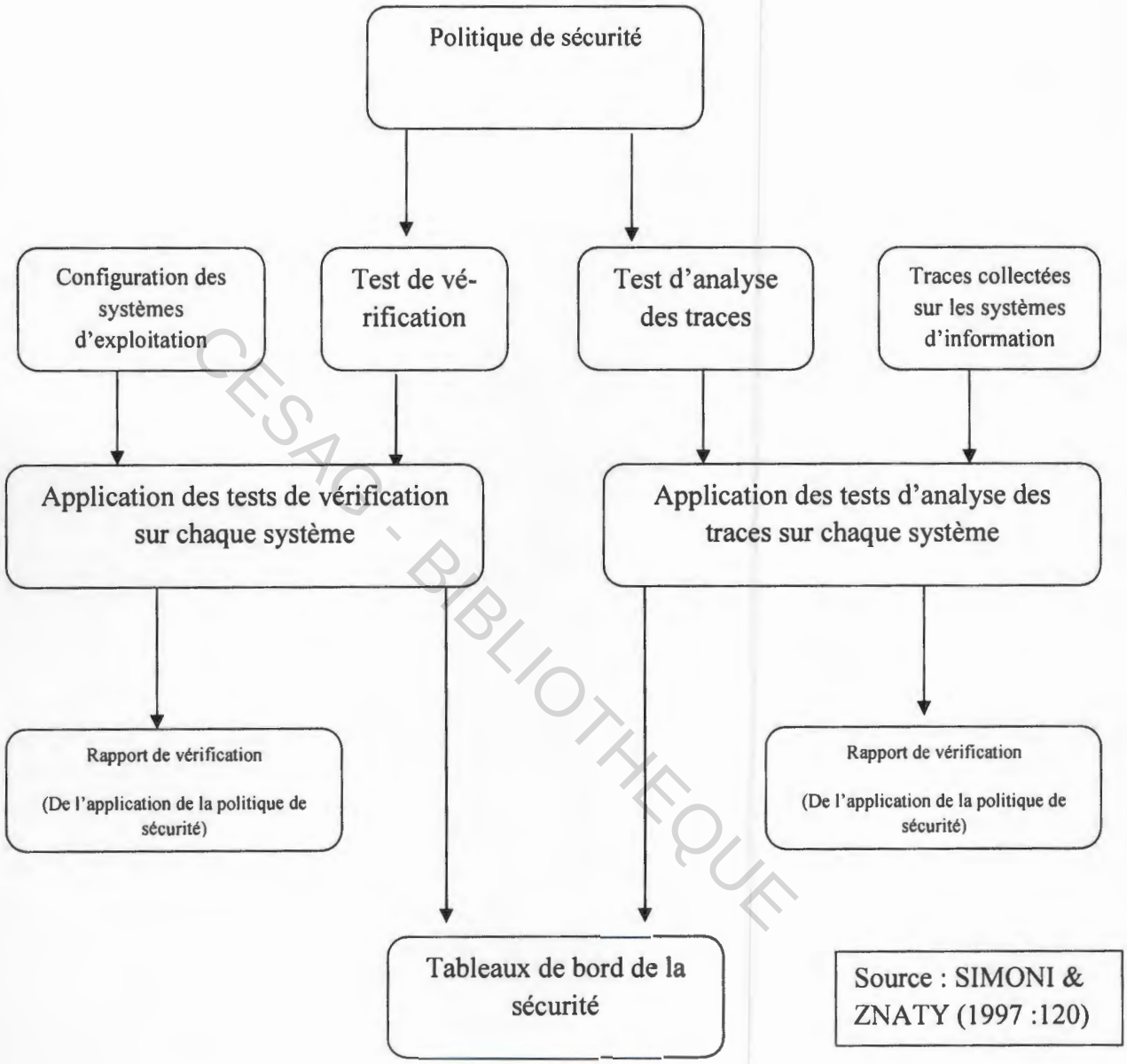
Des problèmes de consistance de la configuration des équipements réseau ou des erreurs de configuration, qu'elles soient volontaires ou involontaires, peuvent mettre en danger le réseau mais aussi les équipements attachés au réseau. Suivant une hypothèse de TANEMBAUM (2002 :89), imaginons qu'une personne mal intentionnée prenne pied sur un routeur de l'intranet de l'entreprise suite à une faiblesse de configuration des accès en administration. Cette personne peut modifier des filtres, les mots de passe de l'équipement, écouter le réseau au travers d'un tunnel GRE (Generic Routing Encapsulation), faire chuter le réseau intranet en altérant les tables de routage, etc. Altérer un processus de routage est simple, rapide et généralement efficace : plus de routage, plus de trafic, et donc plus de réseau. L'analyse de la configuration des équipements réseau est donc un axe majeur de la sécurité du réseau. Voyons à présent le déroulement d'une procédure de vérification des configurations des équipements réseau.



Source : SIMONI & ZNATY (1997 :88)

Suivant ATELIN (2006 :67), les équipements de sécurité passifs, tels que sondes de détection d'intrusion IDS (Intrusion Detection System), tables d'écoute, pots de miel (honeypots) ou sondes de prévention d'intrusion IPS (Intrusion Preventing System), n'ont pas pour fonction de protéger le réseau ou le système d'information. Ils sont chargés d'effectuer des contrôles proactifs ou réactifs du réseau, selon la manière dont ils sont paramétrés et contrôlés. Puisque ces équipements n'ont habituellement pas un rôle actif dans le réseau (sinon on pourrait les utiliser contre celui-ci), c'est l'analyse de leurs traces (logs) qui apporte l'information importante. Nous les considérons donc comme faisant partie des contrôles internes de sécurité. La vérification de l'application de la politique de sécurité consiste à définir un contrôle interne de sécurité sur les fichiers de configuration de ces

équipements, mais également de contrôler les traces collectées par ceux-ci. Pour y parvenir, un ensemble d'étapes doivent être accomplies, comme illustré ci-dessous.



2.1.2.3. Analyse de la configuration des systèmes d'information

« Un système d'exploitation offre différents services selon les choix de son administrateur. Chacun de ces services est généralement paramétrable par l'intermédiaire d'un fichier de configuration. Sachant que l'éventail des services réseau existants nécessite une connaissance pointue, il n'est pas rare de trouver des erreurs de configuration qui engen-

drent des faiblesses de sécurité. Comme dans le cas des équipements réseau, les fichiers de configuration sont généralement sous forme texte et peuvent donc être analysés afin d'y détecter des faiblesses », LLORENS (2006 : 361).

Un système de collecte des traces (logs) peut être appliqué à de multiples niveaux, notamment les suivants :

- Tentatives de connexion sur des services réseau (FTP, SSH, etc.) ou tentatives de passer outre le filtrage d'un pare-feu système (IPfilter, IPtables, etc.).
- Tentatives de connexions à des services applicatifs et échanges avec les clients qui les utilisent, telles les URL demandées à un serveur HTTP.
- Tentatives d'obtention de privilèges d'administration sur le système d'exploitation lui-même (commande su sous Unix), messages d'alerte tels que syslog sous Unix, lui même alimenté par tous les services du système d'exploitation, y compris le noyau, etc.

Selon TANEMBAUM (2002 : 90), les services réseau sont généralement les premiers éléments qui sont attaqués par une personne malveillante. Les fichiers de configuration de ces services sont donc souvent la première source de faiblesses. Dans la définition d'un service réseau, certains paramètres sont toujours associés au fonctionnement dudit service. Ainsi, un serveur HTTP peut être exécuté en tant que super utilisateur, avec tous les privilèges possibles du système, ou en tant que simple utilisateur. Un serveur SSH peut autoriser l'accès root direct ou l'interdire. Tous ces paramètres augmentent ou réduisent le niveau de vulnérabilité associé à un service réseau donné. Il est donc nécessaire de contrôler ces fichiers de configuration quand le système d'exploitation le permet.

« Un service réseau est exécuté avec un minimum de privilèges. » SANDOVAL (1996 : 90). Une telle politique de sécurité engendre un certain nombre d'exceptions, notamment les suivantes :

- services réseau qui ne savent pas fonctionner autrement qu'avec tous les privilèges du système.
- Applications mal conçues (souvent des serveurs HTTP), qui ont besoin d'avoir un accès direct à tous les privilèges du système.

Suite aux innombrables attaques qui ont exploité ce type de faiblesse, de plus en plus de services ne réclament pas davantage de privilèges que nécessaire.

Différentes méthodes permettent d'effectuer le contrôle des fichiers de configuration. Cela peut se faire manuellement, en fournissant à un expert de la sécurité les éléments qu'il analysera afin de fournir son évaluation de sécurité. Si le nombre de systèmes est important, cette méthode devient cependant vite ingérable. Il est possible d'automatiser l'accès aux fichiers de configuration par la mise en place d'un standard sur les différents systèmes. Ainsi, un système central peut aller chercher par une méthode de confiance (accès authentifié et chiffré) les fichiers de configuration afin de les rapatrier régulièrement et de les analyser automatiquement.

LLORENS (2006 : 366) affirme que les fichiers de configuration d'un système d'exploitation sont eux aussi fondamentaux pour la sécurité du système. Ils doivent être vérifiés afin de limiter les faiblesses potentielles dudit système face aux attaques externes. Les fichiers de configuration concernent notamment les éléments suivants :

- Les fichiers de configuration des programmes tels que le gestionnaire d'impression, le programme effectuant les sauvegardes de fichiers, etc.
- Les contrôles d'accès (permissions) aux fichiers et répertoires, mais aussi de zones particulières, telles que la mémoire, les périphériques physiques, etc.
- Les mots de passe des utilisateurs.
- Les signatures des exécutables afin de s'assurer qu'ils sont à jour en terme de correctif de sécurité.

Une fois tous ces éléments analysés, un recoupement des informations permet de limiter les attaques initiales du système.

« Chaque utilisateur n'effectue que les actions qui lui sont autorisées. » FOROUZAN (2002 : 372). Il s'agit d'appliquer une politique de séparation des privilèges sur le système d'exploitation. Toujours suivant FOROUZAN (2002 :375), une telle politique signifie qu'un seul compte super utilisateur doit exister et qu'il n'est utilisé que de manière exceptionnelle. Chaque service ne doit disposer que des droits dont il a besoin. Dans le même esprit, un logiciel de sauvegarde a le droit de lire l'intégralité des données dans les zones dont il a la charge, mais ne doit pas pouvoir modifier les permissions. Des outils, tels que CIS-Tools permettent d'assurer une partie de cette analyse. Ce type d'outil, dit de Host Based Security Assessment, a pour mission d'analyser un système d'exploitation de l'intérieur mais n'est pas toujours à même d'analyser la configuration d'un service réseau qui n'est pas fourni d'origine par le système.

Il existe de multiples solutions commerciales d'outils de Host Based Security Assessment, notamment chez Symantec, BindView, NetIQ, etc. De telles solutions sont généralement fondées sur le principe d'agents en charge de lancer les tests sur les machines à contrôler, de contrôleurs de groupes d'agents et de consoles gérant les contrôleurs et mettant en forme les résultats. Les tests sont périodiquement mis à jour, évitant ainsi le fastidieux développement de nouvelles vérifications. La plupart des outils proposent un langage de programmation permettant aux équipes de sécurité de faire leurs propres tests.

2.1.2.4. Analyse des traces

La dernière étape est l'analyse des traces du système d'exploitation. Il s'agit d'analyser des événements du système d'exploitation issus d'un système donné. L'utilisation de commandes permettant de gagner des privilèges telles que su ou sudo ou l'apparition de fichiers core peuvent témoigner d'une situation en relation avec un problème de sécurité.

« Chaque utilisateur n'effectue que les actions qui lui sont autorisées. » (LLORENS 2006 : 372). Une telle politique doit être valable au sein même d'un système d'exploitation. Certaines fonctions des OS (Operating System) sont chargées de n'autoriser l'accès à l'information (fichiers et répertoires) qu'aux comptes autorisés. Selon le système d'exploitation considéré, des traces peuvent être engendrées par de tels événements. Un système normalisé C2, fondé sur les critères Trusted Computer System Evaluation Criteria, doit augmenter non seulement la qualité des mécanismes de contrôle d'accès internes au système d'exploitation, mais également celle des traces associées.

Les dispositifs de contrôle interne sont avant tout des sortes de barricades que les entreprises édifient afin de s'assurer que la valeur qu'elle crée ne sera pas affectée par les risques qu'elle peut encourir. Pourtant, nul n'est à l'abri. La loi de Murphy nous enseigne que si quelque chose peut mal tourner, alors cette chose finira infailliblement par mal tourner. Il devient indispensable pour les organisations de procéder à des évaluations continues de ceux-ci pour une meilleure prise de décision du fait que les risques sont en constante évolution.

2.2. Evaluation de la maîtrise des risques liés au réseau informatique

Toute entreprise est confrontée à un ensemble de risques externes et internes qui doivent être évalués et maîtrisés par le contrôle interne. L'évaluation de la maitrise des risques consiste à déterminer dans quelle mesure le dispositif de l'entité est efficace contre les évènements potentiels susceptibles d'avoir un impact sur la réalisation des objectifs. L'objectif d'une sécurité bien gérée et ciblée consiste à protéger les éléments critiques d'une entreprise. Toute erreur sur la cible à protéger conduit à une analyse erronée de la situation et peut mettre en péril l'entreprise. La détermination de ces éléments critiques et de ces objectifs de sécurité est donc primordiale pour élaborer une politique de sécurité cohérente. Selon les normes de fonctionnement et normes de mise en œuvre associées, l'évaluation de la maitrise des risques doit être au moins annuelle et considérer tous les points de vue de l'entreprise. Selon FOROUZAN (2002:87), la détermination des éléments critiques d'une entreprise est une tâche délicate et qui prête à discussion, chaque service ou département se considérant souvent comme un secteur clé. Un bon moyen pour y parvenir consiste à mener avec les responsables de l'entreprise une analyse des risques. Une telle analyse consiste tout d'abord à identifier les ressources ou les biens vitaux de l'entreprise. Ces derniers peuvent être de plusieurs ordres, LLORENS (2006 : 376) :

- matériel (ordinateurs, équipements réseau, etc.) ;
- données (bases de données, sauvegardes, etc.) ;
- logiciels (sources des programmes, applications spécifiques, etc.) ;
- personnes (salariés, personnel en régie, etc.).

Une fois l'analyse effectuée, il faut encore déterminer les objectifs de sécurité. Ceux-ci visent à spécifier les besoins en termes de confidentialité, d'intégrité et de disponibilité des éléments critiques de l'entreprise. Une fois les éléments critiques et les objectifs de sécurité identifiés, il convient, pour chacune des ressources vitales, d'associer les trois éléments suivants, qui visent à définir l'analyse de risques proprement dite, telle que définie par l'ISO comme la combinaison de la probabilité d'un événement et de ses conséquences.

La connaissance des faiblesses de sécurité n'est possible que par des audits réguliers de sécurité, effectués soit par l'équipe sécurité, soit par des consultants externes. Les

sociétés d'assurance ont généralement accès aux données statistiques, aux experts et aux actuaires pour quantifier la valeur des ressources et chiffrer le montant des primes d'assurance. Le rapprochement entre les ressources critiques de l'entreprise, les objectifs de sécurité et les risques de sécurité associés (déterminés par le triptyque menace/vulnérabilité/ conséquence) permet de définir la stratégie sécuritaire de l'entreprise. Cette stratégie de sécurité permet de déterminer les exigences de sécurité ainsi que la sélection et l'implémentation de contrôles de sécurité afin de protéger le système concerné. Elles ont pour but de garantir les objectifs de sécurité, de protéger les éléments critiques et de mitiger les risques.

De nombreuses méthodes d'évaluation qualitative de la sécurité ont vu le jour pour permettre de bâtir des plans de sécurité efficaces. Elles sont souvent génériques, afin de prendre en compte les aspects techniques et organisationnels. Rappelons qu'une méthode qualitative permet d'analyser des données qui ne sont pas chiffrées et qui sont généralement disponibles sous forme de textes.

2.2.1. Modèles d'évaluation des dispositifs de maîtrise des risques

La gestion des risques ne doit pas se limiter uniquement à une simple identification, c'est-à-dire à un recensement plus ou moins exhaustif des risques potentiels et pertinents et à une analyse plus ou moins approfondie de leurs caractéristiques. Elle doit s'appuyer également sur une analyse qualitative et/ou quantitative des éléments de sécurité pour mieux juger leur efficacité face à la survenance et la gravité des risques.

L'informatique et les systèmes d'informations sont des domaines très normés et règlementés. A cet effet, nous distinguons quelques principales méthodes d'analyse des risques, établis conformément aux normes de sécurité de l'information, tels qu'EBIOS (Expression des besoins et Identification des Objectifs de Sécurité), MEHARI (Méthode Harmonisé d'Analyse des Risques) et OCTAVE (Operationnally Critical Threat, Asset and Vulnerability Evaluation). Toutefois, celle qui retient notre attention est la méthode MEHARI pour plusieurs raisons. En effet, MEHARI intègre une base de connaissance permettant :

- la définition des services de sécurité,

- la définition des critères d'évaluation des niveaux de qualité de service,
- l'élaboration d'une base de connaissance des services de sécurité,
- la définition d'une base métrologique pour évaluer la qualité des services de sécurité.

Toutefois certains inconvénients doivent être éclaircis telle que la nécessité d'un modèle complet de représentation des risques et la représentation de chaque situation de risque dans sa complexité, conditions que la méthode MEHARI remplit amplement. Elle est présentée sur l'organisation décrite dans la norme ISO/IEC/27005 et peut se résumer à ceci : les risques doivent être identifiés et décrit par des scénarios contenant un certain nombre d'éléments précis ; chaque scénario peut être évalué quantitativement et cette évaluation prend en compte l'impact intrinsèque, la potentialité intrinsèque et les facteurs de réduction de risque (voir glossaire). En sus, MEHARI est doté d'une base de connaissances renfermant un cadre dédié au réseau, facilitant la tâche des auditeurs des systèmes d'informations.

Selon MEHARI, quel que soit le domaine d'application, une méthode d'évaluation de la qualité des services de sécurité devrait prendre en compte :

- l'efficacité du service : pour les services dits techniques, l'efficacité mesure la capacité à assurer effectivement la fonction demandée face à des acteurs ayant des compétences plus ou moins fortes ou des circonstances plus ou moins courants.
- Sa robustesse qui mesure sa capacité à résister à une action visant à le court-circuiter ou à l'inhiber.
- Les moyens de contrôle de son bon fonctionnement afin de détecter toute interruption du service et que des mesures palliatives soient alors décidées.

Il en ressort que les méthodes doivent être personnalisées selon divers facteurs afin d'apporter un gain de valeur à l'entreprise.

2.2.2. Les enjeux de l'évaluation de la maîtrise des risques liés au réseau informatique

Les organisations vivent chaque minute au diapason d'évènements susceptibles d'enfreindre l'atteinte de leurs objectifs. Ce postulat est renchérit par le fait que l'information est la donnée intrinsèque de leurs activités et qu'elles sont toutes bâties sur des systèmes d'information intégrant pour la plupart des réseaux.

Les attributs de ceux-ci démontrés au chapitre précédent, nous permet d'avoir une vue sur leurs aspects vulnérables dont la criticité doit être hautement appréciée par les entités. L'entreprise doit de ce fait, depuis l'élaboration de sa politique générale, mettre en œuvre des actions qui lui permettront de protéger ses actifs informationnels et cela, conformément aux best practices dont l'application est gage de crédibilité auprès des partenaires.

Le processus itératif et continu de maîtrise des risques doit être basé sur des outils reconnus ou efficaces développés par les entreprises elles-mêmes et qui lui assurent une couverture des secteurs clés de son réseau. Ceci procurera aux organisations un aperçu de ce qui peut leur être nuisible car il est bénéfique de savoir ce qui peut être une entrave avant de chercher comment y remédier. L'ouverture du système d'informations étant source d'innombrables problèmes, l'entreprise pourra une fois les risques connus, rassembler les moyens financiers, matériels, humains et intellectuels qui lui permettront de faire face aux intempéries dont nul n'est à l'abri.

2.2.3. Gestion juridique et financière d'un risque informatique du réseau

La gestion des risques suppose de prendre toutes les mesures utiles afin d'empêcher que la responsabilité de la société ou de ses dirigeants puisse être engagé du fait d'une utilisation illicite ou fautive des moyens informatiques, notamment par un membre de l'entreprise.

En Référence à CALE & TOUITOU (2007 :214),la réponse à cette problématique aboutit à la mise en place d'une politique de gestion juridique et financière du risque basée sur une charte d'utilisation des outils informatiques définissant les droits et obligations de

chacun, la souscription de contrats d'assurance adaptés et une évaluation régulière des risques et des mesures de sécurités appropriées.

Conclusion

L'informatique et les systèmes d'informations sont aujourd'hui des domaines extrêmement normés et protégés ; ceci offre aux entités une pléthore de choix en ce qui concerne les méthodes de gestion des risques, selon la volonté des dirigeants et les objectifs qu'ils poursuivent dans l'évaluation de ses dispositifs de contrôle de sécurité et la protection de ces actifs.

Aucune méthode n'est cependant appropriée pour telle ou telle organisation, tout s'adapte et se modèle au gré des attentes de tout un chacun. Néanmoins, un ensemble d'aspects, comme identifiés plus haut, doivent être respectés comme prévu par la norme ISO 27000.

Dans le chapitre prochain, nous identifierons les techniques de collecte de données que nous utiliserons ; nous déterminerons le modèle d'évaluation de la maitrise des risques que nous utiliserons en fonction des informations recueillies et des objectifs de l'entité.

Chapitre 3 : Méthodologie de l'étude

Introduction

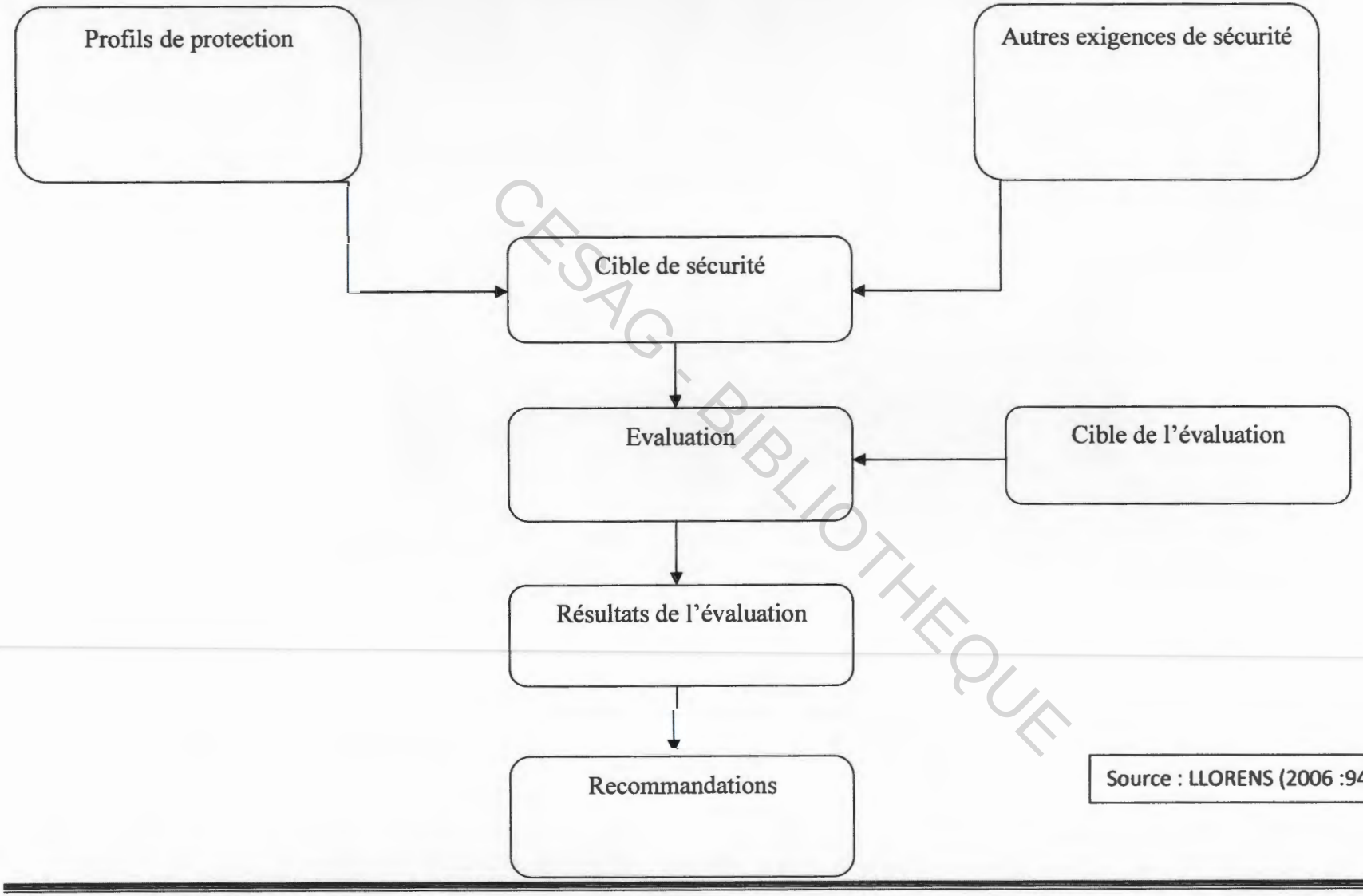
Le dictionnaire LAROUSSE 2010 définit la méthodologie comme une manière de faire ou de procéder. DESCARTES dans le discours de la méthode avance qu'on ne peut se passer d'une méthode pour se mettre en quête de la vérité des choses. Cette citation, certes philosophique, exprime le fait qu'une démarche corrélée de savoir-faire est inextricablement une source primaire de résultats probants.

Evaluer la maîtrise des risques s'inscrit dans ce même ordre d'idée dans la mesure où des préalables sont indispensables à la mise en orbite des sécurités annihilant les évènements pouvant empêcher la réalisation des objectifs. Il s'agit d'une suite d'opérations bien cohérentes et réfléchies par des professionnels du domaine que l'entreprise peut néanmoins ajuster selon ses besoins.

Ce chapitre nous sert de présentation du modèle que nous utiliserons dans l'évaluation de la maîtrise des risques liés au réseau informatique ainsi qu'à la justification des outils que nous brandirons dans la quête d'informations utiles et pertinentes. En fin de compte, nous évoquerons la manière dont les données recueillies seront traitées.

3.1.Modèle d'analyse des données

Notre démarche basée entièrement sur le modèle évoqué, sera effectuée comme suit



Source : LLORENS (2006 :94)

Les profils de protection permettent de définir les exigences fonctionnelles d'un type de produit en fonction d'une cible d'évaluation. Un profil de protection est donc réutilisable par tous et présente l'avantage d'exposer des exigences reconnues comme étant nécessaires pour satisfaire les objectifs de sécurité. Par exemple, dans le domaine des cartes à puce, des sociétés ont défini des profils de protection pointant des domaines spécifiques, tels que les circuits intégrés ou les applications financières. Les profils de protection permettent donc d'établir des ensembles communs d'exigences de sécurité apportant le concept de réutilisabilité pour l'évaluation d'un type de produit.

Une cible de sécurité contient les exigences de sécurité du produit à évaluer. Il s'agit de la définition d'un ensemble de services de sécurité rendus par un produit ou un système, des exigences de sécurité couvertes et des spécifications des fonctions de sécurité proposées. La cible de sécurité est le dossier qui servira de base à l'évaluation.

La cible d'évaluation, qui désigne le produit ou le système utilisant les technologies de l'information et qui fait l'objet de l'évaluation.

3.2. Collecte des données

Pour accomplir ces travaux, nous utiliserons différents outils à notre disposition. Une mise en œuvre judicieuse de ceux-ci nous permettra d'atteindre nos objectifs avec une meilleure efficacité. Nous distinguerons :

- les outils de collecte de l'information ;
- les outils descriptifs.

3.2.1. Les outils de collecte de l'information

Les outils de collecte de l'information qui seront les plus utilisés tout au long de l'évaluation sont les suivants :

- L'entretien

Cet outil est souvent celui qui est le plus difficile à conduire et celui pour lequel un débutant n'est souvent pas préparé. C'est pourquoi sa préparation est importante. Il nous aidera

à amasser des informations sur le fonctionnement du réseau informatique de l'entreprise, sur les mesures de sécurités érigées pour la sauvegarde des actifs et sur la description réelle des tâches du personnel du service informatique.

- L'observation physique

L'entretien n'est pas suffisant pour bien comprendre les procédures étudiées. Il faut voir les documents et les liens entre eux. C'est ainsi qu'à la fin d'un entretien au cours duquel une procédure a été décrite, nous essayerons de résumer la compréhension en demandant à l'interlocuteur de prendre un exemple et d'en suivre le cheminement. Cela a deux avantages :

- S'apercevoir si dans les explications une partie de la procédure a été omise.
- S'assurer de la bonne compréhension de l'ensemble des procédures.

Par ailleurs, l'observation directe est une source d'information très productive. L'auditeur qui observe attentivement soulève souvent des problèmes qui ne sont pas connus, ou qui ne peuvent être déduits de l'analyse de l'information écrite. L'ouverture d'esprit, la communication, le respect des subordonnés… sont autant d'indicateurs sur le climat de l'unité vérifiée. L'observation est aussi une source riche d'exemples spécifiques qui sont utiles à l'illustration des conclusions générales.

Toutefois, l'observation physique présente des limites :

- Elle n'est pas toujours possible : par exemple lorsque l'activité de l'entreprise est la construction de pipeline au fond de l'océan.
- A partir d'une observation physique ou directe il n'est pas possible de généraliser les constats.

- Les questionnaires

Nous utiliserons énormément des questionnaires puisque la base de connaissances de MEHARI est fondée sur cela. Ces questionnaires sont déjà standardisés et correspondent aux spécifications de MEHARI. Toutefois, nous élaborerons certains questionnaires à des fins de complément d'informations. Nous les adapterons au maximum possible au métier de l'entreprise et à la structure de ses actifs.

- L'analyse documentaire

Elle consiste en l'exploitation des documents de l'organisation faisant l'objet de l'étude. Cela s'est imposé pour permettre d'avoir un aperçu de la gestion sécuritaire du réseau informatique de la BCI. Il s'est agit de consulter les manuels de procédures relatifs au fonctionnement du service informatique de la banque

3.2.2. Les outils descriptifs

On distingue quatre catégories qui généralement se complètent.

- Les organigrammes

La collecte des organigrammes de la banque par l'auditeur est importante afin de pouvoir comprendre les responsabilités respectives du personnel. L'auditeur est très souvent amené à mettre à jour les organigrammes ou à rajouter ses propres commentaires sur les responsabilités réelles. En effet, très souvent, pour des raisons liées à la gestion des ressources humaines de l'entreprise, il peut exister des différences non négligeables entre l'organigramme « officiel » et les responsabilités réelles. L'auditeur peut ainsi comprendre quels sont ses interlocuteurs pour traiter d'une procédure.

- Le narratif

L'avantage du narratif est qu'il est à la portée de tous (les auteurs et les lecteurs). Toutefois, il est généralement difficile à exploiter du fait de lourdeur et du manque de rigueur. Décrire une procédure à l'aide d'un narratif ne permet pas de décrire rigoureusement le processus. Il est donc souvent plus judicieux d'utiliser des diagrammes auxquels on ajoute des narratifs.

3.3. Analyse des données

Le système de mesure de la qualité des services de sécurité de la base de connaissance MEHARI est basé sur un système de cotation des réponses aux questions, questions auxquelles il est demandé de répondre par oui ou par non, avec des conventions de cotation et de pondération que nous évoquerons plus loin.

Les questionnaires comprennent à la fois des questions axées sur l'efficacité des mesures de sécurité (par exemple : fréquence des sauvegardes, type de contrôle d'accès

physiques, existence d'un système de détection d'incendie, etc.), des questions axées sur la robustesse des mesures de sécurité et généralement une ou deux questions sur le contrôle ou l'audit des fonctionnalités attendues du service. Néanmoins, certaines questions feront l'objet d'un retrait du à leur caractère confidentiel au niveau de la banque et à la sensibilité des informations divulguées par les réponses dont elles peuvent être sujettes.

Toutefois, une distinction est à effectuer entre ces questions. Certains ont trait à des mesures qui ont un certain rôle, au sens où elles contribuent à la qualité de service sans, pour autant que leur mise en œuvre soit indispensable (mesures contributives). D'autres mesures peuvent être jugées suffisantes pour atteindre un certain niveau de qualité. Par contre, des mesures peuvent être encore jugées indispensables pour atteindre un certain degré de service de qualité.

Ce triple système de mesure de la qualité de service évite le risque de voir une série de mesures faiblement efficaces surévaluer un niveau de qualité qi les mesures essentielles ne sont pas actives ou, au contraire, une série de mesure de poids faible sous évaluer la qualité de service alors qu'une mesure essentielle est effectivement en place. Cette approche est une valeur distinctive de MEHRAI et s'appuie sur l'expertise des personnes qui tiennent à jour les bases de connaissance. Puisque les questionnaires d'audit des services de sécurité sont précisément organisés en fonction des domaines de responsabilité, il suffira de dupliquer les questionnaires pour couvrir chacune des variantes du domaine et analyser et d'y répondre ensuite avec la personne ou le groupe de personnes le mieux placé pour cela.

Conclusion

Ce chapitre formalise la démarche que nous emprunterons dans le cadre de notre étude et les outils que nous manipulerons pour l'atteinte de nos objectifs. Il s'agira donc d'observer un respect de la méthode utilisée et de ses spécifications. Il se présente aussi comme une transition dont les les racines sont ancrées dans la partie théoriques et dont les fruits naitront dans la partie pratique si bien évidemment, son élaboration a été correcte et bien respectée.

Il marque donc l'achèvement de la revue de littérature et le passage à la partie pratique de notre étude.

Conclusion de la partie théorique

Le réseau informatique est un composant essentiel des systèmes d'informations au vu de ses attraits et fonctionnalités. Il est évident que nous ne pouvons nous en passer dans l'exécution de nos activités. Ainsi, pour juger l'efficacité d'un item, il faut savoir d'abord ce en quoi celui-ci consiste : fait que nous avons étayé dans le premier chapitre de notre partie.

L'évaluation du réseau informatique tient à plusieurs éléments de plus en plus complexes selon la taille de l'entreprise. Plusieurs organismes ou auteurs ont publié des méthodes d'évaluation dont la plus-value ne pourrait être perçue que lorsqu'elles sont appliquées dans un contexte approprié et correspondant aux attentes des dirigeants. Il s'agit alors de relier plusieurs points pour aboutir à une harmonie entre l'entité, son réseau local et la méthode d'évaluation de celle-ci. Néanmoins, rien ne peut être effectué à point nommé sans l'implication de tous les acteurs de l'organisation.

Basé essentiellement sur MEHARI, notre évaluation a voulu tenir compte des avantages de la gestion individuelle des risques pour mieux les traiter. En dépit de du large champ d'éléments qu'il recouvre, entrainant une forte implication des dirigeants, elle est celle dont le déroulement est plus aisé du fait de l'existence d'une base de données. Cette partie consolide les tenants et les aboutissants du réseau informatique ainsi que de son évaluation, tout en évoquant un choix de mode et ses justificatifs. Dans la seconde partie, nous verrons ce qui en est réellement dans la structure.

CADRE PRATIQUE

Introduction à la partie

Cette partie nous permet de rentrer dans la sphère de la banque et de nous imprégner du contexte dans lequel notre évaluation sera faite. En effet, après avoir élucidé les pourtours et aspects inhérents à la maitrise des risques liés au réseau informatique, nous appliquerons les acquis à la structure tout en gardant en ligne de mire un gain partagé par la banque et nous-mêmes.

Nous essayerons pour ce faire, de capitaliser la théorie évoquée précédemment en s'appropriant dans un premier temps du contexte dans lequel est située notre étude, à savoir la BCI. Secundo, nous présenterons les informations recueillies tout en les analysant via le modèle décrit plus haut et nous achèverons notre travail par des recommandations bâties toujours sur la base de connaissance de MEHARI.

Cette partie s'avère être donc être un indicateur de réussite de ce mémoire dans la mesure où il renferme les résultats de notre mise en situation.

Chapitre 4 : Présentation de la Banque du Commerce et de l'Industrie du Mali

Introduction

Au sorti de la 1ère journée de l'association des banques et établissements financiers du Mali tenue en Mars 2011 à Bamako, l'ambition notable relevée est la réalisation d'un objectif de 20% de taux de bancarisation à l'horizon 2012. Ainsi, suite à la volonté affichée par l'Union Economique et Monétaire Ouest-Africaine (UEMOA) d'aller vers une bancarisation à grande échelle de la sous région, les banques Maliennes se sont inscrites dans un processus d'envergure qui modifiera plusieurs aspects de leurs entités allant de la stratégie aux actifs notamment. Il en ressort de facto que pour faire face aux soucis des Etats et concurrencer convenablement, il faut se doter des moyens pour ce faire en l'occurrence des actifs technologiques et sécuritaires.

La Banque pour le Commerce et l'Industrie n'est pas en marge de tout cela depuis son entrée dans le secteur bancaire Malien. Comme toutes les banques, elle se dote de ressources pour se faire une place dans ce milieu déjà occupé par 12 banques en activité. Le pays est l'un des rares à avoir un taux de bancarisation supérieur à celui de l'UEMOA qui est d'une moyenne de 6,5%. 65% de crédits concernent le commerce, domaine de la BCI, et l'hôtellerie. Le marché est dont important, de même que les risques. Dans les lignes à suivre, nous présenterons la banque dans ses principales facettes et nous porterons notre notre analyse sur son dispositif de maitrise des risques liés au réseau informatique.

4.1. Présentation de la banque

La BCI-Mali fait partie du groupe BCI dont le siège se trouve en Mauritanie. Elle s'intéresse notablement au secteur du commerce et de l'industrie. Selon le président de son conseil d'administration, elle est la manifestation, non seulement d'une ambition internationale, mais aussi d'une volonté de participer activement au développement des échanges entre deux pays frères. Son directeur général ajoutera qu'elle entend ainsi, par une action

solidaire, proche de son cœur de métier, apporter une nouvelle contribution à l'emploi et à la lutte contre la pauvreté.

4.1.1. Historique

Nous ne pouvons évoquer un passé de la Banque pour le Commerce et l'Industrie du Mali sans porter un œil sur sa mère située en Mauritanie.

Conscient des nouveaux enjeux, et des opportunités économiques que cela supposait, un homme d'affaires connu, Isselmou ould Didi ould Tajedine, décide en 1998 d'introduire une demande d'agrément pour la création d'une nouvelle banque. Outre des associés mauritaniens représentatifs du tissu socio-économique national, il fait appel à trois partenaires européens avec lesquels il travaille depuis plusieurs années. Ces derniers (deux hollandais et un français) s'engagent à hauteur du tiers dans le projet.

L'agrément de la Banque Centrale est obtenu en avril 1999, et, en septembre de la même année la Banque pour le commerce et l'Industrie ouvre ses portes à Nouakchott. Dans ce pays réputé difficile, et inclassable entre le Maghreb et l'Afrique Subsaharienne, sur un marché étroit et apparemment très concurrencé, la nouvelle institution va rapidement s'imposer sur la place bancaire.

Grace à des performances très satisfaisantes, la plaçant parmi les toutes premières banques du pays, la BCI ouvre des agences dans toute la Mauritanie et s'installe au Mali. En 2007, La BCI Mali voit le jour pour annoncer une meilleure intégration entre la Mauritanie et tous les pays de l'espace que constitue l'UEMOA. Elle est aujourd'hui forte de 10 agences sur l'ensemble du territoire Malien.

4.1.2. Dénomination

L'institution porte la raison sociale de Banque pour le Commerce et l'Industrie, mettant en avant les secteurs dont elle se reconnait sur la base de la segmentation décidée par ses dirigeants.

4.1.3. Cadre juridique

Comme le prévoit la loi portant sur la règlementation bancaire à son article 1er : « sont considérées comme établissements de crédit, les personnes morales qui effectuent, à titre de profession habituelle, des opérations de banque. Constituent des opérations de banque, au sens de la présente loi, la réception de fonds du public, les opérations de crédit, ainsi que la mise à disposition de la clientèle et la gestion de moyens de paiement. Les établissements de crédit sont agréés en qualité de banque ou d'établissement financier à caractère bancaire. »

L'article 31, le premier portant sur la forme juridique, nous dit que : « sont considérées comme établissements de crédit, les personnes morales qui effectuent, à titre de profession habituelle, des opérations de banque. Constituent des opérations de banque, au sens de la présente loi, la réception de fonds du public, les opérations de crédit, ainsi que la mise à disposition de la clientèle et la gestion de moyens de paiement. Les établissements de crédit sont agréés en qualité de banque ou d'établissement financier à caractère bancaire. Elles ne peuvent revêtir la forme d'une société unipersonnelle. Exceptionnellement, elles peuvent revêtir la forme d'autres personnes morales. Elles doivent avoir leur siège social sur le territoire d'un des Etats membres de l'UMOA. »

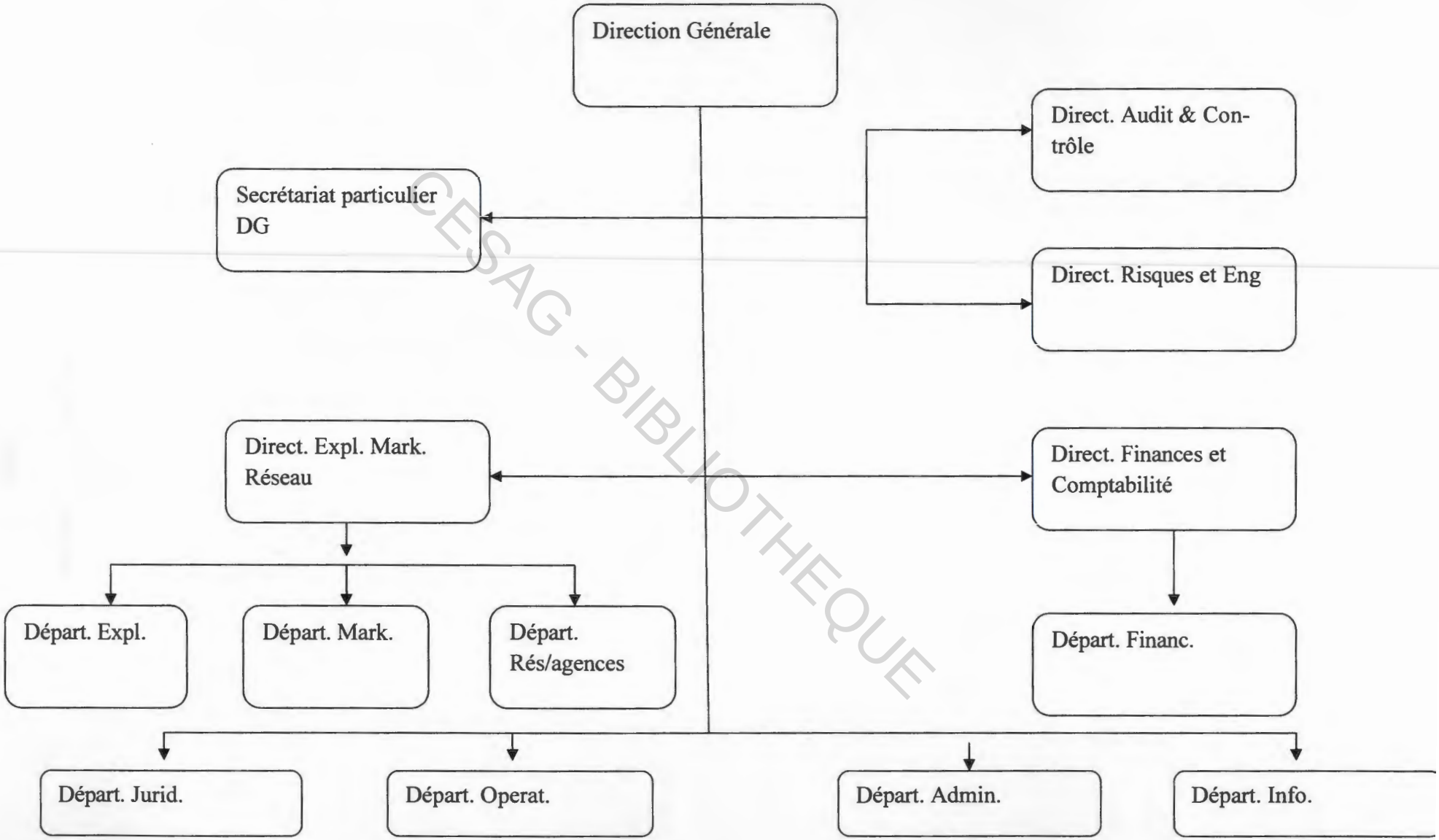
L'ensemble des dispositions relatives à l'aspect juridique et fonctionnel des banques est inscrit dans la loi portant sur la règlementation bancaire. Tout y est scrupuleusement énoncé et soumis au respect de chaque établissement financier.

4.1.4. Organisation et fonctionnement de la banque

La banque, encore nouvelle sur la place, s'est dotée d'une organisation peu complexe afin de ne pas créer des fonctions inutilisées pour son âge et pour pouvoir correspondre au volume de ses activités.

4.1.4.1. Organisation

La banque dispose d'un organigramme peu complexe.



Source : Mémo Direction générale 002/31-07-2011

4.1.4.2. Fonctionnement

Le fonctionnement du système administratif de la banque peut être décrit à travers les rôles des principales directions de façon basique :

La direction audit & contrôle interne est chargée du contrôle des tâches confiées aux services et veille au respect des règles de travail édictées par les procédures de la banque. Il aide l'établissement à atteindre ses objectifs en évaluant, par une approche systématique et méthodique, ses processus de management des risques, de contrôle informatique et de gouvernement d'entreprise et en faisant des propositions pour renforcer leur efficacité.

Le département juridique et contentieux comprend deux services, le juridique et le contentieux. Le département est chargé de toutes les questions juridiques de la banque en sus du recouvrement amiable et contentieux afin d'optimiser le taux de recouvrement des créances clients de la banque.

Le département exploitation coordonne et anime les activités et la politique commerciale de la banque, des agences, en assure la gestion clientèle et la prise en charge des dossiers de crédit.

Le département des opérations est divisé en 3 services : les opérations locales (en relation étroite avec l'ensemble des agences et les exploitants qui lui assurent les prestations de front office) et internationales (réseau international, les services des opérations documentaires et les transferts extérieurs) et l'administration des engagements.

Le département réseau-agence coordonne et anime les activités et la politique commerciale de la banque des agences.

La direction des risques et engagements a pour fonction générale la définition des politiques de risques et la gestion des engagements de la banque.

4.1.4.3. Missions

Forte de sa reconnaissance internationale que lui apporte sa maison mère, la BCI-Mali veut apporter sa pierre à l'édifice d'intégration économique entre les différents pays à travers des échanges commerciaux.

4.1.4.4. Objectifs

La BCI-Mali Sa développe ses activités autour de 5 orientations majeures :

- Mobiliser davantage les ressources afin de créer de la richesse à travers des financements adaptés.
- Favoriser une meilleure intégration économique à travers des échanges entre la Mauritanie, le Mali, et tous les pays de la zone UEMOA.
- Mettre en place une politique de proximité fondée sur une stratégie intégrée : agence, monétique, Internet Banking etc.
- Offrir des produits et services bancaires de qualité à tous les acteurs économiques : particuliers, professionnels, Etat, organismes publics et para publics, les entreprises nationales et étrangères ;
- Accroître le taux de bancarisation au Mali.

4.2. Données significatives de la banque

Les valeurs significatives de la banque sont les suivantes :

4.2.1. Produits

La BCI offre à sa clientèle le portefeuille de produits ci-après :

- Comptes courants;
- Comptes d'épargne et de dépôt;
- Cartes bancaires : Monétique;
- Banque par Internet : BCI net;
- Opération par devises;
- Prêts et escomptes d'effets (chèques ou traites);
- Cautions : Engagements par signature;
- Western Union.

La BCI a mis en place une solution monétique qui permet l'émission de cartes bancaires et l'ouverture d'un réseau GAB (Guichet Automatique Bancaire/distributeur de billets). Un réseau de TPE (Terminaux de Paiement Electronique) sera également disponible et acceptera les cartes bancaires maliennes et internationales.

Elle est également à mesure d'offrir à ses clients un service de gestion directe de leurs comptes via Internet. En plus d'offrir la gamme habituelle, la BCI vous propose des services inédits et novateurs vous facilitant le quotidien :

- BCI net : La BCI sur internet vous permet de consulter vos comptes, tous vos virements et autres transactions.
- Operations bancaires via SMA /sms banking : Grâce a ce service, vous pourrez de façon journalière connaitre le solde de vos comptes et consulter vos dernières transactions réalisées (retrait, dépôt, etc.).
- Règlement des factures : ce service permet de payer aux guichets (factures EDM[15], SOTELMA[16], orange, impôts, etc.)
- Recharges téléphoniques : ce produit permet d'acheter des cartes de recharge téléphonique a nos guichets.
- Guichet mobile : le guichet mobile offre la possibilité de faire des versements sans avoir à se déplacer.
- Extrait de compte en plusieurs langues : la BCI est à mesure de produire des extraits de comptes en français et en anglais. Bientôt ce service sera disponible en arabe et en allemand.
- Politique de prêt islamique : A travers l'expertise de la maison mère, la banque sa propose des prêts adaptés.

[15] EDM : Energie Du Mali
[16] SOTELMA : Société des Télécommunications du MALI

4.2.2. La clientèle

Les clients de la banque sont des particuliers et des entreprises de tout secteur mais principalement du commerce et de l'industrie.

4.2.3. Données clés (En Milliards)

Tableau 1 : Données clés

	2010	2009	2008
Chiffre d'affaires	3,644	2,765	2,076
Produit Net bancaire	2,923	2,443	1,707
Effectif	89		

Source : Bilans de la banque 2009 et 2010

4.2.4. Commercialisation

La banque est aujourd'hui forte de 10 agences, étendues sur l'ensemble du territoire Malien. Toutefois, les dossiers importants sont traités au niveau du siège, à Bamako.

4.2.5. Ressources humaines

Le développement du Mali, accéléré par la mise en valeur de ses ressources naturelles considérables suppose un cadre financier performant adapté à un environnement dont la compétitivité est croissante. Au-delà donc de moyens technologiques modernes, la BCI-Mali dispose d'une équipe de collaborateurs formés et expérimentés, sous la direction des cadres nationaux.

Elle travaille en trois langues internationales (le français, l'anglais, l'arabe) et six langues nationales (bambara, peulh, sonrhaï, dogon, maure, khassonké). Parallèlement à la sélection rigoureuse qu'elle a opéré en amont, la BCI-Mali assure la formation permanente de son personnel tant au Mali qu'à l'étranger.

4.2.6. Ressources financières

La banque a récemment procédé à une augmentation de son capital à 6.250.000.000 F.CFA, qui était initialement de 2.000.000.000 F.CFA. Cette augmentation est relative à un besoin des activités mais aussi une volonté de la Banque Centrale imposée à toutes les banques de la sous-région.

4.2.7. Ressources matérielles

L'existence et la maîtrise d'un outil technologique performant sont des requis pour une meilleure compétitivité de la banque. A cet effet, la BCI s'est dotée d'un progiciel de gestion particulièrement efficace qui permet de :

- couvrir l'ensemble des fonctionnalités bancaires (y compris la gestion des technologies de l'information, de la communication et des produits financiers);
- automatiser la totalité des fonctions comptables ;
- sécuriser la totalité des opérations via un système d'habilitation contrôlant la saisie, la validation et les interrogations;
- travailler en temps réel (tous les états financiers), tant avec le siège qu'avec chacune des agences.

Cet équipement répond à trois exigences majeures :

- la sécurité et la rapidité des transactions ;
- la facilité du traitement;
- la réduction des coûts tout en maximisant la qualité du service.

Conclusion

Le groupe BCI tâche à ne négliger aucun effort pour poursuivre et confirmer la croissance de la BCI-Mali, et son engagement aux côtés de sa clientèle, et pour répondre aux besoins de l'économie nationale.

Chapitre 5 : Description du dispositif de maîtrise des risques liés au réseau informatique et présentation des résultats

Introduction

Le dispositif de maîtrise de risques ici évoqué correspond au contrôle interne en place au sein de la banque afin d'appréhender les risques pouvant émaner de son réseau local et contribuer à l'atteinte des objectifs de la structure. Le réseau local étant sous la responsabilité du service informatique dans l'entité, il sera question de présenter ce département dans ses aspects principaux ainsi que ses apports à la gestion sécuritaire. Ce chapitre sera clôturé par une description du dispositif sécuritaire et des méthodes ou processus de gestion du réseau local.

5.1. Présentation du service de sécurité informatique

Il est prépondérant de préciser qu'il n'existe pas encore au sein de la banque un service en charge des systèmes d'informations. Nous rajoutons encore, comme il en a été fait cas au chapitre précédent, que cet état est observable dans presque toutes les banques de la place pour maintes raisons. Cependant, le service informatique en activité, essaie tant bien que mal d'aller vers une formalisation de son fonctionnement dans un manuel ainsi qu'une extension de ces attributions. Cette ambition est ralentie par de nombreux facteurs dont l'environnement et le marché.

5.1.1 Les objectifs du service sécurité informatique

Ce service assure le traitement des informations pour les besoins de gestion comptable et administrative ; il est chargé de la maintenance des applications existantes et de la conception d'applications nouvelles répondant aux besoins des utilisateurs. Il peut produire, sur demande, des statistiques comme support aux décisions de la banque.

Ses objectifs se résument donc à :

- s'assurer de la sécurisation du système informatique ;
- s'assurer que la banque opère dans un environnement informatique sécurisé, fiable et contrôlé ;
- orienter de façon optimale et efficiente les choix de la direction générale en matière de technologie ;
- s'assurer d'une bonne adéquation entre l'outil informatique et la stratégie globale des entités supportées ;
- veiller à la maîtrise du système d'information par les agents dans un délai raisonnable ;
- mettre en œuvre la politique et les procédures informatiques ;
- gérer de façon efficace les aspects techniques de la monétique et western-union
- gérer la sécurité physique des matériels et veiller à leur entretien ;
- veiller à l'identification et au développement de nouveaux systèmes de traitement de l'information répondant aux besoins de la banque.

Les missions de la banque consistent en ceux-ci :

- le traitement des journées comptables ;
- la création et la mise à jour des fichiers nécessaires à la gestion de la banque ;
- les traitements de la paie et la mise à jour du fichier du personnel ;
- l'édition des différents documents :
    - documents comptables ;
    - documents de gestion et tableaux de bord ;
    - relevés de comptes et échelles d'intérêts,
    - diverses déclarations er sécurité des fichiers et programmes ;
- la gestion rationnelle du matériel mis à sa disposition ;
- la gestion et le suivi de l'approvisionnement en disques, disquettes bandes, listings,…
- l'encadrement des opérations sur périphériques ;
- la maintenance et la sécurisation des équipements et du centre informatique dans son ensemble ;
- la réalisation de travaux d'analyse et de la constitution des dossiers appropriés ;

- la veille technologique ;
- la conception et le suivi de la réalisation des applications ;
- le contrôle des dossiers de programmations ;
- l'étude des nouvelles techniques et des caractéristiques de tout matériel informatique à acquérir ;
- l'assistance technique au réseau western union ;
- la gestion du parc informatique ;
- la mise en œuvre des applications sur micro en relation avec les autres structures concernées ;
- la gestion du réseau informatique ;
- la maintenance du réseau et du matériel informatique ;
- l'interface avec les prestataires extérieurs.

5.1.2 Les moyens du service sécurité informatique

Le service dispose des équipements modernes et adéquats aux activités de la banque. Le caractère confidentiel de ces outils est à l'origine de leur non mention dans cette partie. Le département dispose également d'un budget conséquent lui permettant d'assurer l'amélioration de la technologie, la maintenance des outils et la délivrance de services optimums. Les objectifs qu'il se doit d'atteindre lui fournissent aussi la latitude de proposer aux dirigeants les potentialités optimales sur le marché et les évolutions que l'institution peut entreprendre pour se conformer davantage à ce qui se fait de mieux.

5.1.3 L'organisation du service sécurité informatique

Le département a un effectif de trois personnes activant les leviers nécessaires à la bonne marche du service. Il est scindé en deux parties : l'exploitation et le réseau.

Le responsable de l'exploitation gère et anime l'ensemble de son équipe, veille au bon fonctionnement et à la maintenance des équipements informatiques dont il a la charge. Il veille au respect des objectifs : qualité et sécurité, et à l'application des procédures de recette et de validation avant la mise en production. Il assure le suivi des coûts et met en

place les tableaux de bord de gestion. Il participe au choix et à l'implantation de méthodologies et de procédures d'automatisation ainsi qu'à la définition de l'architecture matérielle. En collaboration avec les différentes directions, il dimensionne les moyens informatiques à mettre en œuvre. Il conseille la direction générale sur la stratégie relative aux équipements.

Le responsable du réseau apporte une assistance technique (méthode, produit...), suivant le domaine d'intervention aux utilisateurs, avec pour objectif d'optimiser les traitements et les systèmes informatiques. Il conseille généralement la direction générale lors de l'étude de solutions nouvelles (choix de logiciel, de matériel, d'architecture de réseau...).

5.1.4 Le niveau de rattachement du service

L'informatique est directement rattachée à la direction générale au sein d'une structure assez simple. Elle reçoit donc directement les directives du directeur général selon la politique générale et sécuritaire édifiée, et la stratégie de la banque.

5.2 Description des constitutifs de la maitrise des risques liés au réseau informatique en place

Le dispositif de contrôle interne en place au sein de l'entité dans le cadre de la maîtrise des risques liés au réseau informatique est encore en phase de démarrage. Pour le moment, le service de la banque s'évertue à assurer uniquement l'optimisation des opérations et la bonne circulation des informations sur le réseau. A cet effet, bon nombre d'aspects sont gérés de manière informels car aucun écrit ne les définis. Certains éléments leur sont encore méconnus mais l'on ne peut leur imputer cela car l'environnement même en est la cause. A ce jour, il n'a pas encore été effectué d'évaluation de leur maitrise des risques informatiques mais cela est compréhensible dans la mesure que sa prise en considération n'est que récente. Le service en charge ne fait cas des risques, encore moins de leur maitrise. Toutefois, Il est dans les objectifs de l'institution de mettre sur pied des états formels tels que des manuels de procédures traitant de la gestion des incidents, des pannes et de la sécurité du réseau, mais également d'accroître l'importance des systèmes

d'informations et la prépondérance de la gouvernance des technologies. Il est dans leur volonté de développer une culture à cet endroit.

5.2.1 Les méthodes de contrôle du trafic réseau

Il faut souligner que les postes de travail de travail sont reliés entre eux mais ils ne partagent rien comme on l'observe sur un réseau. C'est la plateforme de travail qui est partagé. Les transferts de fichiers via le réseau sont peu nombreux car le partage de dossiers est inexistant. Toute circulation d'informations dans le cadre des activités de la banque s'effectue via les applications de travail, les clés USB ou les boîtes électroniques. A ce niveau, un contrôle du trafic est encore absent au sein de la banque car il faut qu'il ait un échange d'informations entre les postes pour pouvoir contrôler un trafic. Lequel permettra de vérifier les flux et le débit afin d'éviter des congestions.

5.2.2 Les différents types d'accès au réseau

Les accès au réseau local en place concernent surtout les applications de travail de la banque. Selon, les fonctions et la hiérarchie, sont définies les possibilités d'accès aux ressources informationnelles des progiciels de travail. Le département Audit a, en l'occurrence, accès à tous les aspects de ces outils sauf les rubriques d'administration. Tous disposent d'un droit d'accès aux applications, représenté par un code tandis que les postes de travail ne sont pas tous protégés par des mots de passe d'entrée aux sessions.

5.2.3 Les méthodes de contrôle sécurité des accès

La sécurité des accès est assurée notablement par les identifiants et mots de passe d'accès. Tous en disposant, il devient facile pour les administrateurs de localiser les responsabilités en cas d'incidents et d'élaborer un état des accès durant une période donnée. La cryptographie utilisée relève de la confidentialité de l'institution.

5.2.4 Les méthodes et procédures de gestion de la sécurité du réseau

La sécurité du réseau est une émanation de la politique générale de sécurité de la banque et du plan de continuité d'activité. Ceci est encore en voie d'élaboration, d'où une gestion sécuritaire basique par le département informatique. Les procédures sont encore à un état conceptuel et la méthode embryonnaire en place a pour dessein la disponibilité permanente des applications et la réduction à un seuil acceptable des incidents.

5.2.5 Les méthodes de gestion des incidents

Du fait de sa jeunesse, la banque ne dispose pas encore de représentatifs scripturaux formels décrivant les procédures et méthodes de gestion des incidents au sein de la banque. Les principaux problèmes rencontrés au niveau du réseau peuvent être des mauvaises manipulations, des défauts de paramétrages ou des indisponibilités des serveurs.

Ces incidents sont gérés au cas par cas sans qu'il ait une traçabilité formelle déjà établie faisant cas de la manière dont le département résout le problème. Tous ces aspects ont été rapportés aux dirigeants de la banque, par le service, qui envisagent d'accroître le taux de formalisation au niveau de ce département avec la collaboration du département audit.

5.2.6 Les méthodes sécuritaires de sauvegarde des actifs, des données et des processus

Le système d'informations étant géré de façon informelle sans couvrir tous ses requis et facettes, il n'est pas encore établi de méthodes dans ce cadre. Ceci n'est pas corrélé aux ambitions de la banque, mais plutôt au niveau de développement de la banque et à l'environnement Malien. Il est notable de préciser aussi qu'il n'y a pas de préférence apportée à telle ou telle aspect de l'activité mais il est établi une priorisation des besoins.

La sécurité des actifs, des données et de processus comme le conçoit MEHARI, manque encore à l'appel puisque la gouvernance des systèmes d'informations n'est pas totalement intégrée dans la gouvernance de la banque.

5.3. Présentation des résultats

Ce volet nous permettra de faire sortir ce qui est requis en matière d'exigences fonctionnelles relativement à un réseau local. Par la suite, nous ferons cas des exigences de sécurité du produit à évaluer et du réseau lui-même. Et enfin, nous présenterons les résultats de l'évaluation effectuée par le biais de la base de connaissances MEHARI.

5.3.1 Profils de protection et cible de sécurité

Comme nous l'avons mentionné précédemment, les profils se présentent comme des impératifs à remplir pour le fonctionnement idéal du réseau. Les exigences de sécurité qu'une entité doit intégrer, conformément aux profils de protection précédemment définis, sont citées en dessous de chacun d'eux :

- Sécurité de l'architecture du réseau local :
  - Partitionnement du réseau local en domaines de sécurité.
  - Sûreté de fonctionnement des éléments d'architecture du réseau local.
  - Organisation de la maintenance des équipements du réseau local.
  - Procédures et plans de reprise du réseau local sur incidents.
  - Plan de sauvegarde des configurations du réseau local.
  - Plan de Reprise d'Activité (PRA) du réseau local.
  - Gestion des fournisseurs critiques vis-à-vis de la permanence de la maintenance.
- Contrôle d'accès sur le réseau local de données :
  - Gestion des profils d'accès au réseau local de données.
  - Gestion des autorisations d'accès et privilèges (attribution, délégation, retrait).
  - Authentification de l'utilisateur ou de l'entité demandant un accès au réseau local depuis un point d'accès interne. Ce mécanisme correspond à l'authentification réalisée sous Windows par un contrôleur de domaine.
  - Authentification de l'utilisateur ou de l'entité demandant un accès au réseau local depuis un site distant via le réseau étendu.

- Authentification de l'utilisateur ou de l'entité demandant un accès au réseau local depuis l'extérieur. (depuis le Réseau Téléphonique Commuté, X25, RNIS, ADSL, Internet, etc.).
- Authentification de l'utilisateur ou de l'entité demandant un accès au réseau local depuis un sous-réseau WiFi.
- Filtrage général des accès au réseau local.
- Contrôle du routage des accès sortants.
- Authentification de l'entité accédée lors des accès sortants vers des sites sensibles.

- Sécurité des données lors des échanges et des communications sur le réseau :
  - Chiffrement des échanges sur le réseau local.
  - Protection de l'intégrité des échanges sur le réseau local.
  - Chiffrement des échanges lors des accès distants au réseau local.
  - Protection de l'intégrité des échanges lors des accès distants au réseau local.
- Contrôle, détection et traitement des incidents du réseau local :
  - Surveillance (en temps réel) du réseau local.
  - Analyse (en temps différé) des traces, logs et journaux d'événements sur le réseau local.
  - Traitement des incidents du réseau local.

Concernant l'exploitation du réseau, ces éléments sont à observer :

- Contrôle d'accès aux systèmes :
  - Gestion des profils d'accès (droits et privilèges accordés en fonction des profils de fonction).
  - Gestion des autorisations d'accès et privilèges (attribution, délégation, retrait).
  - Authentification de l'utilisateur ou de l'entité demandant un accès.
  - Filtrage des accès et gestion des associations.
  - Authentification du serveur lors des accès à des serveurs sensibles.
- Confinement des environnements :
  - Contrôle des accès aux résidus.
- Gestion et enregistrement des traces :

- Enregistrement des accès aux ressources sensibles.
- Enregistrement des appels aux procédures privilégiées.

- Sécurité de l'architecture :
  - Sûreté de fonctionnement des éléments d'architecture.
  - Isolement des systèmes sensibles.

Les exigences fonctionnelles sont ainsi regroupées sous forme de classes, chaque classe couvrant un domaine particulier. Chaque classe contient un ensemble de familles, et chaque famille contient un ensemble de composants. Chaque composant définit une exigence de sécurité. Ce sont ces exigences de sécurité qui représentent dans la cible de sécurité à savoir l'ensemble des mesures que l'on doit édifier afin de parer ses risques informatiques. Il s'agira justement dans le prochain chapitre d'effectuer une analyse de ce qui se fait dans l'entreprise comparativement à ces postulats et de mesurer l'efficacité du dispositif en place.

5.3.2 Evaluation du dispositif de maîtrise

Il est nécessaire de préciser que les questionnaires d'audit de la sécurité sont précisément organisés en fonction des domaines de responsabilité. Dans le cadre de la banque, la direction informatique est en charge du réseau et de sa sécurité. Notre étude a donc été effectuée avec ladite direction et le service d'audit interne.

En ce qui concerne l'usage des questionnaires, certains cas de difficultés se sont avérés telles que des réponses de ce genre :

- Oui en général mais avec des exceptions.
- Oui en théorie, mais, en pratique, ce n'est pas certain ou pas appliqué partout.
- Oui partiellement, à X%.
- Oui, en cours de déploiement.
- Oui, c'est prévu mais non encore appliqué.

Toutefois, en fonction des explications accompagnant les réponses, nous avons du prendre parti afin que nos recommandations n'occultent pas l'imperfection constatée ou

démotivent les utilisateurs et décrédibilise notre évaluation. En outre, tel que le précise MEHARI pour les entités qui ne sont qu'en phase de démarrage de la sécurité en l'occurrence la BCI, l'ensemble des questionnaires de la base peut s'avérer disproportionné par rapport à l'état de sécurité. C'est pour cette raison que nous avons modulé les questionnaires afin de les limiter à des interrogations plus déterminantes.

5.3.2.1. Importance des services du réseau local selon les directions

Ainsi nous avons interrogé les responsables de chaque direction de la banque sur l'importance qu'ils accordent au réseau local de la banque, selon une échelle de 1 à 4, suivant sa disponibilité et son intégrité. Ces données se pondérés par la base de connaissances aux questionnaires afin d'aboutir à des recommandations pertinentes. Il en est ressorti ceci :

Tableau 2 : Cotation de l'importance des services du réseau local par direction

Processus métier, application ou domaine applicatif **Services communs**	**FONCTION (descriptif)**	**CLASSIFICATION DES SERVICES**	
		Services du réseau local	
		D	**I**
Nom de colonne pour formules Classification		**R02**	**R02**
Processus métiers			
Domaine 1 : Direction audit et contrôle interne	Contrôle des tâches confiées aux services et veille au respect des règles de travail édictées par les procédures de la banque	**4**	**4**
Domaine 2 : Direction risques et engagements	Définition des politiques de risques et la gestion des engagements de la banque.	**4**	**4**
Domaine 3 : Direction exploitation et réseau	Administration des opérations avec l'ensemble des agences ainsi	**4**	**4**

	qu'à l'international		
Domaine 4 : Direction finances et comptabilité	Mettre au service de la rentabilité de l'entreprise les ressources et les techniques financières, et apprécier, puis contrôler l'intérêt économique des projets.	**4**	**4**
Domaine 5 : Département juridique	Chargée de toutes les questions juridiques de la banque en sus du recouvrement amiable et contentieux afin d'optimiser le taux de recouvrement des créances clients de la banque.	**4**	**4**
Domaine 6 : Département opérations	Coordination de l'ensemble des transactions et activités de la banque	**4**	**4**
Domaine 7 : Département informatique	Garantir l'assurance d'une qualité de service optimum	**4**	**4**
Processus transverses			
Administration/ politique d'ensemble		**3**	**3**
Classification		**4**	**4**

Source : Feuille T², DB-Mehari_2010_Exc_Fr_2-20, Base de connaissances de MEHARI exploitée suivant les données recueillies auprès des directeurs de département.

5.3.2.2. Importance des données circulant par le réseau local selon les directions

En sus, nous avons recueilli leur avis sur l'importance qu'ils accordaient aux données circulant sur le réseau par rapport à leur disponibilité, leur intégrité et leur conformité. Tout ceci concourt à la pondération interne de la base de connaissances.

Tableau 3 : Réponses des directeurs sur l'importance accordée aux données

Processus métier, domaine applicatif ou domaine d'activité Services communs à particulariser	CLASSIFICATION DES DONNÉES																				
	Données applicatives (bases de données)			Données applicatives isolées, en transit Messages			Fichiers bureautiques partagés			Fichiers bureautiques personnels			Courrier électronique			Archives informatiques			Données publiées (web ou interne)		
	D	I	C	D	I	C	D	I	C	D	I	C	D	I	C	D	I	C	D	I	C
Types d'actifs	D01	D01	D01	D06	D06	D06	D02	D02	D02	D03	D03	D03	D07	D07	D07	D10	D10	D10	D11	D11	D11
Processus métiers																					
Domaine 1 : Direction audit et contrôle interne	4	4	4	3	4	3	3	3	3	1	1	1	1	1	1	3	4	3	1	1	1
Domaine 2 : Direction risques et engagements	2	3	4	1	3	2	3	4	4	1	1	1	1	1	1	4	4	4	3	4	4
Domaine 3 : Direction exploitation et réseau	4	4	4	3	4	4	2	3	3	1	1	1	3	4	3	4	4	4	3	4	4
Domaine 4 : Direction finances et comptabilité	4	4	4	4	4	4	3	4	3	1	1	1	3	4	3	4	4	4	3	4	3
Domaine 5 : Département juridique	3	4	4	2	2	2	2	2	2	2	3	3	2	2	2	4	4	4	4	4	4

Domaine 6 : Département opérations	4	4	4	3	4	4	2	2	2	1	1	1	2	2	2	4	4	4	4	4	4
Domaine 7 : Département informatique	4	4	4	4	4	4	3	3	3	1	1	1	2	2	2	3	3	3	3	3	3
Processus transverses																					
Direction générale / politique d'ensemble	2	3	4	2	3	4	1	2	2	3	3	3	3	3	3	4	4	4	4	4	4
Classification	4	4	4	4	4	4	3	4	4	3	3	3	3	4	3	4	4	4	4	4	4

Source : Feuille T[1], DB-Mehari_2010_Exc_Fr_2-20, Base de connaissances de MEHARI exploitée suivant les données recueillies auprès des directeurs de département.

5.3.2.3. Résultats du questionnaire d'audit sur le réseau local et son exploitation

MEHARI considère dans le déploiement de son questionnaire que les réponses « oui » sont intégrées par la valeur « 1 » et les réponses « non » par la valeur « 0 ». Comme nous l'avons précisé dans les lignes antérieures, certaines question seront sans objet avec la mention « X » parce que non applicables à la banque dont la sécurité est en phase de démarrage. Ces résultats sont présentés respectivement en ANNEXE 2 et 3.

5.3.2.4. Résultats de la cotation des services de sécurité

En fonction des résultats des questionnaires, la base de connaissances de MEHARI établit une évaluation des services de sécurité que l'entité devrait considérer. A ce niveau, elle intègre déjà un niveau minimum que certains services doivent atteindre en les désignant par « Min ». Il s'agit du niveau acceptable qui offre à l'entité des garanties quand à l'efficacité du service. Cependant, ce niveau peut être modifié selon les attentes de la banque et ses finalités d'où la colonne « Fin ». Dans le cadre de la banque, nous avons considéré que le niveau minimum est celui recherché donc il sera identique à la finalité. C'est partant de la cotation sur le niveau des services actuels que la base effectue la comparaison avec le niveau minimum recherché et suggère ce qui devrait être mis en place par la suite afin d'atteindre ledit niveau. Ainsi, nous avons obtenu :

Tableau 4 : Cotation des services de sécurité

SERVICES ET SOUS-SERVICES DE SECURITE			Prise en compte objectifs :		
DOMAINES					
	SERVICES				
		SOUS-SERVICES		Min	Fin
05	**Réseau local**		**VI**		
	A - Sécurité de l'architecture du réseau local				
	05A01	Partitionnement du réseau local en domaines de sécurité	2,0	2,0	2,0
	05A02	Sûreté de fonctionnement des éléments d'architecture du réseau local	2,0	2,0	2,0
	05A03	Organisation de la maintenance des équipements du réseau local	0,0	0,0	1,0
	05A04	Procédures et plans de reprise du réseau local sur incidents	2,0	2,0	2,0

	05A05	Plan de sauvegarde des configurations du réseau local	0,6	1,0	1,0
	05A06	Plan de Reprise d'Activité (PRA) du réseau local	2,0	2,0	2,0
	05A07	Gestion des fournisseurs critiques vis-à-vis de la permanence de la maintenance	0,0	0,0	1,0
	B - Contrôles d'accès sur le réseau local de "données"				
	05B01	Gestion des profils d'accès au réseau local de données	2,0	2,0	2,0
	05B02	Gestion des autorisations d'accès et privilèges (attribution, délégation, retrait)	2,0	2,0	2,0
	05B03	Authentification de l'utilisateur ou de l'entité demandant un accès au réseau local depuis un point d'accès interne Ce mécanisme correspond à l'authentification réalisée sous Windows par un contrôleur de domaine	2,0	2,0	2,0
	05B04	Authentification de l'utilisateur ou de l'entité demandant un accès au réseau local depuis un site distant via le réseau étendu	X	1,0	1,0
	05B05	Authentification de l'utilisateur ou de l'entité demandant un accès au réseau local depuis l'extérieur (depuis le Réseau Téléphonique Commuté, X25, RNIS, ADSL, Internet, etc.)	2,0	2,0	2,0
	05B06	Authentification de l'utilisateur ou de l'entité demandant un accès au réseau local depuis un sous-réseau WiFi	X	1,0	1,0
	05B07	Filtrage général des accès au réseau local	2,0	2,0	2,0
	05B08	Contrôle du routage des accès sortants	X	1,0	1,0
	05B09	Authentification de l'entité accédée lors des accès sortants vers des sites sensibles	X	1,0	1,0
	C - Sécurité des données lors des échanges et des communications sur le réseau local				
	05C01	Chiffrement des échanges sur le réseau local		1,0	1,0
	05C02	Protection de l'intégrité des échanges sur le réseau local		1,0	1,0
	05C03	Chiffrement des échanges lors des accès distants au réseau local	x	1,0	1,0
	05C04	Protection de l'intégrité des échanges lors des accès distants au réseau local	x	1,0	1,0
	D - Contrôle, détection et traitement des incidents du réseau local				
	05D01	Surveillance (en temps réel) du réseau local	0,9	1,0	1,0
	05D02	Analyse (en temps différé) des	0,5	1,0	1,0

		traces, logs et journaux d'événements sur le réseau local			
	05D03	Traitement des incidents du réseau local	1,3	1,0	1,0
06	**Exploitation des réseaux**		VI		
	A - Sécurité des procédures d'exploitation				
	06A01	Prise en compte de la sécurité dans les relations avec le personnel d'exploitation (salariés et prestataires)	1,0	1,0	1,0
	06A02	Contrôle de la mise en production de nouveaux logiciels ou matériels ou d'évolutions de logiciels ou matériels	2,0	2,0	2,0
	06A03	Contrôle des opérations de maintenance	2,7	3,0	3,0
	06A04	Contrôle de la télémaintenance	X	1,0	1,0
	06A05	Gestion des procédures opérationnelles d'exploitation des réseaux	0,0	0,0	1,0
	06A06	Gestion des prestataires ou fournisseurs de services liés aux réseaux	1,3	1,0	1,0
	06A07	Prise en compte de la confidentialité lors des opérations de maintenance sur les équipements de réseau	0,5	1,0	1,0
	06A08	Gestion des contrats de services réseaux	X	1,0	1,0
	B - Paramétrage et contrôle des configurations matérielles et logicielles				
	06B01	Paramétrage des équipements de réseau et contrôle de la conformité des configurations	0,0	0,0	1,0
	06B02	Contrôle des configurations des accès réseaux des postes utilisateurs	0,0	0,0	1,0
	C - Contrôle des droits d'administration				
	06C01	Gestion des droits privilégiés sur les équipements de réseau	0,3	0,0	1,0
	06C02	Authentification et contrôle des droits d'accès des administrateurs et personnels d'exploitation des réseaux	2,3	2,0	2,0
	06C03	Surveillance des actions d'administration des réseaux	2,0	2,0	2,0
	06C04	Contrôle des outils et utilitaires de l'exploitation du réseau	X	1,0	1,0
	D - Procédures d'audit et de contrôle des réseaux				
	06D01	Fonctionnement des contrôles d'audit	0,6	1,0	1,0
	06D02	Protection des outils et résultats d'audit	X	1,0	1,0

Source : Feuille « Services », DB-Mehari_2010_Exc_Fr_2-20, Base de connaissances de MEHARI exploitée suivant les pondérations effectuées par la base.

Conclusion

La structure interne de la banque en charge de ces aspects est encore orientée que vers le maintien des applications, leur amélioration, la maintenance des postes et la garantie de la disponibilité d'un niveau acceptable de la marche de la plateforme de travail. Le dispositif de contrôle interne du réseau est quasi-inexistant ; les dirigeants ont récemment émis la volonté de migrer vers une formalisation de tous ces éléments.

Nombreux aspects relatifs au système d'informations sont encore en gestation. Il est donc opportun de relever cet aspect qui sera prépondérant lors de l'évaluation de la maîtrise risques à venir. Cependant, il est dans les objectifs de la banque, une évolution des responsabilités du service selon le développement des activités et l'élaboration de politiques formels.

Chapitre 6 : Analyse des résultats et recommandations

Introduction

L'analyse des risques est citée et considérée comme devant être la base des actions de sécurité à plus d'un titre. Toutefois, il s'avère que le sens donné à l'expression « gestion des risques » peut varier d'une organisation à une autre et qu'en fonction des objectifs poursuivis, les méthodes supports peuvent être considérablement différentes ainsi que les priorités.

L'institution ne possède pas encore une méthode propre à elle ou modifiée par elle puisqu'aucune évaluation des risques n'a encore été réalisée relativement au réseau informatique encore moins une mise en place de dispositif de maitrise. MEHARI, que nous utilisons dans cette étude, est conçue pour aider les responsables de la sécurité des systèmes d'informations dans leur tâche de gestion et de pilotage de la sécurité de l'information et des systèmes d'informations.

L'objectif premier de la méthode étant de fournir une méthode d'analyse et de gestion des risques dans le domaine de la sécurité de l'information. Néanmoins, cette sécurité englobe plusieurs éléments. Pour ce faire, il a été procédé dans un premier temps à un bilan de l'état de la sécurité du réseau informatique. Nous exposerons la valeur ajoutée qu'apporte les quelques dispositifs en place et les améliorations pouvant être introduites.

6.1 Analyse des résultats

Dans l'utilisation de la base de données de MEHARI, certains éléments ont été sciemment omis parce que non applicables à la banque. Ils sont rappelés au fur et à mesure. Ce point est scindé en trois volets représentant l'épine dorsale même du processus d'évaluation des risques.

6.1.1 Etat de la cible de l'évaluation

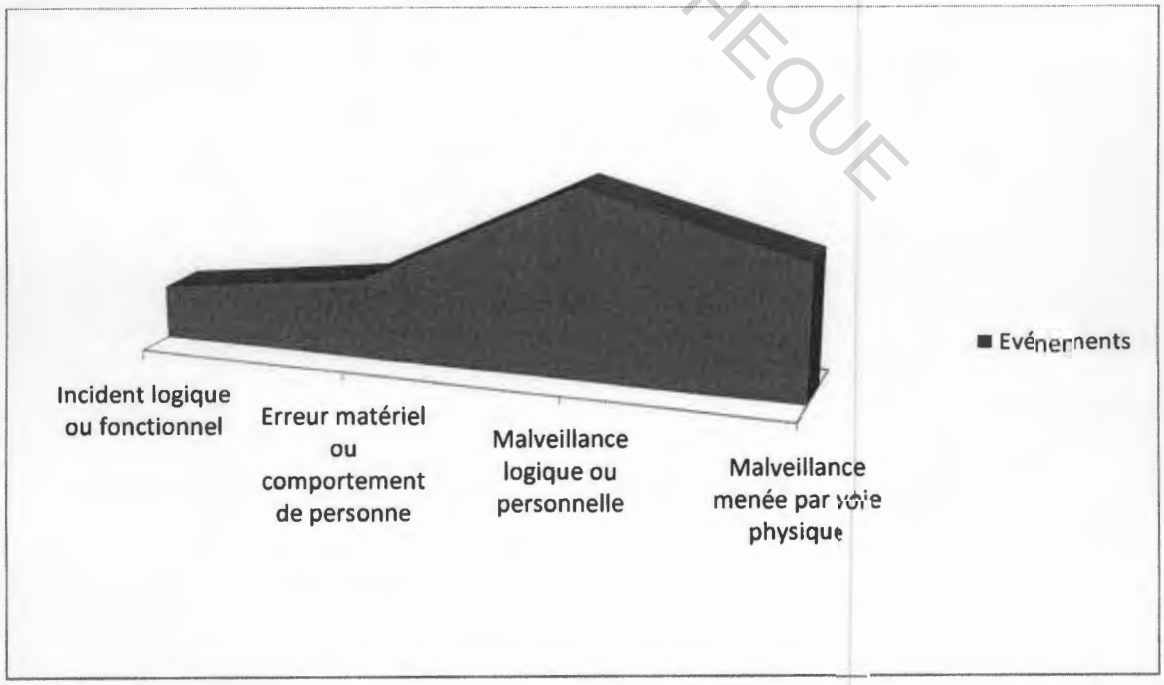
Pour ne retenir que l'essentiel, une situation de risque peut être caractérisée par divers facteurs :

- Des facteurs structurels qui ne dépendent pas des mesures de sécurité, mais du métier de l'entreprise, de son environnement et de son contexte.
- Des facteurs de réduction de risque qui sont directement fonction des mesures de sécurité mises en place.

Il est donc opportun de déterminer d'identifier les mesures dans lesquelles l'institution appréhende ces risques. Ces résultats nous sont présentés dans le tableau 5 mais il serait intéressant avant cela de mettre en exergue les principales menaces dont la banque est l'objet.

Nous regroupons au sein des paramètres de menaces, les évènements, les personnes et les lieux formant le risque en question. A cet effet, notre constat nous montre que le réseau local de la banque est sous la menace des facteurs suivants, sachant que nous avons représenté les plus importants:

Figure 5: Principaux facteurs de menace



Source : Suivant la Feuille Risk%Event sur le tableau des évènements à risques, DB-Mehari_2010_Exc_Fr_2-20, Base de connaissances de MEHARI exploitée.

Au-delà de ces évènements et principales sources de menaces, il a été relevé que les acteurs, qui peuvent être de façon potentielle, essentiellement à l'origine sont dans l'ordre :

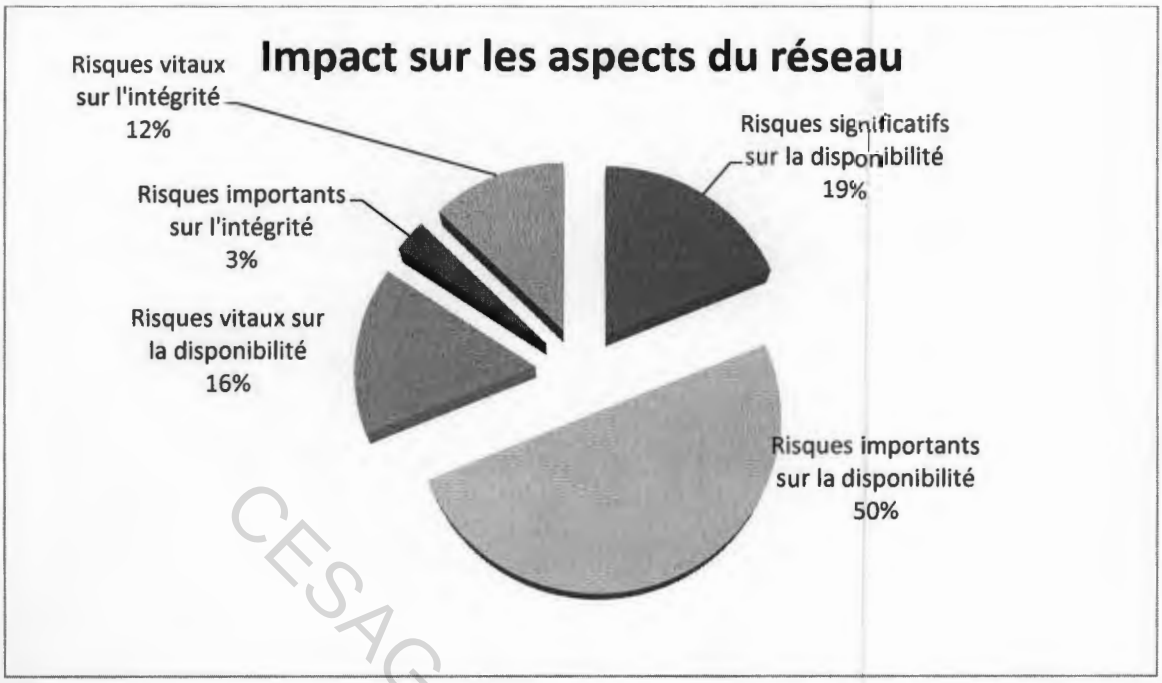
- Le personnel même du service informatique, parce que ayant les entiers privilèges sur le réseau et que les utilisateurs craignent souvent l'intrusion dans certaines fonctionnalités de leurs postes de travail ;
- Les utilisateurs non autorisés comme les stagiaires ;
- Les membres du personnel autorisé.

Pour appréhender ces aspects, la banque a déjà mis en place des parades tels que :

- Le contrôle de la mise en production de nouveaux logiciels ou matériels ou d'évolutions de logiciels ou matériels ;
- L'authentification et contrôle des droits d'accès des administrateurs et personnel d'exploitation des réseaux ;
- La surveillance des actions d'administration réseaux.
- Un plan de sauvegarde quasi formel des configurations du réseau local ;
- Un traitement des incidents du réseau local dès leur apparition ;
- Une analyse des traces, logs et journaux d'événements sur le réseau local ;
- Une assurance du fonctionnement des éléments d'architecture du réseau local ;
- Une organisation de la maintenance du réseau local de la banque ;
- Des procédures et plans de reprise du réseau local sur incidents.

Il faut toutefois remarquer que ces contrôles ne sont pas exercés en entier pour maintes raisons dont certaines ont été évoquées précédemment et comme le tableau 5 nous le montre. Ainsi la figure suivant nous éclaire sur les aspects du réseau les plus impactés en fonction des sécurités en place.

Figure 6: Aspects du réseau impactés



Source : Suivant la Feuille Risk%Actif sur le panorama de la gravité des scénarios de risques, DB-Mehari_2010_Exc_Fr_2-20, Base de connaissances de MEHARI exploitée.

6.1.2 Etude des résultats sur l'évaluation des exigences de l'analyse de la configuration des équipements du réseau

La procédure de vérification de la configuration des équipements du réseau débute par l'analyse de la politique de sécurité. Ce dernier est inexistant dans la banque, donc aucun document ne prédéfinit ce qui devrait être fait, selon la volonté des dirigeants, dans la configuration des équipements. Il en résulte que les équipements sont gérés de manière non officielle sans suivre une procédure au préalable. L'on fait appel à des techniciens externes dans certaines situations et à ce niveau encore, aucune procédure sécuritaire valable n'est établie pour annihiler une quelconque fuite d'informations, hormis un contrat de prestation de service.

L'organisation de la maintenance des équipements du réseau local faisant parti de la configuration du réseau, la cotation nous montre qu'elle n'est pas prise en compte par l'entité avec un niveau 0, de même que la gestion des fournisseurs critiques vis-à-vis de la maintenance. Dans la mesure où la banque ne s'en tient qu'à des éléments basiques de son

réseau, la maintenance devrait avoir un poids beaucoup plus important de ce qui a été constaté.

Les éléments les mieux pris en compte, c'est-à-dire qu'ils ont un niveau correspondant au minimum requis, sont :

- le partitionnement du réseau local en domaines de sécurité ;
- la sûreté de fonctionnement des éléments d'architecture du réseau local ;
- les procédures et plans de reprise du réseau local sur incidents ;
- le plan de reprise d'activités ;
- le contrôle de la mise en production de nouveaux logiciels ou matériels d'évolution ;
- la surveillance d'actions des administrations réseaux.

Nos recommandations concerneront alors dans un dessein d'amélioration :

- l'organisation et la maintenance des équipements du réseau local,
- le plan de sauvegarde des configurations du réseau local,
- la surveillance en temps réel du réseau local,
- le contrôle des opérations de maintenance,
- la prise en compte de la confidentialité lors des opérations de maintenance sur les équipements réseau,
- la gestion gestion des droits privilégiés sur les équipements réseau.

Toutefois, d'autres éléments dépassent largement le minimum exigé en matière de sécurité en l'occurrence :

- le contrôle des opérations de maintenance,
- la gestion des prestataires ou fournisseurs de services liés au réseau.

Il est évident que la banque accorde plus d'importance à la maintenance de ses équipements contrairement à d'autres facettes qui devraient être considérés au même niveau.

6.1.3 Etude du dispositif d'analyse de la configuration des systèmes d'information

A ce niveau, nous avons considéré surtout les accès à la plateforme et les droits d'administration. L'institution remplit les exigences de sécurité minimum concernant :

- la gestion des profils d'accès ;
- la gestion des autorisations d'accès et privilèges ;
- l'authentification de l'utilisateur ou de l'entité demandant un accès au réseau local depuis un point d'accès interne ;
- l'authentification de l'utilisateur ou de l'entité demandant un accès au réseau local depuis l'extérieur ;
- un filtrage général des accès au réseau local ;
- la surveillance des actions d'administration des réseaux.

Sur 10 points essentiels d'exigences de sécurité concourant à l'analyse de la configuration des systèmes d'informations, la banque remplit 7 conditions. Ce fait est du à l'importance qu'elle accorde à sa plateforme via laquelle elle effectue toutes ses opérations. Elle a même franchi le seuil minimum pour ce qui est de l'authentification et le contrôle des droits d'accès des administrateurs et personnels d'exploitation des réseaux. Tout ceci concourt à la sécurité des données mais elle doit se pencher sur la gestion des droits privilégiés sur les équipements de réseau.

6.1.4 Etude du dispositif d'analyse des traces

Dans cette partie, il était question d'examiner si les exigences de sécurité en matière d'analyse des évènements du système d'exploitation sont respectées. Un premier constat à énumérer est que ce volet n'est pas aussi pris en compte par l'entité que le contrôle des accès et les parades techniques tels que les pare-feux.

L'unique élément qui surnage dans ce lot est le traitement des incidents du réseau local. La banque marque un point d'honneur à endiguer ces évènements car ils sont susceptibles d'entacher leur image.

Toutefois, les sécurités de la surveillance du réseau local et l'analyse des traces, logs et journaux d'évènements sur le réseau ne présentent pas tous les éléments acceptables pour un seuil minimum. Bien que le service informatique arrive à identifier les traces des utilisateurs et leurs historiques de log, cette simple exigence ne saurait convenir à l'institution dans le cadre de la sécurisation de son réseau.

6.2 Recommandations

Les sécurités identifiées et analysées, vient la prise de décision des mesures à entreprendre ou à améliorer afin de rendre plus efficace le dispositif de maitrise. La banque étant au démarrage de son système de sécurité, de nombreux pas sont à franchir. Nous ne manquerons pas de les énumérer dans nos recommandations. Nous avons aussi tenu compte du fait que certaines dispositions sont déjà présentes mais non documentées. Nous confinerons dans un tableau les services de sécurité adéquats à mettre en place. Les niveaux de sécurité font l'objet d'une cotation de 1 à 4 de façon croissant selon le degré d'efficacité. Nous partons alors d'un niveau minimum à un niveau ciblé par la banque elle-même. Il est nécessaire de préciser qu'elles sont faites à la fois aux service d'audit interne et au département informatique qui sont les deux principaux domaine de responsabilité dans cette étude.

Tableau 1: Recommandations

Service de sécurité à mettre en place		Niveau actuel	Niveau ciblé	Type de recommandations
Pr	Contrôle de la mise en production de nouveaux logiciels ou matériels ou d'évolutions de logiciels ou matériels	2	4	• Les installations doivent être faites avec un souci de protection physique (accès protégé, absence de vue directe externe sur les équipements, absence de menaces physiques diverses, conditions climatiques, protection contre la foudre, protection contre la poussière, etc.) • Une revue formelle des nouvelles fonctionnalités (ou des changements de fonctionnalités) liées à un changement majeur de logiciel ou d'équipement doit être systématiquement réalisée, avec le concours de la fonction sécurité informatique. • Cette revue doit comprendre une analyse des risques éventuels pouvant naître à cette occasion. • L'exploitation doit recevoir une formation spécifique à l'analyse des risques. • L'exploitation doit avoir la possibilité de faire appel à un support adapté pour de telles analyses de risques. • Les mesures de sécurité décidées pour remédier aux nouveaux risques mis en évidence doivent faire l'objet de contrôles et de tests formels avant mise en exploitation. • Les paramétrages de sécurité et règles de configuration (suppression de tout compte générique, changement de tout mot de passe générique, fermeture de tout port non explicitement demandé et autorisé, paramétrages du contrôle des droits et de l'authentification, contrôles des tables de routage, etc.) doivent faire l'objet d'une liste précise tenue à jour. • Les paramétrages de sécurité et règles de configuration doivent être contrôlés avant toute

				mise en exploitation d'une nouvelle version. • L'impact éventuel des changements de systèmes sur les plans de continuité doit être pris en compte. • Les dérogations au processus d'analyse de risque préalable et aux contrôles des paramètres de sécurité doivent faire l'objet de procédures strictes avec signature d'un responsable de niveau élevé. • La mise en production de nouvelles versions d'équipements ou de logiciels doit être effectuée que par le personnel d'exploitation ? • La mise en production de nouvelles versions d'équipements ou de logiciels doit être possible que selon un processus de validation et d'autorisation défini ? • L'ensemble des procédures de contrôle de la mise en production doit faire l'objet d'un audit régulier.
C	Traitement des incidents du réseau local	1	4	• Un système support de la gestion des incidents doit être établi. • Ce système doit centraliser et prendre en compte aussi bien les incidents détectés par l'exploitation que ceux signalés par les utilisateurs. • Ce système doit permettre un suivi et une relance automatiques des actions nécessaires. • Ce système doit incorporer une typologie des incidents avec élaboration de statistiques et de tableau de bord des incidents à destination du service informatique. • Le système de gestion d'incidents doit être strictement contrôlé vis-à-vis de toute modification illicite ou indue. *Un contrôle strict requiert une protection renforcée pour pouvoir modifier un enregistrement et un audit de toute modification des enregistrements ou un contrôle par scellement électronique de toute modification.*
Pa	Plan de sauvegarde des configura-	1	3	• Le plan de sauvegarde des configurations du réseau local doit être formalisé et traduit en

Pa Pa	tions du réseau local			automatismes de production. • Les sauvegardes des programmes (sources et/ou exécutables), de leur documentation et de leur paramétrage doivent permettre effectivement de reconstituer à tout moment l'environnement de production. • Les automatismes de production assurant les sauvegardes doivent être protégés par des mécanismes de haute sécurité contre toute modification illicite ou indue. *Un tel mécanisme pourrait être un scellement électronique ou tout système de détection de modification équivalent.* • L'ensemble des sauvegardes et fichiers de configuration permettant de reconstituer l'environnement de production doit être également sauvegardé en dehors du site de production (sauvegardes de recours). • Ces copies de sauvegarde de recours doivent être conservées dans un local sécurisé et protégé des risques accidentels et d'intrusion. *Un tel local devrait être protégé par un contrôle d'accès renforcé et, en outre, être protégé contre les risques d'incendie et de dégâts des eaux.* • Il doit être procédé régulièrement à des tests de relecture des sauvegardes et sauvegardes de recours. • L'ensemble des procédures et plans de sauvegarde des fichiers de configuration doit faire l'objet d'un audit régulier ?
Pr	• Sûreté de fonctionnement des éléments d'architecture du réseau local	2	3	• Chaque domaine de sécurité doit être analysé pour déterminer les exigences de continuité de service et en déduire, si nécessaire, une architecture de redondance au niveau des points d'interconnexion, des équipements et du maillage du réseau. • Une recherche systématique des Points Singuliers de Vulnérabilité ("Single Point of Failure") doit être effectuée afin de s'assurer que des équipements, en particulier de servi-

				tude, (alimentation en énergie, climatisation, etc.) n'en introduisent pas ou ne détruisent pas les redondances prévues au niveau des équipements ou de l'architecture. • Une analyse de la charge moyenne et crête de chaque segment de réseau, la compatibilité du réseau et de ses équipements doit être avec cette charge et cette vérification être régulièrement réactualisée. • Cette analyse doit être complétée par une étude des capacités du réseau à assurer les communications dans tous les cas de pannes simples de liaisons ou d'équipements • Les outils de monitoring et de reconfiguration du réseau doivent permettre une action en temps réel compatible avec les besoins des utilisateurs. • L'architecture des équipements de réseau doit permettre une adaptation facile aux évolutions de charge (clusters, grappes, etc.). • Il doit être régulièrement procédé à des tests de performance des mécanismes de détection et de reconfiguration. • Il doit être régulièrement procédé à un audit du paramétrage des systèmes de détection et de reconfiguration. • Il doit être régulièrement procédé à un audit des procédures associées aux systèmes de détection et de reconfiguration.
C	• Plan de Reprise d'Activité (PRA) du réseau local	2	3	• Les sauvegardes des programmes (sources et/ou exécutables), de leur documentation et de leur paramétrage doivent permettre effectivement de reconstituer à tout moment l'environnement de production. • Les automatismes de production doivent assurer les sauvegardes sont protégés par des mécanismes de haute sécurité contre toute modification illicite ou indue. *Un tel mécanisme pourrait être un scellement électronique ou tout système de détection de modification équivalent.*

				• L'ensemble des sauvegardes et fichiers de configuration doivent permettre de reconstituer l'environnement de production et également sauvegardé en dehors du site de production (sauvegardes de recours). • Ces copies de sauvegarde de recours doivent être conservées dans un local sécurisé et protégé des risques accidentels et d'intrusion. *Un tel local devrait être protégé par un contrôle d'accès renforcé et, en outre, être protégé contre les risques d'incendie et de dégâts des eaux.* • Il doit être procédé régulièrement à des tests de relecture des sauvegardes et sauvegardes de recours. • L'ensemble des procédures et plans de sauvegarde des fichiers de configuration doivent faire l'objet d'un audit régulier.
	Organisation de la maintenance des équipements du réseau local	0	3	• Tous les équipements du réseau local doivent être couverts par un contrat de maintenance. • Les équipements critiques pour l'exploitation et la tenue des performances annoncées doivent être identifiés et, pour ceux-ci, les délais de remise en service souhaitable et les délais maximum tolérables en cas de défaillance. • Des clauses particulières et adaptées à ces exigences doivent être intégrées dans les contrats de maintenance. • Les pénalités en cas de non tenue des engagements par le titulaire du contrat de maintenance doit être réellement dissuasives ? • Les procédures d'escalade en cas de difficulté de maintenance doivent être précisées et doivent prévoir l'intervention de spécialistes dans des délais courts compatibles avec la criticité des équipements. • Le nombre et la proximité des spécialistes doivent être précisés et données une bonne ga-

				rantie de maintenance dans des délais acceptables. • Les contrats de maintenance doivent prévoir le remplacement complet des équipements en cas d'endommagement important non susceptible d'être pris en charge par une maintenance curative. • Les contrats de maintenance et les procédures de maintenance associées doivent faire l'objet d'un audit régulier.
Pr	Analyse (en temps différé) des traces, logs et journaux d'événements sur le réseau local	1	4	• Une analyse approfondie des événements ou succession d'événements pouvant avoir un impact sur la sécurité (connexions refusées, reroutages, reconfigurations, évolutions de performances, accès à des informations ou des outils sensibles, etc.) doit être faite. • Il doit être enregistré ces événements ainsi que tous les paramètres utiles à leur analyse ultérieure. • Il doit être défini pour chaque cas d'alerte, la réaction attendue de l'équipe de surveillance et sa disponibilité doit être suffisante pour faire face à cette attente. • Les paramètres définissant les éléments à enregistrer et les synthèses effectuées sur ces éléments doivent être strictement protégés (droits limités et authentification forte) contre tout changement illicite. • Toute inhibition du système d'enregistrement et de traitement des enregistrements doit déclencher une alarme auprès de l'équipe de surveillance. • Les enregistrements ou les synthèses doivent être protégés contre toute altération ou destruction. • Les enregistrements ou les synthèses doivent être conservés sur une longue durée. • Les procédures d'enregistrement, de traitement des enregistrements et d'analyse des synthèses ainsi que la disponibilité de l'équipe d'analyse et d'intervention doivent faire l'objet d'un audit régulier.

C	Surveillance (en temps réel) du réseau local	1	4	• Le système doit disposer d'une fonction automatique de surveillance en temps réel en cas d'accumulation d'événements anormaux (par exemple tentatives infructueuses de connexion sur des ports non ouverts, etc.). • Un système de détection d'intrusion et d'anomalies doit être mis en place. • Pour chaque cas d'alerte, la réaction attendue de l'équipe d'intervention et sa disponibilité doit être définie et être suffisante suffisante pour faire face à cette attente. • Il doit être effectué un archivage (sur disque, cassette, Disque Optique Numérique, etc.) de tous les éléments ayant permis de détecter une anomalie ou un incident. • Les procédures de surveillance du réseau et de détection d'anomalies et la disponibilité de l'équipe de surveillance doivent faire l'objet d'un audit régulier.
Pr	Contrôle de la mise en production de nouveaux logiciels ou matériels ou d'évolutions de logiciels ou matériels	Id	Id	Id
Pr	Paramétrage des équipements de réseau et contrôle de la conformité des configurations	0	4	• Il doit être élaboré un document (ou un ensemble de documents) ou une procédure opérationnelle spécifiant l'ensemble des paramètres de sécurité des équipements de réseau. *Un tel document doit découler de la politique de protection des réseaux et décrire l'ensemble des règles de filtrage décidées. Il devait également contenir les références des versions de systèmes pour pouvoir vérifier l'état des mises à jour.* • Ce document doit établir une liste de l'ensemble des comptes génériques et préconiser leur issue ? • Ces paramétrages doivent être régulièrement mis à jour en fonction de l'état des con-

				naissances, en relation avec un organisme expert (audits spécialisés)/ • Ces documents de référence (ou des copies des paramètres installés, considérées comme des références) doivent être protégés contre toute altération indue ou illicite, par des mécanismes forts. • Il doit procéder à des audits réguliers de la liste des paramètres de sécurité spécifiés ? • Il doit procéder à des audits réguliers des procédures d'exception et d'escalade en cas de difficulté.
D	Contrôle des opérations de maintenance	3	3	• La non application des procédures ci-dessus doit obligatoirement faire l'objet d'une dérogation formelle signée par un membre de la Direction. • L'ensemble des procédures de contrôle de la maintenance doit faire l'objet d'un audit régulier.
Pr	Paramétrage des équipements de réseau et contrôle de la conformité des configurations	Id	Id	Id
D Pr	Authentification et contrôle des droits d'accès des administrateurs et personnels d'exploitation des réseaux	2	3	• Il doit être commandité un audit régulier des profils privilégiés effectivement attribués. • Il doit être commandité un audit régulier des procédures d'attribution de profils privilégiés et des paramètres de sécurité de protection des profils et des droits ?
	Gestion des droits privilégiés sur les équipements de réseau	0	4	• Une politique de gestion des droits privilégiés sur les équipements de réseau s'appuie sur une analyse préalable des exigences de sécurité, basées sur les enjeux de l'activité. • Cette politique doit être documentée, revue régulièrement et approuvée par les responsables concernés. • Il doit être défini au sein de l'exploitation des réseaux, des profils correspondant à chaque type d'activité (administration d'équipements, administration d'équipement de sécurité, pilotage réseau, opérations de gestion de supports et sauvegardes, etc.).

				• Il doit être pour chaque profil, les droits privilégiés nécessaires. • La procédure d'attribution de droits privilégiés doit nécessiter l'accord formel de la hiérarchie (ou du responsable de la prestation pour un prestataire) à un niveau suffisant. • Le processus d'attribution (ou modification ou retrait) de droits privilégiés à un individu doit être strictement contrôlé ? *Un contrôle strict requiert une reconnaissance formelle de la signature (électronique ou non) du demandeur, qu'il existe un contrôle d'accès très renforcé pour pouvoir attribuer ou modifier de tels droits, et que les modifications d'attributions de droits privilégiés soient journalisées et auditées.* • Il doit être entrepris un audit régulier, au moins une fois par an, de l'ensemble des droits privilégiés attribués.

R = réduction
T = Transfert
A = Acceptation
Pr = Solution Préventive
Pa = Solution palliative
C = solution de confinement
D = Solution dissuasive
Id=Idem

Conclusion du chapitre

La jeunesse de la banque culpabilise certaines insuffisances en rapport avec le contrôle interne du réseau. Les mesures en place ne peuvent pas toutes couvrir les risques dont cette dernière peut faire l'objet. De plus, le top management bien qu'étant informé de ces expositions n'intègre pas encore l'élaboration de d'une politique de sécurité dans sa gouvernance. Toutefois, il est opportun de rappeler que comparativement aux autres banques de la place, l'institution est à un stade avancé de la sécurité de son réseau.

L'aspect majeur qui ressort ici est la nécessité de l'intégration dans la gouvernance de la banque d'une politique de sécurité élaborée et conforme aux exigences de sécurité. Nous mettons en exergue la nécessité aussi de faire évoluer le service en place vers un service de la sécurité du système d'informations dont la quintessence couvrent des aspects plus importants et productifs d'une valeur ajoutée.

Conclusion de la partie pratique

L'évaluation de la maitrise des risques liés au réseau informatique de la banque nous a été révélateur et source de valeur ajoutée. Il nous a permis de mettre en exergue certains risques mal perçus, non identifiés, importants comme non significatifs. Aussi a-t-il été un moyen pour attirer l'attention des dirigeants sur la nécessité de prendre en compte les risques liés à cet actif et par ricochet la nécessité d'évoluer vers la gestion des systèmes d'informations. Cette évolution procurerait une plus-value notable et une synergie productive de ressources informationnelles.

De la présentation des exigences requises à leur évaluation, l'implication des acteurs nous a permis d'exposer un certain nombres d'insuffisances déjà pris en compte mais dont les pourtours étaient non identifiés, ou difficilement applicables. Bien que nous n'ayons recouru qu'à l'aspect réseau local et l'exploitation du réseau de MEHARI, et adapter certains aspects au contexte de la banque, nous avons abouti à une cotation du dispositif de sécurité, permettant une analyse.

Les recommandations effectuées et tirées de MEHARI sont appropriées à une entité dans laquelle aucune évaluation n'a encore été effectuée. Les suggestions émises ont fait l'objet d'un consensus avec la direction de l'audit en tenant compte des ressources de l'entreprise, de la stratégie de la banque. Cependant nous nous sommes abstenus d'énoncer un plan d'actions dont les rênes sont aux mains des dirigeants de la banque.

Conclusion générale

Les institutions sont sous l'influence de leur environnement, pris dans tous les aspects. Ainsi, le chemin pris par les entités selon leur stratégie et leurs ressources ne perd pas de vue les apports extérieurs. Dans l'environnement Malien, ces postulats sont de rigueur, et rares sont les organisations qui arrivent à imposer au milieu un mode de fonctionnement tendant vers les modèles occidentaux. Cependant, d'énormes efforts sont entrepris pour uniformiser le milieu bancaire et sensibiliser les institutions sur l'importance de la migration vers certaines technologies et le respect des normes.

La prise en compte des risques dans le secteur bancaire se cantonne souvent à ceux liés au milieu. Les risques pouvant émaner des autres actifs, des autres ressources de la banque font l'objet d'une intégration souvent minime ou même d'aucune action. L'importance de la gestion de l'information change peu à peu cette donne, en plus des directives de la BCEAO, de l'UEMOA et de la volonté des institutions étrangères de tirer leurs partenaires du Sud vers le haut.

La gouvernance de la banque doit parvenir à une prise en compte globale de toutes les facettes de l'institution. Pour ce faire, il est opportun que les dirigeants en aient l'ambition, qu'ils la fassent percevoir dans la culture et leur stratégie et dans l'exercice quotidien des activités. Le réseau informatique étant prépondérant dans la gestion de la banque, il doit y être porté un œil attentif et analytique. Toutefois, il serait opportun de prendre en considération toute la gestion du système d'information, grande cuvette englobant le réseau. Certains « best practices » tel que le COBIT peuvent être implantés et les évaluations faites en fonction de méthodes telle que MEHARI, méthode très méticuleuse. L'on peut alors se pencher sur la manière d'implanter la première citée, et le reengineering à effectuer pour judicieusement appliquer la méthode énoncée.

ANNEXES

Résultats du questionnaire d'évaluation du réseau local

Référence	Questions	R-V1
Questionnaire d'audit : Réseau Local (LAN)		**1**
Le réseau local est vu, ici, comme le réseau reliant les différents serveurs et postes utilisateurs du site. Les connexions de postes nomades sont supposées assurées sur ce réseau.		
05A	**Sécurité de l'architecture du réseau local**	
05A01	***Partitionnement du réseau local en domaines de sécurité***	
05A01-01	A-t-on effectué un partitionnement du réseau local en séparant du réseau strictement interne les zones de communication avec l'extérieur (DMZ) ? *Une DMZ, ou zone démilitarisée, est une zone d'échange avec l'extérieur isolée du réseau interne par un pare-feu.*	0
05A01-02	A-t-on effectué un partitionnement du réseau local en domaines de sécurité correspondant à des exigences de sécurité homogènes et à des espaces de confiance à l'intérieur desquels les contrôles peuvent être adaptés ?	0
05A01-03	En particulier tout réseau sans fil (Wlan) est-il considéré comme un domaine distinct strictement isolé du reste du réseau (par firewall, routeur filtrant, etc.) ?	X
05A01-04	Ces partitionnements sont-ils documentés et tenus à jour ?	0
05A01-05	Existe-t-il une cartographie des liaisons et des équipements de communication en place ?	0
05A01-06	Chaque domaine est-il isolé des autres domaines par des mesures spécifiques de sécurité (routeur filtrant, firewall, portail, etc.) ?	1
05A01-07	La sécurité propre de ces équipements de filtrage fait-elle l'objet d'un suivi permanent par un expert et d'une veille technologique ?	1
05A01-08	A-t-on, pour chacun des domaines, défini une liste strictement limitée des liaisons et des protocoles autorisés pour communiquer de manière standard d'un domaine à un autre, et a-t-on, par défaut, fermé tous les autres protocoles (politique "rien sauf") ?	0
05A01-09	Existe-t-il une procédure de gestion des demandes d'ouvertures de connexions inter domaines, et une structure en charge d'analyser ces demandes, d'accorder des autorisations et de définir les règles de filtrage (filtrage sur les adresses, les services demandés, les protocoles, etc.) ?	X
05A01-10	Existe-t-il une structure en charge de la vérification de l'application des règles définies et de la suppression des droits spécifiques quand le besoin a disparu ou quand les conditions ne sont plus remplies ?	1
05A01-11	Toute adjonction à la liste des connexions autorisées d'un domaine et toute modification de l'un de ses paramètres sont-elles journalisées et auditées ?	1
05A01-12	Procède-t-on régulièrement à une revue des connexions autorisées (standards et non standards) et de leur pertinence ?	1
05A02	***Sûreté de fonctionnement des éléments d'architecture du réseau local***	
05A02-01	A-t-on analysé chaque domaine de sécurité pour déterminer les exigences de continuité de service et en a-t-on déduit, si nécessaire, une architecture de redondance au niveau des	0

points d'interconnexion, des équipements et du maillage du réseau ?

05A02-02	A-t-on fait une recherche systématique des Points Singuliers de Vulnérabilité ("Single Point of Failure") afin de s'assurer que des équipements, en particulier de servitude, (alimentation en énergie, climatisation, etc.) n'en introduisent pas ou ne détruisent pas les redondances prévues au niveau des équipements ou de l'architecture ?	0
05A02-03	A-t-on vérifié, par une analyse de la charge moyenne et crête de chaque segment de réseau, la compatibilité du réseau et de ses équipements avec cette charge et cette vérification est-elle régulièrement réactualisée ?	1
05A02-04	Cette analyse a-t-elle été complétée par une étude des capacités du réseau à assurer les communications dans tous les cas de pannes simples de liaisons ou d'équipements ?	0
05A02-05	Existe-t-il une mesure dynamique de la charge réseau et des outils d'équilibrage (load balancing) ?	X
05A02-06	Les outils de monitoring et de reconfiguration du réseau permettent-ils une action en temps réel compatible avec les besoins des utilisateurs ?	1
05A02-07	L'architecture des équipements de réseau permet-elle une adaptation facile aux évolutions de charge (clusters, grappes, etc.) ?	1
05A02-08	Les équipements et appareils (sondes) assurant la détection de surcharge et le rééquilibrage du réseau ne sont-ils accessibles que par les administrateurs réseau et sont-ils protégés par un contrôle d'accès renforcé ?	1
05A02-09	Toute inhibition ou mise à l'arrêt des équipements et appareils (sondes) assurant la détection de surcharge et le rééquilibrage du réseau est-elle signalée à un poste de surveillance et ou aux administrateurs réseau ?	1
05A02-10	Procède-t-on régulièrement à des tests de performance des mécanismes de détection et de reconfiguration ?	1
05A02-11	Procède-t-on régulièrement à un audit du paramétrage des systèmes de détection et de reconfiguration ?	0
05A02-12	Procède-t-on régulièrement à un audit des procédures associées aux systèmes de détection et de reconfiguration ?	0
05A03	***Organisation de la maintenance des équipements du réseau local***	
05A03-01	Tous les équipements du réseau local sont-ils couverts par un contrat de maintenance ?	0
05A03-02	A-t-on identifié les équipements critiques pour l'exploitation et la tenue des performances annoncées et, pour ceux-ci, les délais de remise en service souhaitable et les délais maximum tolérables en cas de défaillance ?	0
05A03-03	En a-t-on déduit des clauses particulières et adaptées à ces exigences dans les contrats de maintenance ?	0
05A03-04	Les pénalités en cas de non tenue des engagements par le titulaire du contrat de maintenance sont-elles réellement dissuasives ?	0
05A03-05	Les procédures d'escalade en cas de difficulté de maintenance sont-elles précisées et prévoient-elles l'intervention de spécialistes dans des délais courts compatibles avec la criticité des équipements ?	0

05A03-06	Le nombre et la proximité des spécialistes sont-ils précisés et donnent-ils une bonne garantie de maintenance dans des délais acceptables ?	0
05A03-07	Les contrats de maintenance prévoient-ils le remplacement complet des équipements en cas d'endommagement important non susceptible d'être pris en charge par une maintenance curative ?	0
05A03-08	Les contrats de maintenance et les procédures de maintenance associées font-ils l'objet d'un audit régulier ?	0
05A04	***Procédures et plans de reprise du réseau local sur incidents***	
05A04-01	A-t-on établi une liste des incidents pouvant affecter le bon fonctionnement du réseau local et analysé la criticité de chacun d'eux ?	0
05A04-02	A-t-on établi, pour chaque incident critique, la solution à mettre en oeuvre et les opérations à mener par le personnel d'exploitation ?	0
05A04-03	Les moyens d'intervention sur le réseau local (tant de diagnostic que de reconfiguration) couvrent-ils de manière satisfaisante tous les cas de figures analysés et permettent-ils de mettre en œuvre les solutions décidées dans les délais spécifiés ?	0
05A04-04	A-t-on défini, pour chaque incident critique du réseau local, un délai de résolution et une procédure d'escalade en cas d'insuccès ou de retard des mesures prévues ?	1
05A04-05	Les moyens de diagnostic et de pilotage et de reconfiguration du réseau sont-ils protégés contre toute inhibition intempestive ou malveillante ?	1
05A04-06	Les procédures de reprise sur incident tiennent-elles compte d'une éventuelle perte de données (en particulier perte de messages) ?	1
05A04-07	Audite-t-on régulièrement la capacité des moyens de diagnostic et de reconfiguration à assurer un fonctionnement minimal du réseau satisfaisant en cas d'incident ?	0
05A05	***Plan de sauvegarde des configurations du réseau local***	
05A05-01	A-t-on établi un plan de sauvegarde, couvrant l'ensemble des configurations du réseau local, définissant les objets à sauvegarder et la fréquence des sauvegardes ?	1
05A05-02	Ce plan de sauvegarde est-il traduit en automatismes de production ?	0
05A05-03	Teste-t-on régulièrement que les sauvegardes des programmes (sources et/ou exécutables), de leur documentation et de leur paramétrage permettent effectivement de reconstituer à tout moment l'environnement de production ?	0
05A05-04	Les automatismes de production assurant les sauvegardes sont-ils protégés par des mécanismes de haute sécurité contre toute modification illicite ou indue ? *Un tel mécanisme pourrait être un scellement électronique ou tout système de détection de modification équivalent.*	0
05A05-05	L'ensemble des sauvegardes et fichiers de configuration permettant de reconstituer l'environnement de production est-il également sauvegardé en dehors du site de production (sauvegardes de recours) ?	0
05A05-06	Ces copies de sauvegarde de recours sont-elles conservées dans un local sécurisé et protégé des risques accidentels et d'intrusion ? *Un tel local devrait être protégé par un contrôle d'accès renforcé et, en outre, être proté-*	0

gé contre les risques d'incendie et de dégâts des eaux.

05A05-07	Procède-t-on régulièrement à des tests de relecture des sauvegardes et sauvegardes de recours ?	0
05A05-08	L'ensemble des procédures et plans de sauvegarde des fichiers de configuration fait-il l'objet d'un audit régulier ?	0
05A06	***Plan de Reprise d'Activité (PRA) du réseau local***	
05A06-01	Existe-t-il une solution de secours-pour pallier l'indisponibilité de tout équipement ou de toute liaison critique ?	1
05A06-02	Cette solution de secours est-elle parfaitement opérationnelle ?	1
05A06-03	Ces solutions sont-elles décrites en détail dans un (ou plusieurs) Plan de Reprise d'Activité formel et complet ? *Un plan de reprise d'activité complet doit comprendre les règles de déclenchement, les actions à mener, les priorités, les acteurs à mobiliser et leurs coordonnées, ainsi que les conditions de retour à la normale.*	0
05A06-04	Ces plans sont-ils testés de manière opérationnelle au moins une fois par an ?	0
05A06-05	A-t-on la garantie formelle de la compatibilité et de la capacité des solutions de secours à assurer une charge opérationnelle suffisante et approuvée par les utilisateurs ?	0
05A06-06	Si les solutions de secours incluent des livraisons de matériels, qui ne peuvent être déclenchés lors des tests, existe-t-il un contrat d'engagement de livraison des matériels de remplacement dans des délais fixés et prévus au plan de secours, par le constructeur ou un tiers (leaser, broker, autres) ?	1
05A06-07	En cas de mutualisation des moyens de secours utilisés, y a-t-il un nombre d'adhérents limité et connu ?	0
05A06-08	Le cas de défaillance ou d'indisponibilité du moyen de secours a-t-il été envisagé et y a-t-il un back-up de deuxième niveau ?	1
05A06-09	La solution de secours est-elle utilisable pour une durée illimitée ou, à défaut, est-il prévu une deuxième solution venant en remplacement de la première après un temps déterminé ?	1
05A06-10	L'existence, la pertinence et la mise à jour des plans de reprise d'activité font-elles l'objet d'un audit régulier ?	0
05A07	***Gestion des fournisseurs critiques vis-à-vis de la permanence de la maintenance***	
05A07-01	A-t-on analysé les conséquences de la disparition d'un fournisseur d'équipement, de solution logicielle ou de service réseau (en cas de panne, de bug ou de nécessité d'évolution) et en a-t-on déduit une liste de points critiques ?	0
05A07-02	Existe-t-il, pour tout point critique, une solution palliative pour faire face à la disparition ou la défaillance du fournisseur (dépôt de la documentation de maintenance chez un tiers de confiance, remplacement de l'équipement, du logiciel ou du service par des solutions du marché, etc.) ?	0

05A07-03	A-t-on l'assurance que cette solution palliative pourra être rendue opérationnelle dans des délais compatibles avec la poursuite de l'activité et acceptés par les utilisateurs ?	0
05A07-04	A-t-on prévu des variantes de la solution de base au cas où celle-ci rencontrerait des difficultés imprévues ?	0
05A07-05	Procède-t-on régulièrement à une revue des points pouvant être critiques et des solutions palliatives prévues ?	0
05B	**Contrôle d'accès au réseau local de "données"**	
05B01	***Gestion des profils d'accès au réseau local de données***	
05B01-01	A-t-on établi une politique de gestion des droits d'accès au réseau local s'appuyant sur une analyse préalable des exigences de sécurité, basées sur les enjeux de l'activité ?	1
05B01-02	Cette politique est-elle documentée, revue régulièrement et approuvée par les responsables concernés ?	0
05B01-03	Les droits d'accès au réseau local et aux diverses parties de ce réseau sont-ils définis par rapport à des "profils" métiers regroupant des "rôles" ou des "fonctions" dans l'organisation (un profil définissant les droits dont disposent les titulaires de ce profil) ? *Nota : La notion de profil peut, dans certaines circonstances, être remplacée par une notion de "groupe". Par ailleurs les droits attribués éventuellement à des partenaires doivent être pris en compte.* *Les profils d'accès doivent comprendre les profils d'accès à chaque partitionnement du réseau, depuis un poste connecté directement sur le réseau et depuis les diverses possibilités prévues de connexion depuis l'extérieur du réseau (postes nomades, télétravail, partenaires, etc.).*	1
05B01-04	A-t-on introduit, dans les règles de définition des droits d'accès (qui déterminent les droits attribués à un profil), des paramètres variables en fonction du contexte, en particulier la localisation du poste du demandeur (réseau interne, étendu, externe), la nature de la connexion utilisée (LAN, LS, Internet, type de protocoles, etc.) ou la classification du sous-réseau demandé ?	0
05B01-05	Les profils d'accès permettent-ils également de définir des créneaux horaires et des calendriers de travail (heures début et fin de journée, week-end, vacances, etc.) ?	1
05B01-06	Ces profils et l'attribution de droits d'accès aux différents profils, en fonction du contexte, ont-ils reçu l'approbation des propriétaires d'information et du RSSI ?	1
05B01-07	Les processus de définition et de gestion des droits attribués aux profils sont-ils sous contrôle strict ? *Un contrôle strict requiert que la liste des personnes habilitées à changer les droits attribués aux profils d'accès soit très limitée, que la matérialisation de ces droits sous forme de tables soit strictement sécurisée lors de leur transmission et de leur stockage et qu'il existe un contrôle d'accès renforcé pour pouvoir les modifier, et que les modifications soient journalisées et auditées.*	1
05B01-08	Y a-t-il un audit régulier, au moins une fois par an, de l'ensemble des droits attribués à chaque profil d'accès et des procédures de gestion des profils ?	0

05B02 ***Gestion des autorisations d'accès et privilèges (attribution, délégation, retrait)***

05B02-01 La procédure d'attribution d'autorisations d'accès au réseau local nécessite-t-elle l'accord formel de la hiérarchie (à un niveau suffisant) ou de l'organisme gestionnaire de la prestation en cas de droits attribués à des partenaires ? 1

05B02-02 Les autorisations sont-elles attribuées à chaque utilisateur uniquement en fonction de son (ou ses) profil ? 1

05B02-03 Le processus d'attribution (ou modification ou retrait) effectif d'autorisations d'accès au réseau local à un individu (directement ou par le biais de profils) est-il strictement contrôlé ? 1

Un contrôle strict requiert une identification formelle du demandeur (reconnaissance de sa signature, signature électronique, etc.), que la matérialisation des profils attribués aux utilisateurs sous forme de tables soit strictement sécurisée lors de leur transmission et de leur stockage et qu'il existe un contrôle d'accès renforcé pour pouvoir les modifier, et que ces modifications soient journalisées et auditées.

05B02-04 Y a-t-il un processus de mise à jour systématique de la table des autorisations d'accès au réseau local lors de départs de personnel interne ? 1

05B02-05 Y a-t-il un processus de mise à jour systématique de la table des autorisations d'accès au réseau local lors de changements de fonctions (fin de mission ou de mandat de personnel externe ou mutation interne) ? 1

05B02-06 Y a-t-il une liste indiquant l'ensemble des personnes ayant des autorisations d'accès au réseau local ? 1

05B02-07 Y a-t-il un audit régulier, au moins une fois par an, de l'ensemble des autorisations d'accès au réseau local attribuées au personnel ou à des partenaires ? 0

05B03 ***Authentification de l'utilisateur ou de l'entité demandant un accès au réseau local depuis un point d'accès interne***

Ce mécanisme correspond à l'authentification réalisée sous Windows par un contrôleur de domaine.

05B03-01 Y a-t-il un mécanisme d'authentification de chaque utilisateur avant tout accès à une ressource du réseau local ? 1

05B03-02 Le processus de définition ou de modification de l'authentifiant supportant le contrôle d'accès pour les accès internes vérifie-t-il le respect d'un ensemble de règles permettant d'avoir confiance dans sa solidité intrinsèque ? 0

Dans le cas de mots de passe : longueur suffisante (8 caractères ou +), mélange obligatoire de types de caractères, changement fréquent (<1 mois), impossibilité de réemployer un mot de passe ancien, test de non trivialité fait en relation avec un dictionnaire, interdiction des "standards systèmes", des prénoms, de l'anagramme de l'identifiant, de dates, etc.

Dans le cas de certificats ou d'authentification reposant sur des mécanismes cryptologiques, processus de génération évalué ou reconnu publiquement, clés de chiffrement de longueur suffisante, etc.

05B03-03 Le processus de présentation par l'utilisateur de son authentifiant garantit-il son inviolabilité ? 0

La frappe d'un mot de passe sera toujours un point faible notable. Les seuls processus qui soient observables sans divulguer d'information consistent soit à introduire un objet contenant un secret (carte à puce), soit à frapper un code qui change à chaque instant (jeton d'authentification), soit à présenter un caractère biométrique.

05B03-04 La conservation et l'utilisation par les équipements de sécurité d'éléments de référence supportant l'authentification (mots de passe, numéro d'appelant, etc.) font-elles appel à des mécanismes qui en garantissent l'inviolabilité et l'authenticité ? X

Dans le cas de mots de passe, ils doivent être stockés chiffrés et un contrôle d'accès préliminaire à l'utilisation de ces éléments par l'utilisateur doit être effectué. Dans le cas d'authentification faisant appel à des procédés cryptologiques, le mécanisme doit présenter des garanties de solidité validées par un organisme de référence.

05B03-05 La transmission entre le poste appelant et les équipements de sécurité d'éléments de référence supportant l'authentification (mots de passe, numéro d'appelant, etc.) fait-elle appel à des mécanismes qui en garantissent l'inviolabilité et l'authenticité ? X

La transmission d'un mot de passe doit être chiffrée ou utiliser un algorithme qui introduise un aléa à chaque transmission.
Dans le cas d'authentification faisant appel à des procédés cryptologiques, le mécanisme doit présenter des garanties de solidité validées par un organisme de référence.

05B03-06 A-t-on mis en place une dévalidation automatique de l'utilisateur appelant, en cas de tentatives multiples infructueuses, avec nécessité d'intervention de l'administrateur pour revalider le poste ou l'utilisateur ? X

05B03-07 La procédure permettant de redonner un authentifiant à un utilisateur qui a perdu le sien (mot de passe, jeton d'authentification, etc.) permet-elle de neutraliser instantanément l'ancien authentifiant ? 1

05B03-08 La procédure permettant de redonner un authentifiant à un utilisateur qui a perdu le sien (mot de passe, jeton d'authentification, etc.) permet-elle un contrôle effectif de l'identité du demandeur ? 1

05B03-09 Les paramètres de l'authentification sont-ils sous contrôle strict ? 1

Un contrôle strict requiert que la liste des personnes habilitées à changer les règles de définition des authentifiants, les authentifiants eux-mêmes, les règles de surveillance des tentatives de connexion, etc. soit très limitée, qu'il existe un contrôle d'accès renforcé pour procéder à ces modifications, que les modifications soient journalisées et auditées et qu'il existe un audit général au moins annuel de l'ensemble des paramètres de l'authentification.

05B03-10 Les processus qui assurent l'authentification sont-ils sous contrôle strict ? 1

Un contrôle strict requiert que le logiciel correspondant ait été validé et subisse régulièrement un test d'intégrité (sceau) et qu'il existe un audit au moins annuel des procédures et processus de l'authentification.

05B04	***Authentification de l'utilisateur ou de l'entité demandant un accès au réseau local depuis un site distant via le réseau étendu***	X
05B04-01	Les règles d'appartenance au réseau étendu exigent-elles l'authentification de chaque utilisateur avant tout accès sortant empruntant le réseau étendu ?	
05B04-02	Les règles d'appartenance au réseau étendu et les contrôles effectués permettent-ils d'accorder la même confiance aux utilisateurs du réseau étendu qu'aux utilisateurs locaux ?	
05B04-03	La pertinence des règles d'appartenance au réseau étendu est-elle régulièrement auditée ?	
05B04-04	L'application des règles d'appartenance au réseau étendu par l'ensemble des entités autorisées à se connecter au réseau étendu est-elle régulièrement auditée ?	
05B05	***Authentification de l'utilisateur ou de l'entité demandant un accès au réseau local depuis l'extérieur*** *(depuis le Réseau Téléphonique Commuté, X25, RNIS, ADSL, Internet, etc.)*	
05B05-01	Y a-t-il un mécanisme d'authentification de chaque utilisateur pour toute connexion au réseau local depuis l'extérieur ?	0
05B05-02	Le processus de définition ou de modification de l'authentifiant supportant le contrôle d'accès pour les accès externes vérifie-t-il le respect d'un ensemble de règles permettant d'avoir confiance dans sa solidité intrinsèque ? *Dans le cas de mots de passe : longueur suffisante (8 caractères ou +), mélange obligatoire de types de caractères, changement fréquent (<1 mois), impossibilité de réemployer un mot de passe ancien, test de non trivialité fait en relation avec un dictionnaire, interdiction des "standards systèmes", des prénoms, de l'anagramme de l'identifiant, de dates, etc.* *Dans le cas d'authentifiants fixes (numéro de l'appelant), procédure de call-back.* *Dans le cas de certificats ou d'authentification reposant sur des mécanismes cryptologiques, processus de génération évalué ou reconnu publiquement, clés de chiffrement de longueur suffisante, etc.*	0
05B05-03	Le processus de présentation par l'utilisateur de son authentifiant garantit-il son inviolabilité ? *La frappe d'un mot de passe sera toujours un point faible notable. Les seuls processus qui soient observables sans divulguer d'information consistent soit à introduire un objet contenant un secret (carte à puce) soit à frapper un code qui change à chaque instant (jeton d'authentification), soit à présenter un caractère biométrique.*	0
05B05-04	La conservation et l'utilisation par les équipements de sécurité d'éléments de référence supportant l'authentification (mots de passe, numéro d'appelant, etc.) font-elles appel à des mécanismes qui en garantissent l'inviolabilité et l'authenticité ? *Dans le cas de mots de passe, ils doivent être stockés chiffrés et un contrôle d'accès préliminaire à l'utilisation de ces éléments par l'utilisateur doit être effectué.* *Dans le cas d'authentification faisant appel à des procédés cryptologiques, le mécanisme doit présenter des garanties de solidité validées par un organisme de référence.*	X

05B05-05	La transmission entre le poste appelant et les équipements de sécurité d'éléments de référence supportant l'authentification (mots de passe, numéro d'appelant, etc.) fait-elle appel à des mécanismes qui en garantissent l'inviolabilité et l'authenticité ? *La transmission d'un mot de passe doit être chiffrée ou utiliser un algorithme qui introduise un aléa à chaque transmission.* *Dans le cas d'authentification faisant appel à des procédés cryptologiques, le mécanisme doit présenter des garanties de solidité validées par un organisme de référence.*	X
05B05-06	A-t-on mis en place une dévalidation automatique du poste ou de l'utilisateur appelant, en cas de tentatives multiples infructueuses, avec nécessité d'intervention de l'administrateur pour revalider le poste ou l'utilisateur ?	X
05B05-07	La procédure permettant de redonner un authentifiant à un utilisateur qui a perdu le sien (mot de passe, jeton d'authentification, etc.) permet-elle de neutraliser instantanément l'ancien authentifiant ?	I
05B05-08	La procédure permettant de redonner un authentifiant à un utilisateur qui a perdu le sien (mot de passe, jeton d'authentification, etc.) permet-elle un contrôle effectif de l'identité du demandeur ?	I
05B05-09	Les paramètres de l'authentification sont-ils sous contrôle strict ? *Un contrôle strict requiert que la liste des personnes habilitées à changer les règles de définition des authentifiants, les authentifiants eux-mêmes, les règles de surveillance des tentatives de connexion, etc. soit très limitée, qu'il existe un contrôle d'accès renforcé pour procéder à ces modifications, que les modifications soient journalisées et auditées et qu'il existe un audit général au moins annuel de l'ensemble des paramètres de l'authentification.*	I
05B05-10	Les processus qui assurent l'authentification sont-ils sous contrôle strict ? *Un contrôle strict requiert que le logiciel correspondant ait été validé et subisse régulièrement un test d'intégrité (sceau) et qu'il existe un audit au moins annuel des procédures et processus de l'authentification.*	I
05B06	***Authentification de l'utilisateur ou de l'entité demandant un accès au réseau local depuis un sous-réseau WiFi***	X
05B06-01	Tout sous-réseau WiFi est-il isolé du réseau local par un pare-feu ?	
05B06-02	Y a-t-il un mécanisme d'authentification de chaque utilisateur pour toute connexion au réseau local depuis un sous-réseau WiFi ?	
05B06-03	Le processus de définition ou de modification de l'authentifiant supportant le contrôle d'accès pour les accès depuis un sous-réseau WiFi vérifie-t-il le respect d'un ensemble de règles permettant d'avoir confiance dans sa solidité intrinsèque ? *Dans le cas de mots de passe : longueur suffisante (8 caractères ou +), mélange obligatoire de types de caractères, changement fréquent (<1 mois), impossibilité de réemployer un mot de passe ancien, test de non trivialité fait en relation avec un dictionnaire, interdiction des "standards systèmes", des prénoms, de l'anagramme de l'identifiant, de dates, etc.*	

Dans le cas d'authentifiants fixes (numéro de l'appelant), procédure de call-back. Dans le cas de certificats ou d'authentification reposant sur des mécanismes cryptologiques, processus de génération évalué ou reconnu publiquement, clés de chiffrement de longueur suffisante, etc.

05B06-04 Le processus de présentation par l'utilisateur de son authentifiant garantit-il son inviolabilité ?
La frappe d'un mot de passe sera toujours un point faible notable. Les seuls processus qui soient observables sans divulguer d'information consistent soit à introduire un objet contenant un secret (carte à puce) soit à frapper un code qui change à chaque instant (jeton d'authentification), soit à présenter un caractère biométrique.

05B06-05 La conservation et l'utilisation par les équipements de sécurité d'éléments de référence supportant l'authentification (mots de passe, numéro d'appelant, etc.) font-elles appel à des mécanismes qui en garantissent l'inviolabilité et l'authenticité ?
Dans le cas de mots de passe, ils doivent être stockés chiffrés et un contrôle d'accès préliminaire à l'utilisation de ces éléments par l'utilisateur doit être effectué. Dans le cas d'authentification faisant appel à des procédés cryptologiques, le mécanisme doit présenter des garanties de solidité validées par un organisme de référence.

05B06-06 La transmission entre le poste appelant et les équipements de sécurité d'éléments de référence supportant l'authentification (mots de passe, numéro d'appelant, etc.) fait-elle appel à des mécanismes qui en garantissent l'inviolabilité et l'authenticité ?
La transmission d'un mot de passe doit être chiffrée ou utiliser un algorithme qui introduise un aléa à chaque transmission.
Dans le cas d'authentification faisant appel à des procédés cryptologiques, le mécanisme doit présenter des garanties de solidité validées par un organisme de référence.

05B06-07 A-t-on mis en place une dévalidation automatique du poste ou de l'utilisateur appelant, en cas de tentatives multiples infructueuses, avec nécessité d'intervention de l'administrateur pour revalider le poste ou l'utilisateur ?

05B06-08 La procédure permettant de redonner un authentifiant à un utilisateur qui a perdu le sien (mot de passe, jeton d'authentification, etc.) permet-elle de neutraliser instantanément l'ancien authentifiant ?

05B06-09 La procédure permettant de redonner un authentifiant à un utilisateur qui a perdu le sien (mot de passe, jeton d'authentification, etc.) permet-elle un contrôle effectif de l'identité du demandeur ?

05B06-10 Les paramètres de l'authentification pour les accès depuis un sous-réseau WiFi sont-ils sous contrôle strict ?
Un contrôle strict requiert que la liste des personnes habilitées à changer les règles de définition des authentifiants, les authentifiants eux-mêmes, les règles de surveillance des tentatives de connexion, etc. soit très limitée, qu'il existe un contrôle d'accès renforcé pour procéder à ces modifications, que les modifications soient journalisées et auditées

et qu'il existe un audit général au moins annuel de l'ensemble des paramètres de l'authentification.

05B06-11	Les processus qui assurent l'authentification pour les accès depuis un sous-réseau WiFi sont-ils sous contrôle strict ? *Un contrôle strict requiert que le logiciel correspondant ait été validé et subisse régulièrement un test d'intégrité (sceau) et qu'il existe un audit au moins annuel des procédures et processus de l'authentification.*	
05B07	***Filtrage général des accès au réseau local***	
05B07-01	Tout accès au réseau local requiert-il la présentation d'un identifiant reconnu par le système ?	1
05B07-02	Tout identifiant reconnu par le système correspond-il à une personne physique unique et identifiable, directement ou indirectement ?	1
05B07-03	Tous les comptes génériques ou par défaut ont-ils été supprimés ?	0
05B07-04	L'acceptation de l'identifiant par le contrôle d'accès au réseau local est-elle systématiquement sujette à une authentification ? *L'authentification systématique requiert que ce processus soit effectivement mis en oeuvre pour l'ensemble des voies et ports d'accès (accès interne, tous types d'accès depuis l'extérieur, y compris les ports réservés tels que la télémaintenance éventuelle).*	1
05B07-05	Y a-t-il un contrôle systématique du contexte du demandeur d'accès (réseau local, réseau étendu, liaison externe, nature de la liaison utilisée et protocoles) ?	X
05B07-06	Y a-t-il un contrôle systématique du profil du demandeur d'accès, de son contexte et de l'adéquation de ce profil et du contexte avec l'accès demandé ?	X
05B07-07	Y a-t-il une dévalidation automatique de l'identifiant de l'utilisateur, en cas d'absence de trafic après un délai défini, nécessitant une nouvelle identification - authentification ?	0
05B07-08	Pour les connexions qui l'exigent, y a-t-il une identification de l'équipement appelant (adresse MAC, adresse IP, etc.) en association avec des règles de contrôle d'accès ?	X
05B07-09	Les processus de définition et de gestion des règles de filtrage des accès sont-ils sous contrôle strict ? *Un contrôle strict requiert que la liste des personnes habilitées à changer les paramètres de sécurité du filtrage des accès soit très limitée, qu'il existe un contrôle d'accès renforcé pour pouvoir les modifier, et que les modifications soient journalisées et auditées.*	1
05B07-10	Procède-t-on à des tests périodiques de pénétration du réseau et à des audits techniques spécialisés approfondis ?	0
05B08	***Contrôle du routage des accès sortants***	X
05B08-01	Tout accès sortant requiert-il la présentation d'un identifiant reconnu par le système ?	
05B08-02	Cet identifiant correspond-il à une personne physique unique et identifiable, directement ou indirectement ?	
05B08-03	L'acceptation de l'identifiant par le contrôle d'accès sortant est-elle systématiquement sujette à une authentification ?	

L'authentification systématique requiert que ce processus soit effectivement mis en oeuvre pour l'ensemble des voies et ports d'accès sortants.

05B08-04 A-t-on défini, dans une politique de sécurité relative aux accès sortants, des règles définissant les types d'accès sortants autorisés (type de réseau externe, nature de la liaison utilisée et protocoles) en fonction des types de sous-réseaux internes ?

05B08-05 Y a-t-il, avant tout accès sortant, un contrôle des règles définies dans la politique de sécurité ?

05B08-06 Y a-t-il une dévalidation automatique de l'identifiant de l'utilisateur, en cas d'absence de trafic après un délai défini, nécessitant une nouvelle identification - authentification ?

05B08-07 Les processus de définition et de gestion des règles de filtrage des accès sortants sont-ils sous contrôle strict ?

Un contrôle strict requiert que la liste des personnes habilitées à changer les paramètres de sécurité du filtrage des accès soit très limitée, qu'il existe un contrôle d'accès renforcé pour pouvoir les modifier, et que les modifications soient journalisées et auditées.

05B08-08 Procède-t-on à des tests périodiques de violation des règles de contrôle des accès sortants et à des audits techniques spécialisés approfondis ?

05B09 Authentification de l'entité accédée lors des accès sortants vers des sites sensibles X

05B09-01 Existe-t-il une possibilité de déclarer des sites ou des accès distants comme sensibles et, comme tels, requérant une authentification de l'entité accédée ?

05B09-02 Y a-t-il un mécanisme d'authentification de l'entité appelée avant tout accès sortant vers des sites sensibles depuis le réseau interne ?

05B09-03 Le processus d'authentification des entités sensibles accédées est-il un processus reconnu comme "fort" ?

Un simple mot de passe sera toujours un point faible notable. Les seuls processus qui soient reconnus comme forts, c'est-à-dire observables sans divulguer d'information et pratiquement inviolables sont basés sur des algorithmes cryptologiques.

05B09-04 La conservation et l'utilisation par les équipements de sécurité d'éléments de référence supportant l'authentification (mots de passe, numéro d'appelant, etc.) font-elles appel à des mécanismes qui en garantissent l'inviolabilité et l'authenticité ?

Dans le cas de mots de passe, ils doivent être stockés chiffrés et un contrôle d'accès préliminaire à l'utilisation de ces éléments par l'utilisateur doit être effectué. Dans le cas d'authentification faisant appel à des procédés cryptologiques, le mécanisme doit présenter des garanties de solidité validées par un organisme de référence.

05B09-05 La transmission entre le poste appelant et les équipements de sécurité d'éléments de référence supports de l'authentification (mots de passe, numéro d'appelant, etc.) fait-elle appel à des mécanismes qui en garantissent l'inviolabilité et l'authenticité ?

La transmission d'un mot de passe doit être chiffrée ou utiliser un algorithme qui introduise un aléa à chaque transmission.

Dans le cas d'authentification faisant appel à des procédés cryptologiques, le mécanisme doit présenter des garanties de solidité validées par un organisme de référence.

05B09-06 Les procédures de gestion des clés révoquées garantissent-elles que les systèmes de contrôle testent systématiquement que les clés ne sont pas révoquées ?

05B09-07 Les procédures de gestion des clés révoquées garantissent-elles que les systèmes de contrôle prennent en compte ces révocations en temps réel ?

05B09-08 Les processus qui assurent l'authentification des entités accédées sont-ils sous contrôle strict ?

Un contrôle strict requiert que le logiciel correspondant ait été validé et subisse régulièrement un test d'intégrité (sceau) et qu'il existe un audit au moins annuel des procédures et processus de l'authentification.

05C Sécurité des données lors des échanges et des communications sur le réseau local x

05C01 Chiffrement des échanges sur le réseau local

Le chiffrement peut être effectué au niveau 3 (IPSEC, alors on parle de VPN) ou au niveau 4-5 (SSL, fonction de l'application utilisée) ou effectué directement par l'application (couche 6-7, par ex. chiffrement avant ou lors de l'envoi), cas vraiment traité par le domaine 09.

Il peut être systématique sur le "tuyau" (physique ou logique) ou limité à certains flux (en fonction des adresses ou du type, ou autre?), il peut être réalisé sur des systèmes intermédiaires (boîtiers VPN) ou finaux (postes, serveur) ou mixtes.

05C01-01 A-t-on défini les liens permanents et les échanges de données devant être protégés par des solutions de chiffrement et mis en place de telles solutions au niveau du réseau local ?

05C01-02 La solution de chiffrement offre-t-elle des garanties de solidité dignes de confiance et a-t-elle été approuvée par le RSSI ?

Une longueur de clés suffisante est un des paramètres à prendre en compte (en fonction de l'algorithme) mais bien d'autres paramètres également. La recommandation d'un organisme officiel peut être un facteur de confiance.

05C01-03 La procédure et les mécanismes de conservation, de distribution et d'échange de clés, et plus généralement de gestion des clés, offrent-ils des garanties de solidité dignes de confiance et ont-ils été approuvés par le RSSI ?

05C01-04 Les mécanismes de chiffrement sont-ils réalisés par des composants électroniques très solidement protégés, au niveau physique, contre toute violation ou altération ?

Il s'agit ici de boîtiers de chiffrement protégés physiquement de telle sorte qu'il soit impossible d'accéder aux mécanismes de chiffrement ou de carte à microprocesseur dont l'algorithme de chiffrement est contenu dans le microprocesseur et protégé physiquement et logiquement.

05C01-05 La mise hors service ou le by-pass de la solution de chiffrement sont-ils immédiatement détectés et signalés à une équipe permanente ou d'astreinte capable d'engendrer une réaction immédiate ?

05C01-06 En cas d'inhibition ou de by-pass de la solution de chiffrement ou de mise en oeuvre d'une solution de secours du réseau par une voie non protégée, existe-t-il une procédure

permettant d'en alerter immédiatement l'ensemble des utilisateurs ?

Par exemple par un avertissement lors de l'utilisation de ce réseau demandant la validation active de l'utilisateur.

05C01-07 Y a-t-il un audit régulier, au moins une fois par an, de l'ensemble des systèmes de chiffrement des données échangées et des procédures associées ?

05C02 Protection de l'intégrité des échanges sur le réseau local

05C02-01 A-t-on défini les liens permanents et les échanges de données devant être protégés par des solutions de scellement et mis en place de telles solutions au niveau du réseau local ?

05C02-02 La solution de scellement offre-t-elle des garanties de solidité dignes de confiance et a-t-elle été approuvée par le RSSI ?

Une longueur de clés suffisante est un des paramètres à prendre en compte, mais bien d'autres paramètres également. La recommandation d'un organisme officiel peut être un facteur de confiance.

05C02-03 La procédure et les mécanismes de conservation, de distribution et d'échange de clés, et plus généralement de gestion des clés, offrent-ils des garanties de solidité dignes de confiance et ont-ils été approuvés par le RSSI ?

05C02-04 Les mécanismes de scellement sont-ils réalisés par des composants électroniques très solidement protégés, au niveau physique, contre toute violation ou altération ?

Il s'agit ici de boîtiers de scellement protégés physiquement de telle sorte qu'il soit impossible d'accéder aux mécanismes de scellement ou de carte à microprocesseur dont l'algorithme de chiffrement est contenu dans le microprocesseur et protégé physiquement et logiquement.

05C02-05 La mise hors service ou le by-pass de la solution de scellement sont-ils immédiatement détectés et signalés à une équipe permanente ou d'astreinte capable d'engendrer une réaction immédiate ?

05C02-06 En cas d'inhibition ou de by-pass de la solution de scellement ou de mise en oeuvre d'une solution de secours du réseau par une voie non protégée, existe-t-il une procédure permettant d'en alerter immédiatement l'ensemble des utilisateurs ?

Par exemple par un avertissement lors de l'utilisation de ce réseau demandant la validation active de l'utilisateur.

05C02-07 Y a-t-il un audit régulier, au moins une fois par an, de l'ensemble des systèmes de scellement des données échangées et des procédures associées ?

05C03 Chiffrement des échanges lors des accès distants au réseau local x

05C03-01 A-t-on défini et mis en place des solutions de chiffrement pour les échanges avec des utilisateurs se connectant depuis l'extérieur (nomades, prestataires autorisés à se connecter au réseau, etc.) ?

05C03-02 La solution de chiffrement offre-t-elle des garanties de solidité dignes de confiance et a-t-elle été approuvée par le RSSI ?

Une longueur de clés suffisante est un des paramètres à prendre en compte (en fonction de l'algorithme) mais bien d'autres paramètres également. La recommandation d'un

organisme officiel peut être un facteur de confiance.

05C03-03	La procédure et les mécanismes de conservation, de distribution et d'échange de clés, et plus généralement de gestion des clés, offrent-ils des garanties de solidité dignes de confiance et ont-ils été approuvés par le RSSI ?	
05C03-04	Les mécanismes de chiffrement sont-ils réalisés par des composants électroniques très solidement protégés, au niveau physique, contre toute violation ou altération ? *Il s'agit ici de boîtiers de chiffrement protégés physiquement de telle sorte qu'il soit impossible d'accéder aux mécanismes de chiffrement ou de carte à microprocesseur dont l'algorithme de chiffrement est contenu dans le microprocesseur et protégé physiquement et logiquement.*	
05C03-05	La connexion au réseau depuis l'extérieur est-elle impossible en dehors du chiffrement ?	
05C04	***Protection de l'intégrité des échanges lors des accès distants au réseau local***	x
05C04-01	A-t-on défini et mis en place des solutions de scellement ou de contrôle d'intégrité pour les échanges avec des utilisateurs se connectant depuis l'extérieur (nomades, prestataires autorisés à se connecter au réseau, etc.) ?	
05C04-02	La solution de scellement offre-t-elle des garanties de solidité dignes de confiance et a-t-elle été approuvée par le RSSI ? *Une longueur de clés suffisante est un des paramètres à prendre en compte, mais bien d'autres paramètres également. La recommandation d'un organisme officiel peut être un facteur de confiance.*	
05C04-03	La procédure et les mécanismes de conservation, de distribution et d'échange de clés, et plus généralement de gestion des clés, offrent-ils des garanties de solidité dignes de confiance et ont-ils été approuvés par le RSSI ?	
05C04-04	Les mécanismes de scellement sont-ils réalisés par des composants électroniques très solidement protégés, au niveau physique, contre toute violation ou altération ? *Il s'agit ici de boîtiers de scellement protégés physiquement de telle sorte qu'il soit impossible d'accéder aux mécanismes de scellement ou de carte à microprocesseur dont l'algorithme de chiffrement est contenu dans le microprocesseur et protégé physiquement et logiquement.*	
05C04-05	La connexion au réseau depuis l'extérieur est-elle impossible en dehors du contrôle d'intégrité ?	
05D	**Contrôle, détection et traitement des incidents du réseau local**	
05D01	***Surveillance (en temps réel) du réseau local***	
05D01-01	A-t-on analysé les événements ou successions d'événements pouvant être révélateurs de comportements anormaux ou d'actions illicites et en a-t-on déduit des points ou indicateurs de surveillance ?	1
05D01-02	Le système dispose-t-il d'une fonction automatique de surveillance en temps réel en cas d'accumulation d'événements anormaux (par exemple tentatives infructueuses de connexion sur des ports non ouverts, etc.) ?	0

05D01-03	Emploie-t-on un système de détection d'intrusion et d'anomalies ?	0
05D01-04	Existe-t-il une (ou plusieurs) application capable d'analyser les divers diagnostics individuels d'anomalies et de déclencher une alerte à destination du personnel d'exploitation ?	0
05D01-05	Existe-t-il, parmi le personnel d'exploitation, une équipe permanente ou disponible sur appel (astreinte) capable de réagir en cas d'alerte de la surveillance réseau ?	1
05D01-06	A-t-on défini pour chaque cas d'alerte, la réaction attendue de l'équipe d'intervention et sa disponibilité est-elle suffisante pour faire face à cette attente ?	0
05D01-07	Les paramètres définissant les alarmes sont-ils strictement protégés (droits limités et authentification forte) contre tout changement illicite ?	0
05D01-08	Toute inhibition du système d'alerte déclenche-t-elle une alarme auprès de l'équipe de surveillance ?	0
05D01-09	Existe-t-il un archivage (sur disque, cassette, Disque Optique Numérique, etc.) de tous les éléments ayant permis de détecter une anomalie ou un incident ?	0
05D01-10	Les procédures de surveillance du réseau et de détection d'anomalies et la disponibilité de l'équipe de surveillance font-elles l'objet d'un audit régulier ?	0
05D02	***Analyse (en temps différé) des traces, logs et journaux d'événements sur le réseau local***	
05D02-01	A-t-on fait une analyse approfondie des événements ou succession d'événements pouvant avoir un impact sur la sécurité (connexions refusées, reroutages, reconfigurations, évolutions de performances, accès à des informations ou des outils sensibles, etc.) ?	0
05D02-02	Enregistre-t-on ces événements ainsi que tous les paramètres utiles à leur analyse ultérieure ?	0
05D02-03	Existe-t-il une application capable d'analyser ces enregistrements ainsi que les mesures de performances, d'en déduire des statistiques, un tableau de bord et des diagnostics d'anomalies examinés par une structure ad hoc ?	0
05D02-04	La structure chargée d'analyser ces éléments de synthèse (ou éventuellement les journaux des incidents, et événements liés à la sécurité) a-t-elle l'obligation de le faire à période fixe et déterminée et a-t-elle la disponibilité suffisante ?	0
05D02-05	A-t-on défini pour chaque cas d'alerte, la réaction attendue de l'équipe de surveillance et sa disponibilité est-elle suffisante pour faire face à cette attente ?	0
05D02-06	Les paramètres définissant les éléments à enregistrer et les synthèses effectuées sur ces éléments sont-ils strictement protégés (droits limités et authentification forte) contre tout changement illicite ?	0
05D02-07	Toute inhibition du système d'enregistrement et de traitement des enregistrements déclenche-t-elle une alarme auprès de l'équipe de surveillance ?	0
05D02-08	Les enregistrements ou les synthèses sont-ils protégés contre toute altération ou destruction ?	1
05D02-09	Les enregistrements ou les synthèses sont-ils conservés sur une longue durée ?	1
05D02-10	Les procédures d'enregistrement, de traitement des enregistrements et d'analyse des synthèses ainsi que la disponibilité de l'équipe d'analyse et d'intervention font-elles l'objet d'un audit régulier ?	0

05D03	***Traitement des incidents du réseau local***	
05D03-01	Y a-t-il une équipe (hot line) chargée de recueillir les appels et de signaler et d'enregistrer tous les incidents ?	1
05D03-02	Cette équipe (hot line) est-elle accessible en permanence ?	1
05D03-03	Y a-t-il un système support de la gestion des incidents ?	0
05D03-04	Ce système centralise-t-il et prend-il en compte aussi bien les incidents détectés par l'exploitation que ceux signalés par les utilisateurs ?	0
05D03-05	Ce système permet-il un suivi et une relance automatiques des actions nécessaires ?	0
05D03-06	Ce système incorpore-t-il une typologie des incidents avec élaboration de statistiques et de tableau de bord des incidents à destination du RSSI ?	0
05D03-07	Le système de gestion d'incidents est-il strictement contrôlé vis-à-vis de toute modification illicite ou indue ? *Un contrôle strict requiert une protection renforcée pour pouvoir modifier un enregistrement et un audit de toute modification des enregistrements ou un contrôle par scellement électronique de toute modification.*	0
05D03-08	Chaque incident réseau majeur fait-il l'objet d'un suivi spécifique (nature et description, priorité, solutions techniques, études en cours, délai prévu de résolution, etc.) ?	1

ANNEXE 1 : Questionnaire d'évaluation du réseau local

Résultats du Questionnaire d'évaluation de l'exploitation des réseaux

Questionnaire d'audit : Exploitation des réseaux		**1**
Référence	**Questions**	**R-V1**
06A	**Sécurité des procédures d'exploitation**	
06A01	***Prise en compte de la sécurité dans les relations avec le personnel d'exploitation (salariés et prestataires ou fournisseurs)***	
06A01-01	A-t-on rédigé, à l'usage des personnels d'exploitation des réseaux, une politique de sécurité spécifique couvrant tous les aspects de la sécurité des systèmes d'information (confidentialité des informations, disponibilité des informations et services, intégrité des informations et configurations, traçabilité, etc.) ?	0
06A01-02	Fait-on signer au personnel d'exploitation des réseaux employé par l'entreprise (quel que soit le statut, CDI, CDD, intérimaire, stagiaire, etc.) des clauses de respect de la politique de sécurité ?	1
06A01-03	Ces clauses précisent-elles que le devoir de respect de la politique de sécurité s'applique en général à toute information quel qu'en soit le support (papier, magnétique, optique, etc.) ?	1
06A01-04	Ces clauses précisent-elles, quand cela est nécessaire et juridiquement possible, que le devoir de respect de la politique de sécurité s'applique sans limitation de durée ? *En particulier, pour les clauses touchant à la confidentialité, les clauses de non divulgation peuvent (et souvent doivent) s'étendre au delà du contrat de travail ou du contrat liant l'entreprise à son sous-traitant ou partenaire.*	1
06A01-05	Ces clauses précisent-elles que le personnel a l'obligation de ne pas favoriser les actions qui pourraient être menées par d'autres personnes au détriment de la sécurité ?	1
06A01-06	La signature de ces clauses constitue-t-elle un engagement formel du signataire ? *Pour qu'il s'agisse d'un engagement formel, il est souhaitable que le signataire reconnaisse explicitement en avoir pris connaissance et les accepter.*	1
06A01-07	Les mêmes clauses sont-elles rendues obligatoires pour le personnel des entreprises intervenant dans l'exploitation des réseaux ? *En pratique, cela conduit à faire obligation auxdites entreprises de les faire signer individuellement, et dans les mêmes conditions, à son personnel.*	1
06A01-08	Le personnel d'exploitation suit-il systématiquement une formation à la sécurité adaptée à sa fonction ?	1
06A01-09	Les clauses de respect de la politique de sécurité signées par le personnel sont-elles conservées de manière sûre (au moins dans une armoire fermée à clé) ?	1
06A01-10	Les clauses de respect de la politique de sécurité signées par le personnel des entreprises contractées sont-elles conservées de manière sûre (au moins dans une armoire fermée à clé) ?	1
06A01-11	Y a-t-il un audit régulier, au moins une fois par an, de l'application effective des procédures de signature des clauses de confidentialité par le personnel d'exploitation (directement employé par l'entreprise ou par l'intermédiaire d'une société prestataire) ?	0
06A02	***Contrôle de la mise en production de nouveaux logiciels ou matériels ou d'évolutions de logiciels ou matériels***	
06A02-01	Les décisions de changements majeurs des équipements et systèmes font-elles l'objet de procédures de contrôle (enregistrement, planning, approbation formelle, communication à l'ensemble des personnes concernées, etc.) ?	1
06A02-02	Les décisions de changement s'appuient-elles sur des analyses de la capacité des nouveaux équipements et systèmes à assurer la charge requise en fonction des évolutions des demandes prévisibles ?	1

06A02-03	Les installations sont-elles faites avec un souci de protection physique (accès protégé, absence de vue directe externe sur les équipements, absence de menaces physiques diverses, conditions climatiques, protection contre la foudre, protection contre la poussière, etc.) ?	0
06A02-04	Une revue formelle des nouvelles fonctionnalités (ou des changements de fonctionnalités) liées à un changement majeur de logiciel ou d'équipement est-elle systématiquement réalisée, avec le concours de la fonction sécurité informatique ?	1
06A02-05	Cette revue comprend-elle une analyse des risques éventuels pouvant naître a cette occasion ?	0
06A02-06	L'exploitation a-t-elle reçu une formation spécifique à l'analyse des risques ?	0
06A02-07	L'exploitation peut-elle faire appel à un support adapté pour de telles analyses de risques ?	1
06A02-08	Les mesures de sécurité décidées pour remédier aux nouveaux risques mis en évidence font-elles l'objet de contrôles et de tests formels avant mise en exploitation ?	0
06A02-09	Les paramétrages de sécurité et règles de configuration (suppression de tout compte générique, changement de tout mot de passe générique, fermeture de tout port non explicitement demandé et autorisé, paramétrages du contrôle des droits et de l'authentification, contrôles des tables de routage, etc.) font-ils l'objet d'une liste précise tenue à jour ?	0
06A02-10	Les paramétrages de sécurité et règles de configuration sont-ils contrôlés avant toute mise en exploitation d'une nouvelle version ?	1
06A02-11	L'impact éventuel des changements de systèmes sur les plans de continuité est-il pris en compte ?	1
06A02-12	Les dérogations au processus d'analyse de risque préalable et aux contrôles des paramètres de sécurité font-elles l'objet de procédures strictes avec signature d'un responsable de niveau élevé ?	1
06A02-13	La mise en production de nouvelles versions d'équipements ou de logiciels n'est-elle possible que par le personnel d'exploitation ?	1
06A02-14	La mise en production de nouvelles versions d'équipements ou de logiciels n'est-elle possible que selon un processus de validation et d'autorisation défini ?	1
06A02-15	L'ensemble des procédures de contrôle de la mise en production fait-il l'objet d'un audit régulier ?	0
06A03	***Contrôle des opérations de maintenance***	
06A03-01	Conserve-t-on une trace de toute opération de maintenance ?	1
06A03-02	Toute opération de maintenance doit-elle être conclue par une vérification systématique des paramètres de sécurité (tels que définis lors de la mise en production) ?	1
06A03-03	Toute opération de maintenance doit-elle être conclue par une vérification systématique des paramètres d'enregistrement des événements de sécurité (événements à enregistrer, contextes des événements à enregistrer, durée de rétention, etc.) ?	1
06A03-04	Toute opération de maintenance doit-elle être conclue par une vérification systématique des paramètres de contrôle de l'administration des équipements (profil nécessaire, type d'authentification, suppression des login standards, etc.) ?	1
06A03-05	La non application des procédures ci-dessus doit-elle obligatoirement faire l'objet d'une dérogation formelle signée par un membre de la Direction ?	0
06A03-06	L'ensemble des procédures de contrôle de la maintenance fait-il l'objet d'un audit régulier ?	0
06A04	***Contrôle de la télémaintenance***	X
06A04-01	En cas de télémaintenance, y a-t-il une procédure d'authentification forte du centre de télémaintenance ?	
06A04-02	En cas de télémaintenance, y a-t-il une procédure d'authentification forte de l'agent de maintenance ?	
06A04-03	Existe-t-il un ensemble de procédures couvrant l'attribution de droits d'utilisation à un nouvel agent, le retrait de droits et l'ouverture de droits pour les situations d'urgence ?	

06A04-04	Les procédures et protocoles d'échange de conventions secrètes, de stockage, etc. ont-elles été approuvées par le RSSI ou un organisme spécialisé ?	
06A04-05	L'utilisation de la ligne de télémaintenance nécessite-t-elle l'agrément préalable (à chaque utilisation) de l'exploitation (après que le constructeur ou l'éditeur ait envoyé une demande spécifiant la nature, la date et l'heure de l'intervention) ?	
06A04-06	Les équipements ouverts à la télémaintenance sont-ils protégés contre toute inhibition ou modification des conditions d'accès à la télémaintenance avec émission d'une alarme en cas de violation ?	
06A04-07	L'ensemble des procédures de contrôle de la télémaintenance fait-il l'objet d'un audit régulier ?	
06A05	***Gestion des procédures opérationnelles d'exploitation des réseaux***	
06A05-01	Les procédures opérationnelles d'exploitation des réseaux découlent-elles d'une étude de l'ensemble des cas à couvrir par ces procédures (cas normaux de fonctionnement et incidents) ?	0
06A05-02	Les procédures opérationnelles d'exploitation sont-elles documentées et maintenues à jour ?	0
06A05-03	Les procédures opérationnelles d'exploitation sont-elles rendues disponibles à toute personne en ayant besoin ?	0
06A05-04	Les modifications de ces procédures sont-elles approuvées par les responsables concernés ?	0
06A05-05	Ces procédures sont-elles protégées contre des altérations illicites ?	0
06A05-06	L'authenticité et la pertinence des procédures opérationnelles font-elles l'objet d'un audit régulier ?	0
06A06	***Gestion des prestataires ou fournisseurs de services liés aux réseaux***	
06A06-01	S'assure-t-on régulièrement que les services de sécurité mis en œuvre par des prestataires ou fournisseurs de services réseaux sont effectivement assurés par lesdits prestataires ou fournisseurs ?	1
06A06-02	S'assure-t-on que les prestataires ou fournisseurs de services réseaux ont effectivement prévu les dispositions nécessaires pour être à même d'assurer les prestations de services convenues ?	1
06A06-03	Le respect des clauses de sécurité, par les prestataires ou fournisseurs, fait-il l'objet de revues régulières ?	0
06A06-04	S'assure-t-on que les prestataires ou fournisseurs de services réseaux signalent et documentent tout incident de sécurité touchant l'information ou les réseaux ?	0
06A06-05	Y a-t-il une revue régulière de ces incidents ou des dysfonctionnements avec les prestataires ou fournisseurs concernés ?	0
06A06-06	Tout changement dans les relations contractuelles (obligations diverses, niveaux de service, etc.) fait-il l'objet d'une analyse des risques induits potentiels ?	0
06A07	***Prise en compte de la confidentialité lors des opérations de maintenance sur les équipements de réseau***	
06A07-01	Existe-t-il une procédure décrivant en détail les opérations à mener, avant appel à la maintenance, pour empêcher que le personnel de maintenance ait accès aux données critiques (clés de chiffrement ou de protection de réseau, configurations des équipements de sécurité, etc.) ?	0
06A07-02	Existe-t-il une procédure et une clause contractuelle vis-à-vis du personnel de maintenance (interne et externe), spécifiant que tout support ayant contenu des informations sensibles doit être détruit en cas de mise au rebut ?	0
06A07-03	Existe-t-il une procédure de vérification de l'intégrité des systèmes après intervention de la maintenance (absence de logiciel espion, absence de cheval de Troie, etc.) ?	1
06A07-04	La non application des procédures ci-dessus doit-elle obligatoirement faire l'objet d'une dérogation formelle signée par un membre de la Direction ?	0
06A07-05	Les procédures ci-dessus font-elles l'objet d'un audit régulier ?	0
06A08	***Gestion des contrats de services réseaux***	X

06A08-01	Les niveaux de services ont-ils été identifiés pour chaque service réseau ? *Les niveaux de services comprennent non seulement le service rendu aux utilisateurs, mais les dispositifs de sécurité nécessaires et les obligations des parties prenantes.*	
06A08-02	Les niveaux de services ont-ils été inclus dans un contrat de service (que ces services soient assurés en interne ou par un prestataire externe) ?	
06A08-03	L'application des mesures correspondantes est-elle contrôlée ?	
06B	**Paramétrage et contrôle des configurations matérielles et logicielles**	
06B01	***Paramétrage des équipements de réseau et contrôle de la conformité des configurations***	
06B01-01	Existe-t-il un document (ou un ensemble de documents) ou une procédure opérationnelle spécifiant l'ensemble des paramètres de sécurité des équipements de réseau ? *Un tel document doit découler de la politique de protection des réseaux et décrire l'ensemble des règles de filtrage décidées. Il devait également contenir les références des versions de systèmes pour pouvoir vérifier l'état des mises à jour.*	0
06B01-02	Ce (ou ces) document impose-t-il de supprimer l'ensemble des comptes génériques ou par défaut et en établit-il la liste ?	X
06B01-03	Ce document ou cette procédure impose-t-elle la mise en place d'un dispositif de synchronisation avec un référentiel de temps précis ?	X
06B01-04	Ces paramétrages sont-ils régulièrement mis à jour en fonction de l'état des connaissances, en relation avec un organisme expert (audits spécialisés, abonnement à un centre de service, consultation régulière des avis des CERTs, etc.) ?	X
06B01-05	Ces documents de référence (ou des copies des paramètres installés, considérées comme des références) sont-ils protégés contre toute altération indue ou illicite, par des mécanismes forts (sceau électronique) ?	X
06B01-06	L'intégrité des configurations par rapport aux configurations théoriquement attendues est-elle testée très régulièrement (au moins hebdomadairement, si ce n'est à chaque initialisation du système) ?	0
06B01-07	Procède-t-on à des audits réguliers de la liste des paramètres de sécurité spécifiés ?	0
06B01-08	Procède-t-on à des audits réguliers des procédures d'exception et d'escalade en cas de difficulté ?	0
06B01-09	Les environnements de développement et de test sont-ils séparés des environnements opérationnels ?	0
06B02	***Contrôle des configurations des accès réseaux des postes utilisateurs***	
06B02-01	Existe-t-il un document décrivant l'ensemble des paramètres à contrôler sur les postes utilisateurs concernant leurs possibilités de connexion externe (modem, WiFi, ...) ?	0
06B02-02	Ce document est-il régulièrement mis à jour en fonction de l'état des connaissances, en relation avec un organisme expert (audits spécialisés, abonnement à un centre de service, consultation régulière des avis des CERTs, etc.) ?	0
06B02-03	Ce document de référence est-il protégé contre toute altération indue ou illicite, par des mécanismes forts (sceau électronique) ?	0
06B02-04	Contrôle-t-on la conformité des configurations des équipements réseau des postes de travail des utilisateurs par rapport à ce document de référence ?	0
06B02-05	Ce contrôle est-il fait systématiquement à chaque connexion au réseau ?	0
06B02-06	Y a-t-il des automates analysant systématiquement l'utilisation du réseau de télécommunication pour transmettre des données ?	0
06B02-07	Y a-t-il des automates analysant la présence de borne non déclarée de réseau sans fil (WiFi) ?	0
06B02-08	La configuration des postes utilisateurs les empêche-t-elle de modifier les configurations et d'installer des logiciels systèmes ?	0

06B02-09	Procède-t-on à des audits réguliers du document de référence spécifiant les configurations utilisateurs, et de l'application régulière des procédures de contrôle des configurations ?	0
06C	**Contrôle des droits d'administration**	
06C01	***Gestion des droits privilégiés sur les équipements de réseau***	
06C01-01	A-t-on établi une politique de gestion des droits privilégiés sur les équipements de réseau s'appuyant sur une analyse préalable des exigences de sécurité, basées sur les enjeux de l'activité ?	0
06C01-02	Cette politique est-elle documentée, revue régulièrement et approuvée par les responsables concernés ?	1
06C01-03	A-t-on défini, au sein de l'exploitation des réseaux, des profils correspondant à chaque type d'activité (administration d'équipements, administration d'équipement de sécurité, pilotage réseau, opérations de gestion de supports et sauvegardes, etc.) ?	0
06C01-04	A-t-on défini, pour chaque profil, les droits privilégiés nécessaires ?	0
06C01-05	La procédure d'attribution de droits privilégiés nécessite-t-elle l'accord formel de la hiérarchie (ou du responsable de la prestation pour un prestataire) à un niveau suffisant ?	0
06C01-06	La procédure d'attribution de droits privilégiés n'est-elle attribuée qu'en fonction du profil du titulaire ?	0
06C01-07	Le processus d'attribution (ou modification ou retrait) de droits privilégiés à un individu est-il strictement contrôlé ? *Un contrôle strict requiert une reconnaissance formelle de la signature (électronique ou non) du demandeur, qu'il existe un contrôle d'accès très renforcé pour pouvoir attribuer ou modifier de tels droits, et que les modifications d'attributions de droits privilégiés soient journalisées et auditées.*	0
06C01-08	Y a-t-il un processus de suppression systématique des droits privilégiés lors de départs ou mutations de personnel ?	0
06C01-09	Y a-t-il un audit régulier, au moins une fois par an, de l'ensemble des droits privilégiés attribués ?	0
06C02	***Authentification et contrôle des droits d'accès des administrateurs et personnels d'exploitation des réseaux***	
06C02-01	Le protocole d'authentification des administrateurs réseaux ou possesseurs de droits privilégiés est-il considéré comme "fort" ? *Un protocole d'authentification est considéré comme fort s'il n'est pas susceptible d'être mis en brèche par une observation ou une écoute de réseau, ni mis en défaut par des outils de spécialistes (en particulier des outils de craquage de mots de passe). Il s'agit de protocole s'appuyant généralement sur des procédés cryptologiques.*	1
06C02-02	A défaut, s'il s'agit de mots de passe, les règles imposées peuvent-elles être considérées comme très strictes ? *Des règles très strictes supposent des mots de passe non triviaux et testés comme tels avant acceptation, des mélanges de différents types de caractères avec une longueur importante (10 caractères ou +). Il est souhaitable que de telles règles soient élaborées en accord avec le RSSI.*	X
06C02-03	Cette authentification forte est-elle la règle aussi bien pour la connexion des administrateurs au système de supervision des machines virtuelles du réseau qu'entre ce système et les équipements de réseau ? *Si l'administrateur se connecte à un hyperviseur de gestion du réseau (genre HP OpenView, IBM TIVOLI, Unicenter de CA, Patrol de BMC ou Bull OpenMaster) avec une authentification éventuellement forte et un contrôle d'accès réel, il faut également que le contrôle soit effectif, avec la même robustesse, au niveau des différents objets à administrer (en évitant, par ex. en snmp les mots de passe en clair, les groupes community et public par défaut, les accès par telnet ou SQL simple) pour*	1

éviter des actions malveillantes directes sur les équipements.

06C02-04	Y a-t-il un contrôle systématique des droits de l'administrateur, de son contexte et de l'adéquation de ces droits et du contexte avec l'accès demandé, en fonction de règles de contrôle d'accès formalisées ?	0
06C02-05	Les paramètres de l'authentification sont-ils sous contrôle strict ? *Un contrôle strict requiert que la liste des personnes habilitées à changer les règles de définition des authentifiants, les authentifiants eux-mêmes, les règles de surveillance des tentatives de connexion, etc. soit très limitée, qu'il existe un contrôle d'accès renforcé pour procéder à ces modifications, que les modifications soient journalisées et auditées et qu'il existe un audit général au moins annuel de l'ensemble des paramètres de l'authentification.*	1
06C02-06	Les processus qui assurent l'authentification sont-ils sous contrôle strict ? *Un contrôle strict requiert que le logiciel correspondant ait été validé et subisse régulièrement un test d'intégrité (sceau) et qu'il existe un audit au moins annuel des procédures et processus de l'authentification.*	1
06C02-07	Existe-t-il un audit régulier des profils privilégiés effectivement attribués ?	0
06C02-08	Existe-t-il un audit régulier des procédures d'attribution de profils privilégiés et des paramètres de sécurité de protection des profils et des droits ?	0
06C03	***Surveillance des actions d'administration des réseaux***	
06C03-01	A-t-on fait une analyse approfondie des événements ou successions d'événements menés avec des droits d'administration et pouvant avoir un impact sur la sécurité des réseaux (configuration des systèmes de sécurité, accès à des informations sensibles, utilisation d'outils sensibles, téléchargement ou modification d'outils d'administration, etc.) ?	0
06C03-02	Enregistre-t-on ces événements (journalisation) ainsi que tous les paramètres utiles à leur analyse ultérieure ?	0
06C03-03	Existe-t-il un système permettant de détecter toute modification ou suppression d'un enregistrement passé et de déclencher une alerte immédiate auprès d'un responsable ?	1
06C03-04	Existe-t-il une synthèse de ces enregistrements permettant à la hiérarchie de détecter des comportements anormaux ?	1
06C03-05	Existe-t-il un système permettant de détecter toute modification des paramètres d'enregistrement et de déclencher une alerte immédiate auprès d'un responsable ?	0
06C03-06	Toute inhibition du système d'enregistrement et de traitement des enregistrements déclenche-t-elle une alarme auprès d'un responsable ?	0
06C03-07	Les enregistrements ou les synthèses sont-ils protégés contre toute altération ou destruction ?	1
06C03-08	Les enregistrements ou les synthèses sont-ils conservés sur une longue durée ?	1
06C03-09	Les procédures d'enregistrement des actions privilégiées et de traitement de ces enregistrements font-elles l'objet d'un audit régulier ?	1
06C04	***Contrôle des outils et utilitaires de l'exploitation du réseau***	X
06C04-01	Les outils ou utilitaires sensibles de l'exploitation du réseau (administration des privilèges, gestion des configurations, sauvegardes, copies, reprises à chaud, etc.) sont-ils recensés de manière exhaustive pour chaque type de profil de personnel d'exploitation ?	

06C04-02	Les outils ou utilitaires sensibles d'un profil d'exploitation ne sont-ils utilisables que par les titulaires du profil correspondant, après authentification individuelle forte (carte à puce, jeton d'authentification, etc.) ?	
06C04-03	Est-il interdit d'ajouter ou de créer des outils ou utilitaires d'exploitation de réseau sans autorisation formelle ?	
06C04-04	Cette interdiction est-elle régulièrement contrôlée par un automatisme avec alerte auprès d'un responsable ?	
06C04-05	La limitation des privilèges accordés aux équipes d'exploitation les empêche-t-elle de modifier les outils ou les utilitaires de l'exploitation ou, à défaut, existe-t-il un contrôle de toute modification avec alerte auprès d'un responsable?	
06C04-06	L'attribution des profils et la mise en œuvre des mesures de sécurité précédentes font-elles l'objet d'un audit régulier ?	
06D	**Procédures d'audit et de contrôle des réseaux**	
06D01	***Fonctionnement des contrôles d'audit***	
06D01-01	Les exigences et les procédures à respecter pour les audits menés sur les réseaux ont-elles été édictées par les responsables ?	0
06D01-02	Les règles concernant les audits menés sur les réseaux, les procédures et responsabilités associées, sont-elles définies et documentées ? *Les limites à apporter concernent les types d'accès aux équipements, les contrôles et les traitements admis, l'effacement des données sensibles obtenues, le marquage de certaines opérations, ... ainsi que l'habilitation des personnes réalisant l'audit.*	0
06D01-03	Les auditeurs sont-ils indépendants des activités concernées ?	1
06D01-04	Les opérations d'audit réalisées pour les données critiques sont-elles enregistrées ?	0
06D01-05	L'activité des auditeurs est-elle délimitée ? *Une telle délimitation est particulièrement recommandée s'il s'agit d'intervenants externes.*	0
06D02	***Protection des outils et résultats d'audit***	X
06D02-01	Les outils d'audit sont-ils protégés afin d'éviter toute utilisation indue ou malveillante ? *Ceci s'applique, en particulier, aux tests de pénétration et aux évaluations de vulnérabilité.*	
06D02-02	Les résultats d'audit sont-ils protégés contre toute modification ou divulgation ?	
06D02-03	L'utilisation des outils et des résultats d'audit est-elle délimitée ? *Une telle délimitation est particulièrement recommandée s'il s'agit d'intervenants externes.*	

ANNEXE 2

QUESTIONNAIRE D'EVALUATION DE L'EXPLOITATION DES RESEAUX

Questionnaire de prise de connaissance générale du réseau informatique

Fait par :	Client :			
Date :	Validé par :			
1	**Réseau Informatique**	**OUI**	**NON**	**OBSERVATIONS**
1.1	L'ensemble des postes de travail sont-ils reliés au sein d'un réseau local ?			
1.2	Chaque poste de travail dispose t'il d'un accès internet ?			
1.3	Les accès internet font-ils l'objet de restriction ?			
1.4	La banque dispose t'elle d'une plateforme ouverte à ses partenaires et accessible via internet ?			
1.5	Si oui, la plateforme a-t-elle un lien avec les applications internes de la banque ?			
1.6	Tous les postes de travail disposent t'ils des applications de travail ?			
1.7	La plateforme interne de travail de la banque est-elle reliée à internet ?			
1.8	Certains employés de la banque possèdent-ils des ordinateurs portables disposant des applications de travail ?			
1.9	Si oui, emportent-ils les ordinateurs hors de la banque ?			
1.10	Le réseau informatique a déjà t-il été l'objet d'attaques externes ?			
1.11	Le réseau informatique a déjà t-il été perturbé par des attaques externes ?			
1.12	Le réseau informatique a déjà t'il été victime de dysfonctionnements internes ?			
1.13	Le réseau informatique a déjà t'il été perturbé par des dysfonctionnements internes ?			
1.14	L'exploitation a déjà t'il été perturbé par des dysfonctionnements du réseau ?			
1.15	Le réseau informatique est-il fréquemment maintenu ?			
1.16	Est-il effectué une évaluation du dispositif de maîtrise des risques liés au réseau informatique ?			
1.17	Ledit dispositif est-il évalué par le service d'audit interne uniquement ?			
1.18	Ledit dispositif est-il évalué par le service informatique uniquement?			
1.19	Ledit dispositif est-il évalué conjointement par le service d'audit interne et le service informatique ?			
1.20	Existe-t-il un référentiel des risques liés au réseau informatique ?			
1.21	La dernière évaluation du dispositif de maitrise date t'elle de plus d'un an ?			
1.23	La banque prend-elle en compte la probabilité d'être victime d'attaques externes ?			
1.24	La banque prend-elle en compte la probabilité d'être victime d'incidents internes émanant des utilisateurs eux-mêmes?			

Annexe 3

QUESTIONNAIRE DE PRISE DE CONNAISSANCE GENERALE DU RESEAU INFORMATIQUE

BIBLIOGRAPHIE

Ouvrages

1. ATELIN Philippe (2006), *Réseaux informatiques : Notions fondamentales Normes, modèle OSI, TCP-IP, Ethernet, WI-FI*, 3e édition, Editions ENI, France, 452 pages.
2. BERGERET Louis François Etienne (2002), *Les passions dangers et inconvénients pour les individus, la famille et la société – hygiène et morale*, Adamant Media Corporation, 347 pages.
3. BLOCH Laurent & WOLFHUGEL Christophe (2003), *Sécurité informatique : principes et méthodes*, 1ère édition, Eyrolles, France, 276 pages.
4. CALE Stéphane & TOUITOU Philippe (2007), *La sécurité informatique : réponses techniques, organisationnelles et juridiques*, 1ère édition, Hermes Science Lavoisier, France, 282 pages.
5. COMER Douglas (2000), *TCP/IP architecture protocoles applications*, 3e édition, Dunod, France, 608 pages.
6. CLUSIF (2010), Base de connaissances, *MEHARI 2010.*
7. CLUSIF (2010), Guide de la démarche, *MEHARI 2010.*
8. CLUSIF (2010), Guide de l'analyse des enjeux et de la classification, *MEHARI 2010.*
9. CLUSIF (2010), Guide du diagnostic et de l'état des services de sécurité, *MEHARI 2010.*
10. CLUSIF (2010), Guide de l'analyse et du traitement des risques, *MEHARI 2010.*
11. CLUSIF (2010), Manuel de référence des services de sécurité, *MEHARI 2010.*
12. CLUSIF (2010), Présentation générale, *MEHARI 2010.*
13. CLUSIF (2010), Principes fondamentaux et spécifications fondamentales, *MEHARI 2010.*
14. DE LA BRUSLERIE Hubert (2003), *Trésorerie d'entreprise : Gestion de liquidités et des risques*, 2e édition, Dalloz, France, 690 pages.
15. DE MARESCHAL Gilbert (2003), *La cartographie des risques*, Afnor, France, 50 pages.
16. FERRERO Alexis (1995), *Ethernet et ses évolutions*, Addison-Wesley, France, 394 pages.
17. FORAY Bernard (2007), *La fonction RSSI*, 1ère édition, Dunod, 268 pages.

18. FOROUZAN Behrouz (2002), *Local area networks,* 1ère edition, MC Graw-Hill science, 640 pages.
19. FOUQUET Bruno (2000), *Gestion de la qualité de service*, 1ère édition, Eyorlles, 264 pages.
20. HAMZOUI Mohamed (2005), *Audit : gestion des risques et contrôle interne*, 1ère édition, Village mondial, 256 pages.
21. IFACI, COOPERS & LANDWELL (2005), *le management des risques de l'entreprise*, Editions d'organisation, 338 pages
22. IFACI, COOPERS & LYBRAND(200), *La nouvelle pratique du contrôle interne*, 1ère édition, Editions d'organisation, France, 378 pages.
23. LAFITE Michel (2003), *Sécurité des systèmes d'informations et maîtrise des risques*, La revue banque, France, 127 pages.
24. LIMONCELLI Thomas (2007), *Admin'sys : Gérer son temps*, 1ère édition, Eyrolles, 257 pages.
25. LLORENS Cedric (2006), *Tableaux de bord de la sécurité réseau*, 2e édition, Eyrolles, France, 559 pages.
26. MC NAMEE David (1998), *Business risk assessment*, Institute of Internal Auditors, 107 pages.
27. MONTAGNON Jean-Antoine (2001), *Les réseaux d'entreprise d'aujourd'hui : architecture et organisation – haut débit - tendances du marché*, Dunod, France, 376 pages.
28. MONTAIGNER Jean-Luc (2004), *Réseaux d'entreprise par la pratique*, 2e édition, Eyrolles, France, 548 pages.
29. MOREAU Franck (2002), *Comprendre et gérer les risques*, Editions d'organisation, Paris, 222 pages.
30. NORTHCUTT Stephane & NOVAL Judy (2004), *Détection et indtrusion de réseau*, 3e édition, Vuibert, 478 pages.
31. OUAKIL Laurent & PUJOLLE Guy, *Téléphonie sur IP*, 2e édition, Eyrolles, France, 485 pages.
32. PUJOLLE Guy (2008), *Les réseaux informatiques*, Eyrolles, France, 1099 pages.
33. RENARD JACQUES (2003), *Théorie et pratique de l'audit interne*, 5e édition, Editions d'organisation, 485 pages.
34. RENARD JACQUES (2005), *Théorie et pratique de l'audit interne*, 6e édition, Editions d'organisation, 480 pages.

35. RENARD JACQUES (2009), *Théorie et pratique de l'audit interne*, 7e édition, Editions d'organisation, 465 pages.
36. SANDOVAL Victor (1996), *Intranet le réseau d'entreprise*, Hermes Science publications, 138 pages.
37. SIMONI Noëmie & ZNATY Simon (1998), *Gestion de réseau et de service*, Masson, 479 pages.
38. TANEMBAUM Andrew (2002), *Computer networks*, 4e edition, Prentice hall, 912 pages.

Articles

39. BAPST Pierre-Alexandre & BERGERET Florence (2002), Pour un management des risques orientés vers la protection de l'entreprise et la création de la valeur, *Revues Françaises de l'Audit Interne*, n°162, P.30-33.
40. LECLERC, Hélène, D'ALDRAND, Guy, POTVIN, Kim-Andrée & RICARDO, Alexandre (2003), le risk assessment: quelques bonnes pratiques, *Revues Françaises de l'Audit Interne*, n°163, P.6.

Sources Internet

41. FONTUGNE, Muriel (2001), Cartographie des risques: Quelle valeur ajoutée? Quel processus ? www.amrae.asso.fr/les rencontres/Lille2002/actes/p10/p10.Fontugne.pdf