Livre Blanc

Sécurité des systèmes d'Informations : La **qualité**, les **méthodes** et leurs **process** à mettre en œuvre pour atteindre un **niveau de sécurité optimal.**

Sommaire :

Que signifie "Sécurité de l'information" ?

Pour des soucis d'efficacité et de rentabilité, une entreprise communique aujourd'hui avec ses filiales, ses partenaires et va jusqu'à offrir des services aux particuliers, ce qui induit une ouverture massive à l'information. Par l'ouverture des réseaux, la sécurité devient un facteur décisif du bon fonctionnement de l'entreprise ou de l'organisme.

Il reste qu'une entreprise ou un organisme possède certaines informations qui ne doivent être divulguées qu'à un certain nombre de personnes ou qui ne doivent pas être modifiées ou encore qui doivent être disponibles de manière transparente à l'utilisateur. Ces informations feront l'objet d'une attaque si et seulement si des menaces existent et si le système abritant ces informations est vulnérable.

Par conséquent on appelle **sécurité de l'information**, l'état de protection, face aux risques identifiés, qui résulte de l'ensemble des mesures générales et particulières prises pour assurer la confidentialité, l'intégrité et la disponibilité de l'information traitée, où :

- **la confidentialité** est le caractère réservé d'une information dont l'accès est limité aux seules personnes admises à la connaître pour les besoins du service.
- **l'intégrité** de l'information traitée garantit que celle-ci n'est modifiée que par un acte volontaire et légitime.
- **la disponibilité** est l'aptitude d'un système d'accéder à l'information dans des conditions définies d'horaires, de délais et de performances.

Pourquoi dois-je protéger mes informations ?

Parce que j'estime que si je perds ces informations, cela provoquerait :

- **Une perte financière** (exemple : destruction de fichiers client, récupération de contrats par un concurrent,...)
- **Une perte de l'image de marque** (exemple : piratage d'une banque, divulgation d'un numéro de téléphone sur liste rouge,...)
- **Une perte d'efficacité ou de production** (exemple : rendre indisponible un serveur de fichiers sur lequel travaillent les collaborateurs)

D'où l'intérêt pour une entreprise ou un organisme d'avoir une classification de ses informations. Par exemple, on peut citer les informations dites :

- **stratégiques** pour l'entreprise comme les offres de rachat en général ce sont des informations manipulées au niveau de la Direction de l'entreprise ou de l'organisme
- **critiques** comme le plan d'adressage de l'entreprise, la configuration des outils de sécurité, les plans de secours,...
- **internes** comme l'ensemble des informations propres à l'entreprise et qui ne doit pas être forcément de notoriété publique
- **publiques** comme les informations faisant l'objet de communiqué de presse ou les informations figurant que le site Web de l'entreprise ou de l'organisme

Mais tout ce travail de classification demande une réflexion qui doit être menée au sein de l'entreprise et de l'organisme.

Le monde de la Défense possède son propre système de classification de l'information : le Confidentiel Défense (CD), le Secret Défense (SD) et le Très Secret Défense (TS).

Pourquoi ai je perdu mes informations ?

Parce qu'une **menace** (une action ou un événement qui peut porter préjudice à la sécurité) s'est réalisée.

Pourquoi cette menace s'est réalisée ?

Parce que mon système est **vulnérable**. Le système d'information comprend aussi bien le système informatique, le téléphone, la télécopie, la vidéo mais aussi l'homme.

Pourquoi mon système est vulnérable ?

Parce que :

- Il n'existe pas de contrôle d'accès individuel aux applications
- Il n'existe pas de système de sauvegarde

- L'accès à mes locaux est ouvert à tout public
- Le personnel n'est pas sensibilisé à ce qu'il peut faire ou ne pas faire, dire ou ne pas dire.

En effet, informer le personnel sur les règles mises en place pour protéger les informations qu'il manipule participe à la sécurité de l'information. Tout membre du personnel, qui met en péril l'entreprise ou l'organisme, parce qu'il n'a pas été tenu informé des règles de protection de l'information, ne pourra pas être poursuivi pénalement, contrairement au cas inverse selon les articles 226-16 et 226-17 du nouveau code pénal.

L'audit de sécurité

Audit, conformité et référentiel

En informatique, le terme " d'audit " apparu dans les années 70 a été et est utilisé de manière relativement aléatoire. Nous considérons par la suite un "audit de sécurité informatique" comme une mission d'évaluation de conformité par rapport à une politique de sécurité ou à défaut par rapport à un ensemble de règles de sécurité.

Une mission d'audit ne peut ainsi être réalisée que si l'on a défini auparavant un référentiel, c'est-à-dire en l'occurrence, un ensemble de règles organisationnelles, procédurales ou/et techniques de référence. Ce référentiel permet au cours de l'audit d'évaluer le niveau de sécurité réel de " terrain " par rapport à une cible.

Pour évaluer le niveau de conformité, ce référentiel doit être :

- **complet** (mesurer l'ensemble des caractéristiques : il ne doit pas s'arrêter au niveau système, réseau, télécoms ou applicatif, de manière exclusive, de même, il doit couvrir des points techniques et organisationnels) ;
- **homogène** : chaque caractéristique mesurée doit présenter un poids cohérent avec le tout ;
- **pragmatique** : c'est-à-dire, aisé à quantifier (qualifier) et à contrôler. Ce dernier point est souvent négligé.

La mission d'audit consiste à mesurer le niveau d'application de ces règles sur le système d'information par rapport aux règles qui devraient être effectivement appliquées selon les processus édictés. L'audit est avant tout un constat.

Un audit peut être mené en suivant deux approches (non exclusives) :

- une approche " **boîte blanche** " : l'audit est alors déroulé in situ, les auditeurs ont accès à l'organisation, aux données et traitements réalisés, aux documents et processus appliqués. Ils font appels aux interlocuteurs autant que de besoin.

- une approche **" boîte noire** " : l'audit est alors mené en partant d'une connaissance limitée du système d'information cible. Les auditeurs opèrent sans accès a priori aux systèmes et données. Les " tests d'intrusion " ou " tests intrusifs " font partie de cette catégorie d'audit.

Les deux approches précédentes sont complémentaires, en effet :

- Une approche " boîte blanche " est en général un audit plus homogène, l'évaluation possède une caractéristique d'analyse " en complétude " et les aspects techniques et organisationnels sont traités de manière uniforme ;

- Une approche " boîte noire " est en général un audit avec une vue plus parcellaire, révélant plutôt des lacunes ciblées à forte orientation technique. Il est plus délicat de cerner la "complétude " de cette approche mais cela permet de simuler des incidents ou attaques logiques sur le système d'information. Les "tests d'intrusion " font partie de cette seconde catégorie.

Dans les deux cas, il est nécessaire de préserver l'opérationnel pendant les tests et validation technique de sécurité (qualité de service, performances, contraintes d'administration et de supervision).

Pourquoi réaliser un audit ?

Les objectifs d'un audit sont multiples :

- Une **validation des mesures de sécurité** mises en œuvre (contrôle, suivi qualité) ;

- Une **validation des processus** d'alertes, de réaction face à des sinistres ou des incidents : en déclenchant une simulation d'attaque logique par exemple, on analyse la conformité de la réaction des acteurs avec les procédures en vigueur ;

- Une **détection** d'enjeux ou de lacunes "oubliées ";

- Une **sensibilisation** des utilisateurs, de la hiérarchie, des subordonnés aux risques encourus.

Limites d'un audit

Signalons d'abord les limites dues aux démarches de certains audits, en particulier :

- Les audits **"déclaratifs "**, c'est-à-dire dont les résultats reposent uniquement ou en grande majorité sur les déclarations lors d'entretiens avec les acteurs du système audité : cela introduit un biais du au contrôle volontaire/involontaire des audités sur les informations délivrées ;
- Les audits **"techniques"**, c'est-à-dire dont la prise en compte des procédures et de l'organisation sont inexistantes (et parfois même sans adaptation au contexte) ;
- Les audits **"non techniques"**, c'est-à-dire dont la prise en compte directe (tests in situ) des configurations effectives des équipements systèmes, réseaux et applicatives n'est pas réalisée.

Les limites inhérentes des audits sont par ailleurs les suivantes :

- Le temps imparti est restreint (la probabilité qu'une cause possible de futur incident de sécurité ne soit pas détectée n'est pas nulle) ;
- L'appréciation du contexte de l'entreprise (fonctionnelle, métier) est parfois délicate (un audit doit comporter ainsi une analyse minimale des enjeux et de la sensibilité des données et traitements) ;
- Le niveau de sécurité appliquée sur le système d'information est dynamique : il peut évoluer fortement en fonction d'une simple mise à jour de système d'exploitation ou d'applicatif par exemple. Il en ressort qu'un résultat d'audit peut être contredit par le moindre changement sur le système d'information (organisationnel ou technique).

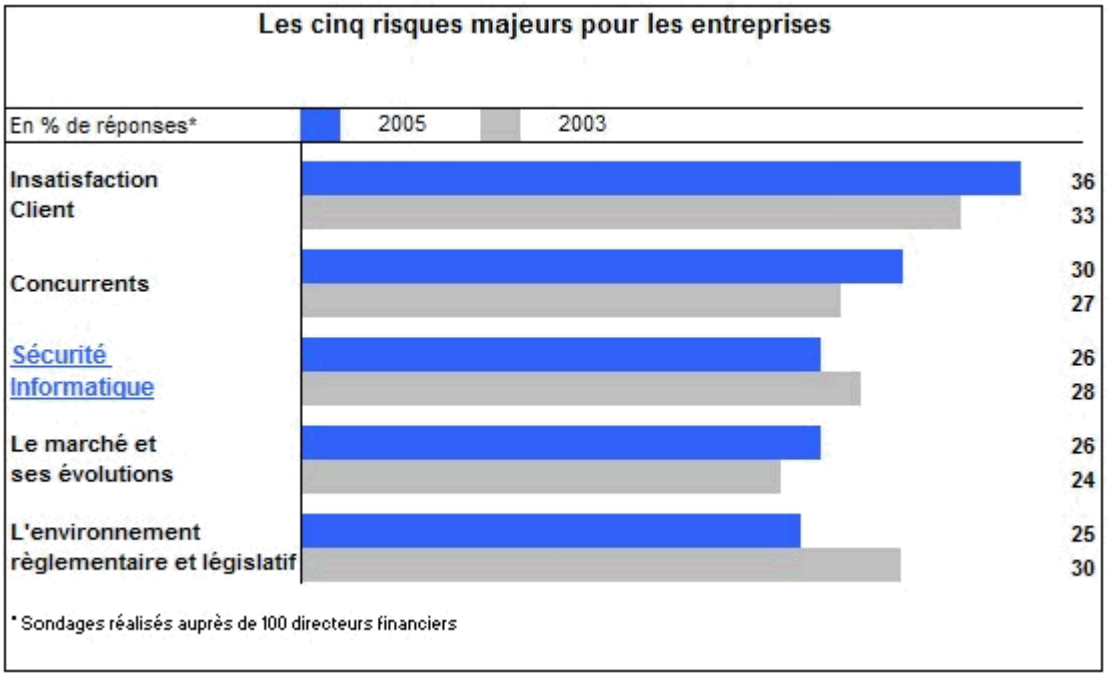
La Qualité

La norme ISO 17799 : Le code de bonnes pratiques pour la gestion de la sécurité de l'Information

La norme ISO 17799 est issue de la norme anglaise BS7799 créée en 1995 et révisée en 1999. Cette norme constitue un code de bonnes pratiques pour la gestion de la sécurité de l'information.

La sécurité de l'information constitue l'un des domaines majeurs au sein des entreprises. Quelque soit le secteur concerné, Banque, Assurance, Recherche, Conseil, Informatique, etc.., L'omniprésence de l'informatique transforme la gestion de l'information en un processus stratégique.

Afin de garantir la disponibilité, la confidentialité ainsi que l'intégrité des données, l'entreprise doit réfléchir sur l'architecture de son système d'information, et mettre en place les moyens de surveillance et de parade adaptée. La pérennité de l'entreprise dépend du succès de la stratégie de sécurité définie.



(Source : Etude Risk Management 2005, TNS Sofres)

Principes de base de la norme

Le modèle ISO 17799 : 2005, par sa reconnaissance internationale et son exhaustivité de bonnes pratiques permettent à tout dirigeant d'améliorer le système de management de la sécurité de l'information de l'entreprise.
Par une analyse de risques approfondie et le choix d'actions ciblées, la société s'engage dans une démarche proactive visant à réduire les vulnérabilités et les risques majeurs détectés.
Ce référentiel s'inscrit dans une philosophie de continuité d'activité et donc de service aux clients et aux partenaires.

L'ISO 17799 : 2006 est très riche et fournit au Responsable du Système de Sécurité de l'Information (RSSI) la matière nécessaire à la bonne gestion de la sécurité au sein de l'entreprise. Quelques chapitres tels que l'analyse de risques, la définition de la PSI (Politique de Sécurité de l'Information) constituent les fondements essentiels à toute application.

Les avantages de ce référentiel sont multiples :

- Gérer les coûts de la sécurité (un management efficace assure un retour sur investissement rapide),
- Minimiser les risques économiques et civils encourus par l'entreprise,
- Développer une culture sécurité à l'ensemble des collaborateurs.
- Améliorer votre niveau de sécurité,
- Se mettre en conformité avec la réglementation.

Rappel : la certification ISO

La **certification** est le moyen d'attester, par l'intermédiaire d'un tiers certificateur, de l'aptitude d'un organisme à fournir un service, un produit ou un système conformes aux exigences des clients et aux exigences réglementaires. L'ISO/CEI donne la définition suivante :

Procédure par laquelle une tierce partie donne une assurance écrite qu'un produit, un processus, ou un service, est conforme aux exigences spécifiées dans un référentiel.

La famille des normes ISO 9000 correspond à un ensemble de référentiels de bonnes pratiques de management en matière de qualité, portés par l'organisme international de standardisation (ISO, *International Organisation for Standardization*).

Les normes ISO 9000 ont été originalement écrites en 1987, puis elles ont été révisées en 1994 et à nouveau en 2000. Ainsi, la norme ISO 9001 version 2000, faisant partie de la famille ISO 9000, s'écrit ISO 9001:2000. La norme ISO 9001:2000 porte essentiellement sur les processus permettant de réaliser un service ou un produit alors que la norme ISO 9001:1994 était essentiellement centrée sur le

produit lui-même. Voici une présentation synthétique des différentes normes de la famille ISO 9000 :

- **ISO 9000** : "Systèmes de management de la qualité - **Principes essentiels et vocabulaire**". La norme ISO 9000 décrit les principes d'un système de management de la qualité et en définit la terminologie.
- **ISO 9001** : "Systèmes de management de la qualité - **Exigences**". La norme ISO 9001 décrit les exigences relatives à un système de management de la qualité pour une utilisation soit interne, soit à des fins contractuelles ou de certification. Il s'agit ainsi d'un ensemble d'obligations que l'entreprise doit suivre.
- **ISO 9004** : "Systèmes de management de la qualité - **Lignes directrices** pour l'amélioration des performances". Cette norme, prévue pour un usage en interne et non à des fins contractuelles, porte notamment sur l'amélioration continue des performances.
- **ISO 10011** : "Lignes directrices pour l'audit des systèmes de management de la qualité et/ou de management environnemental".

L'ISO n'a pas vocation à délivrer elle-même les certifications. Cette tâche est laissée à la charge d'un organisme certificateur tiers, lui-même accrédité par le COFRAC (en France). La certification ainsi obtenue est valable 3 ans et renouvelable suite à un audit.

Il est essentiel de garder en tête que la certification est basée sur les processus permettant d'obtenir un produit ou un service et non sur le produit/service lui-même.

La norme propose plus d'une centaine de mesures possibles réparties en **10 chapitres:**

1. **Politique de sécurité**

   Ce chapitre mentionne notamment la nécessité pour l'entreprise de disposer d'une politique de sécurité et d'un processus de validation et de révision de cette politique.

   Nota : l'existence même de cette mesure (non technique !) montre que l'ISO 17799 est avant tout, un immense catalogue de "bonne pratique" pour gérer de manière sécurisée ses informations.

2. **Organisation de la sécurité**

   Ce chapitre comporte 3 parties. Une partie traite de la nécessite de disposer au sein de l'entreprise d'une organisation dédiée à la mise en place et au contrôle des mesures de sécurité en insistant sur :

   - L'implication de la hiérarchie et sur la coopération qui devrait exister entre les différentes entités de l'entreprise,
   - La désignation de propriétaires de l'information, qui seront responsables de leur classification,
   - L'existence d'un processus pour la mise en place de tout nouveau moyen de traitement de l'information.

   Une deuxième partie traite des accès aux informations de l'entreprise par une tierce partie. Ces accès doivent être encadrés par un contrat qui stipule les conditions d'accès et les recours en cas de problèmes.

   Une troisième partie indique comment traiter du cas où la gestion de la sécurité est externalisée (Outsourcing).

3. **Classification des informations**

   Ce chapitre traite de la nécessité de répertorier l'ensemble des informations (ou types d'information) de l'entreprise et de déterminer leur classification. La mise en place d'une classification de l'information doit s'accompagner de la rédaction de guides pour la définition des procédures de traitement de chaque niveau de classification.

4. Sécurité du personnel

Ce chapitre mentionne trois types de mesures :

- Lors du recrutement de personnel, il est tout aussi important d'enquêter sur le niveau de confiance que l'on peut accorder aux personnes qui auront accès à des informations sensibles que de mentionner dans les contrats d'embauche des clauses spécifiques à la sécurité comme une clause de confidentialité.
- Une sensibilisation à la sécurité doit être proposée à toute personne accédant à des informations sensibles (nouvel arrivant, tierce partie)
- L'ensemble du personnel doit être informé de l'existence et du mode d'emploi d'un processus de remontée d'incidents.

5. Sécurité de l'environnement et des biens physiques

Ce chapitre traite de toutes les mesures classiques pour protéger les bâtiments et les équipements :

- délimitation de zone de sécurité pour l'accès aux bâtiments (attention aux accès par les livreurs)
- mise en place de sécurité physique comme la lutte contre l'incendie ou le dégât des eaux
- mise en place de locaux de sécurité avec contrôle d'accès et alarmes, notamment pour les salles machines
- mise en place de procédures de contrôle pour limiter les vols ou les compromissions
- mise en place de procédures pour la gestion des documents dans les bureaux

6. Administration

Ce chapitre traite des points suivants :

- rédiger et mettre à jour l'ensemble des procédures d'exploitation de l'entreprise (que ce soit pour de l'exploitation réseau, système ou sécurité)
- rédiger et mettre à jour les critères d'acceptation de tout nouveau système
-

- prévoir un planning pour l'achat de composants ou matériels pour éviter toute interruption de service
- mettre en place un certain nombre de politique organisationnelle et technique (anti-virus, messagerie, diffusion de document électronique en interne ou vers l'extérieur, sauvegarde et restauration, etc)

7. Contrôle d'accès

Ce chapitre comprend beaucoup de propositions de mesures par rapport aux autres chapitres. Sans être exhaustif, on peut cependant retenir :

- la nécessité pour l'entreprise de disposer d'une politique de contrôle d'accès (qui a droit à quoi et comment il peut y accéder)
- la mise en place d'une gestion des utilisateurs et de leurs droits d'accès sans oublier la révision de ces droits (gestion de droits, gestion de mot de passe ou plus généralement d'authentifiants)
- la responsabilité des utilisateurs face à l'accès aux informations (ne pas divulguer son mot de passe, verrouiller son écran quand on est absent par exemple)
- des propositions de mesures pour mettre en oeuvre la politique de contrôle d'accès comme l'utilisation de la compartimentation de réseaux, de firewalls, de proxis, ..., la limitation horaire d'accès, un nombre d'accès simultanés limité, etc.
- la mise en place d'un système de contrôle de la sécurité et de tableaux de bord
- l'existence et la mise en place de procédures concernant le télétravail

8. Développement et maintenance

Ce chapitre, de la même manière que précédemment, propose des mesures incontournables comme des exemples de mise en oeuvre. Sans être exhaustif, on peut retenir :

- la nécessité d'intégrer les besoins de sécurité dans les spécifications fonctionnelles d'un système
- des conseils de développement comme la mise en place d'un contrôle systématique des entrées sorties au sein d'un programme

- des propositions d'intégration de services de sécurité comme le chiffrement, la signature électronique, la non-répudiation, ce qui nécessiterait pour l'entreprise la définition d'une politique d'usage et de contrôle d'outils à base de cryptographie ainsi qu'une politique de gestion des clés associées
- la mise en place de procédures pour l'intégration de nouveaux logiciels dans un système déjà opérationnel
- la mise en place d'une gestion de configuration

9. Plan de continuité

Ce chapitre traite de la nécessité pour l'entreprise de disposer de plans de continuité ainsi que de tout le processus de rédaction, de tests réguliers et de mise à jour de ces plans.

10. Conformité légale et audit de contrôle

Ce chapitre traite pour l'essentiel de deux points :

- la nécessité pour l'entreprise de disposer de l'ensemble des lois et règlements qui s'appliquent aux informations qu'elle manipule et des procédures associées
- la mise en place de procédures pour le déroulement d'audit de contrôle

Conclusion

On peut donc noter que le contenu de l'ISO 17799 est à la fois un ensemble de mesures techniques et organisationnelles que l'entreprise devrait mettre en place pour gérer de manière sécurisée ses informations mais aussi un ensemble de propositions de solutions comme l'utilisation de firewall ou la composition des mots de passe (8 caractères, des caractères alphanumériques,...).

Par conséquent il est très intéressant de s'inspirer de cette norme pour s'informer sur les mesures qu'une entreprise peut mettre en place pour gérer la sécurité de ses informations. Par contre comme il n'existe pas encore de référence qui permette de situer une entreprise sur une échelle de gestion allant d'une mauvaise gestion à la gestion idéale, il est aujourd'hui très difficile d'apprécier le respect de cette norme par une entreprise.

Les Méthodes

La méthode MEHARI

La **ME**thode **H**armonisée d'**A**nalyse de **RI**sques (MEHARI) a été élaborée par la Commission Méthodes du CLUSIF (Club de la Sécurité des Systèmes d'Information Français).

Le but de la méthode d'approche top-down est de mettre à disposition des règles, modes de présentation et schémas de décision. L'objectif de la méthode est de proposer, au niveau d'une activité comme à celui d'une entreprise, un plan de sécurité qui se traduit par un ensemble cohérent de mesures permettant de palier au mieux, les failles constatées, et d'atteindre le niveau de sécurité répondant aux exigences des objectifs fixés.

Le modèle de risque MEHARI se base sur :

- Six facteurs de risque indépendants : trois influant sur la potentialité du risque et trois influant sur son impact ;
- Six types de mesures de sécurité, chacun agissant sur un des facteurs de risque (structurelle, dissuasive, préventive et de protection, palliative et de récupération).

Les phases de MEHARI sont les suivantes :

- Phase 1 : établissement d'un plan stratégique de sécurité (global) qui fournit notamment :
    - la définition des métriques des risques et la fixation des objectifs de sécurité,
    - la reconnaissance et la détermination des valeurs de l'entreprise,
    - l'établissement d'une politique de sécurité entreprise,
    - l'établissement d'une charte de management.
- Phase 2 : établissement de plans opérationnels de sécurité réalisés par les différentes unités de l'entreprise ;
- Phase 3 : consolidation des plans opérationnels (global).

La méthode MARION

La méthode MARION (Méthodologie d'Analyse de Risques Informatiques Orientée par Niveaux) est issue du CLUSIF (http://www.clusif.asso.fr/).

Il s'agit d'une méthodologie d'audit, qui, comme son nom l'indique, permet d'évaluer le niveau de sécurité d'une entreprise (les risques) au travers de questionnaires pondérés donnant des indicateurs sous la forme de notes dans différents thèmes concourrant à la sécurité.

Objectif de la méthode

L'objectif est d'obtenir une vision de l'entreprise auditée à la fois par rapport à un niveau jugé " correct ", et d'autre part par rapport aux entreprises ayant déjà répondu au même questionnaire.

Le niveau de sécurité est évalué suivant 27 indicateurs répartis en 6 grands thèmes, chacun d'eux se voyant attribuer une note de 0 à 4, le niveau 3 étant le niveau à atteindre pour assurer une sécurité jugée correcte.

À l'issue de cette analyse, une analyse de risque plus détaillée est réalisée afin d'identifier les risques (menaces et vulnérabilités) qui pèsent sur l'entreprise.

Fonctionnement de la méthode

La méthode est basée sur des questionnaires portant sur des domaines précis. Les questionnaires doivent permettre d'évaluer les vulnérabilités propres à l'entreprise dans tous les domaines de la sécurité.

L'ensemble des indicateurs est évalué par le biais de plusieurs centaines de questions dont les réponses sont pondérées (ces pondérations évoluent suivant les mises à jour de la méthode).

Les thèmes sont les suivants :

- Sécurité organisationnelle
- Sécurité physique
- Continuité
- Organisation informatique
- Sécurité logique et exploitation
- Sécurité des applications

Déroulement de la méthode

La méthode se déroule en 4 phases distinctes :

Phase 0 : Préparation

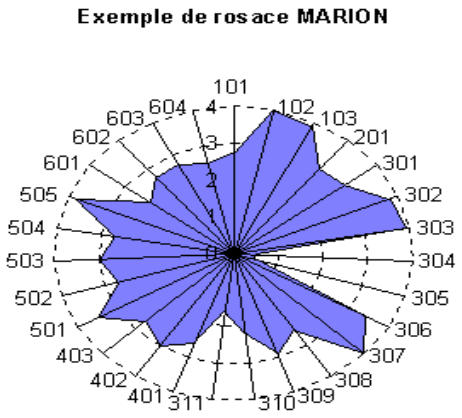
Durant cette phase, les objectifs de sécurité sont définis, ainsi que le champ d'action et le découpage fonctionnel permettant de mieux dérouler la méthode par la suite.

Phase 1 : Audit des vulnérabilités

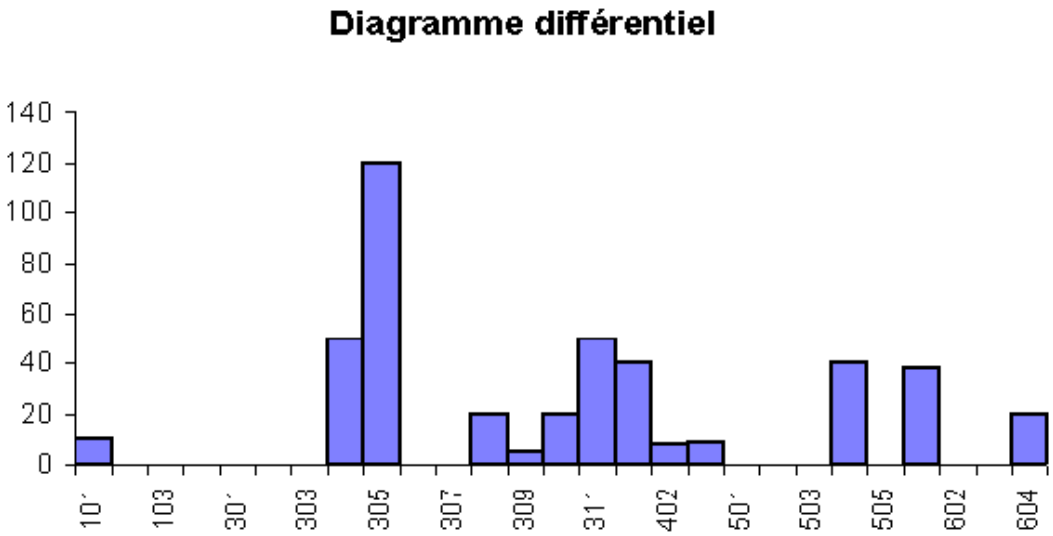
Cette phase voit le déroulement des questionnaires ainsi que le recensement des contraintes propres à l'organisme.

Le résultat des questionnaires permet d'obtenir la "rosace" propre à l'entreprise.

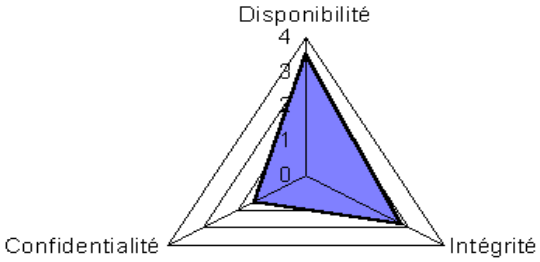
Cette rosace, l'aspect le plus connu de la méthode, présente les 27 indicateurs sur un cercle, avec le niveau atteint. Cela permet de juger facilement et rapidement des domaines vulnérables de l'entreprise, la cohérence et l'homogénéité des niveaux de sécurité des différents indicateurs, et donc d'identifier également rapidement les points à améliorer.

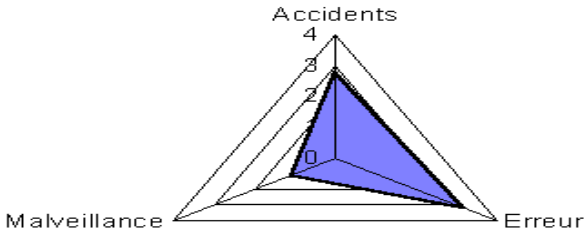


D'autres possibilités de diagrammes existent, parmi lesquels le diagramme différentiel qui permet de mieux comprendre l'importance des différents facteurs (d'après la méthode) et donc également de mettre les vulnérabilités de l'entreprise en perspective. Dans ce diagramme, chaque barre est proportionnelle à la différence entre la cotation 3 et la cotation réelle de l'existant, multipliée par le poids du facteur (le différentiel est nul si le facteur est déjà supérieur à 3)



Enfin, il est également possible d'afficher des diagrammes suivant les types de risques.





Phase 2 : Analyse des risques

Cette phase voit l'exploitation des résultats précédents et permet d'effectuer une ségrégation des risques en Risques Majeurs (RM) et Risques Simples (RS).

Le Système d'Information est alors découpé en fonctions qui seront approfondies en groupes fonctionnels spécifiques, et hiérarchisés selon l'impact et la potentialité des risques les concernant.

En ce qui concerne l'analyse de risque, MARION définit 17 types de menaces :

- Accidents physiques
- Malveillance physique
- Panne du SI
- Carence de personnel
- Carence de prestataire
- Interruption de fonctionnement du réseau
- Erreur de saisie
- Erreur de transmission
- Erreur d'exploitation
- Erreur de conception / développement
- Vice caché d'un progiciel
- Détournement de fonds
- Détournement de biens
- Copie illicite de logiciels
- Indiscrétion / détournement d'information
- Sabotage immatériel
- Attaque logique du réseau

Pour chaque groupe fonctionnel de l'entreprise, chaque fonction est revue en détail afin d'évaluer les scénarii d'attaque possible, avec leur impact et leur potentialité.

Phase 3 : Plan d'action

Durant cette ultime phase de la méthode, une analyse des moyens à mettre en oeuvre est réalisée afin d'atteindre la note " 3 ", objectif de sécurité de la méthode, suite aux questionnaires. Les tâches sont ordonnancées, on indique le degré d'amélioration à apporter et l'on effectue un chiffrage du coût de la mise en conformité.

Autres méthodes

On pourra comparer MARION avec d'autres méthodes du CLUSIF, principalement MEHARI, la dernière en date, probablement vouée à remplacer MARION à terme.

D'autres approches existent, parmi laquelle la méthode EBIOS (publique) de la DCSSI.

L'ISF possède également un ensemble de méthodologies de philosophies similaires mais d'approches souvent plus pragmatiques.

PMI (Project management Institute) est une méthodologie orientée gestion de projets dont la popularité tends à s'accroître, et fait l'objet d'une certification.

La société BlasCom IT l'utilise au sein de ses différents projets.

Process

Introduction à ITIL « Information Technology Infrastructure Library » :

ITIL a été développé avec les entreprises de plus en plus dépendantes de leur service informatique pour atteindre leurs objectifs et satisfaire leurs besoins. Ce qui conduit à la nécessité d'amélioration de la qualité et de l'évolutivité des services IT délivrés.

Le référentiel ITIL prône une démarche d'amélioration itérative des processus composant les services IT. Cette démarche est fondée sur :

- la définition des processus et de leurs interactions
- l'amélioration de la communication au niveau opérationnel, tactique et stratégique entre le SI et l'entreprise
- le rôle central du " service desk ", unique contact entre le SI et les utilisateurs
- le contrôle précis des résultats obtenus (rapports de gestions, KPIs, respect des SLAs)
- la définition des rôles et responsabilités

Le premier objectif de ITIL est de constituer un **référentiel des meilleures pratiques** pour la fourniture de services informatiques, afin d'aider les directions informatiques à atteindre dans ce domaine, leurs objectifs de qualité de service, et de maîtrise des coûts. ITIL représente aujourd'hui l'approche la plus complète, et la plus structurée disponible sur le marché pour le management des services informatiques.

Trois idées importantes sous-tendent la philosophie ITIL:

- **Customer focus** : l'utilisateur - le client - doit être au centre des préoccupations de la direction informatique,

- **Cycle de vie** : la gestion des services doit être prise en considération en amont des projets informatiques, dès la phase d'étude et de conception,

- **Processus** : la qualité de service repose sur une approche par les processus.

Concept

ITIL définit un service informatique comme un ensemble de fonctions assurées pour un utilisateur par un système d'information ; un service s'appuie en général sur plusieurs éléments - matériels, logiciels, réseaux, - constituant l'infrastructure informatique.

ITIL se présente sous la forme d'un ensemble de livres et de CD, traitant les domaines suivants :

- **Business Perspective**, consacré aux questions d'organisation et de structure (organisation de la production, relations entre les différentes fonctions, rôles et responsabilités, relations avec les fournisseurs et prestataires externes).

- **Service Delivery,** consacré à la gestion des services (gestion des niveaux de service, gestion des capacités et de la performance, gestion de la disponibilité, gestion de la continuité de service, gestion financière).

- **Service Support**, consacré à la gestion de l'infrastructure technique (gestion des configurations, gestion des incidents et des problèmes, service desk, gestion des changements, gestion des mises en production).

- **Infrastructure Management**, consacré à l'exploitation informatique (gestion de l'exploitation, automatisation de l'exploitation, maintenance, installation, administration de réseaux, administration des systèmes distribués).

- **Application Management**, consacré à la gestion des relations entre études et exploitation
(support logiciel, mise en production).

- **Security Management**, consacré aux questions de sécurité et de continuité du service.

- **Planning to Implement Service Management**, consacré à la mise en oeuvre pratique d'ITIL.

ITIL rencontre depuis plusieurs années, un succès croissant auprès des entreprises et des organismes publics, en Europe et aux Etats-Unis, pour plusieurs raisons :

- ITIL permet aux entreprises de capitaliser sur une expérience pratique de plus de 20 ans sur la gestion des services informatiques, et de gagner du temps en évitant de réinventer la roue et en utilisant des éléments déjà testés et éprouvés (processus, règles de gestion, descriptions de postes, etc.)

- ITIL offre les avantages d'une méthode publique, qui est un standard de facto.

- Le choix de l'ITIL permet de faciliter le dialogue entre les différents acteurs à partir d'un cadre de référence commun.

Bénéfices d'ITIL pour les entreprises 'dans la pratique' :

- Augmenter la satisfaction du client grâce aux procédures déployées permettant de respecter les SLA
- Améliorer le taux d'utilisation des ressources
- Fournir les services dont l'organisation a vraiment besoin par l'intermédiaire d'un catalogue précis
- Identifier et fournir des indicateurs clés éprouvés
- Réduire le nombre de modifications
- Réduire le coût grâce au développement des bonnes pratiques et des procédures appliquées
- Établir une meilleure communication entre le personnel informatique et les "clients"
- Avoir une plus grande productivité et une meilleure utilisation des qualifications et de l'expérience
- Tirer les leçons des expériences
- Justifier les coûts de fourniture de services de qualité.

1/ Le service support, un des piliers de la méthode ITIL

Ce domaine se compose de 6 processus types :

Configuration management

La gestion de configuration est utilisée pour assurer le contrôle de tous les composants de l'infrastructure informatique, y compris la documentation, et ainsi

faciliter la maîtrise des changements et le traitement des incidents et des problèmes.

Change management

Processus décrivant les activités permettant de conduire rapidement et efficacement tous les changements afin de minimiser le risque d'impact négatif de ces changements sur la qualité de service.
La demande de changement se fait à travers des RFC (Request For Change). Ces RFC sont passés en revue par le CAB (Change Advisory Board).
Le CAB est un comité consultatif chargé d'évaluer le risque et l'impact de ces changements et de conseiller le gestionnaire des changements.

Release management

Processus visant à coordonner l'ensemble des activités liées au stockage, à la gestion, à la distribution et à la mise en place de tous les composants logiciels du système d'information.
Il garantit que les versions autorisées et testées des logiciels sont effectivement mise en production, constitue un référentiel des logiciels autorisés et prend en compte les aspects techniques et non-techniques.
Ces versions sont stockées dans une DLS (Definitive Software Library) – bibliothèque de versions de références –.

Service desk

Le service desk est le point de contact, au quotidien, entre les utilisateurs du SI et le département informatique.

Il est responsable du traitement de toutes les attentes des utilisateurs, que celles-ci soient de simples demandes ou occasionnées par des dysfonctionnements du SI (qu'ils soient directement signalés par des appels utilisateurs et/ou par des remontées d'alarmes automatiques).

Pour tout dysfonctionnements, il doit également s'assurer de la remise en conformité du SI du point de vue de l'utilisateur. Le Service Desk est responsable de l'application des processus de résolution des incidents.

Incident management

Processus permettant de décrire les activités afin de restaurer, aussi rapidement que possible, le service normal, et de réduire, au minimum, l'effet négatif du dysfonctionnement.

Problem management

Processus qui permet d'optimiser le niveau de service en analysant les causes réelles des dysfonctionnements et en y apportant des solutions correctives, afin d'éviter que ces mêmes dysfonctionnements ne se produisent à nouveau.

On constate que plusieurs processus sont imbriqués les uns aux autres. C'est le cas de Configuration Management, Service Desk, Incident Management et Problem Management.
Mais de quoi sont composés les processus de Configuration Management et Service Desk qui sont les processus principaux de ce module ?

Description détaillée du processus de "configuration management" et "service desk"

Le processus de configuration management à pour objectifs de :
- contrôler l'infrastructure informatique en recensant l'ensemble des informations sur toutes les ressources nécessaires à la fourniture des services informatiques ainsi que sur l'état, l'appartenance et l'historique des différents composants de l'infrastructure et enfin sur les relations entre les différents composants,
- mettre à jour et faire le suivi de toute modification,
- vérifier que l'infrastructure ne contient que les composants « autorisés ».

Il permet non seulement de piloter la configuration logiciel mais aussi la gestion de l'organisation autour du logiciel.

Ce processus contient deux éléments :

- des CI pour Configuration Item – c'est un élément de configuration au sens large utilisé pour fournir un service–. Il est identifiable et peut être géré. Il se caractérise par une catégorie, des attributs, des relations et un statut.
- une base de donnée qui regroupe ces CI.

La classification des éléments de configuration se fait par catégorie (groupe d'éléments ayant une ou des caractéristiques communes) et par statut (caractéristiques propres aux éléments d'une même catégorie).

Le statut décrit l'état d'un élément (réparation, production, préparation,…). L'ensemble de ces états constitue le cycle de vie de cet élément.

Le Service Desk a pour objectifs :

- d'être la principale interface entre la DSI et les utilisateurs pour : les incidents, les questions, les améliorations, les remarques,
- de gérer la satisfaction du client par rapport aux services fournis,
- de piloter la fourniture des différents services,
- de gérer initialement les incidents et superviser le processus de gestion des incidents jusqu'à leur résolution,
- de contribuer à l'utilisation optimale du SI en fonction des objectifs et des contraintes du business,
- de fournir une source centrale d'information pour le management des services.

-

Le Service Desk doit :

- recevoir et enregistrer tous les appels utilisateurs,
- réaliser une première évaluation pour tous les incidents,
- suivre dans le temps et affecter tous les incidents en respectant les engagements de niveaux de service,
- contrôler le cycle de vie de tous les appels (validation et fermeture incluses),
- coordonner l'ensemble des activités d'escalade,
- informer régulièrement l'utilisateur sur l'état et la progression de son appel,
- fournir une source centrale d'information pour la gestion des services,
- participer à l'identification des problèmes.

Comme on le constate le Service Desk ne se situe pas au même niveau que les autres processus. En effet, il « pilote » les processus d'Incident et Problem Management. Il intervient aussi bien à un niveau informationnel (gestion de la documentation) que logiciel.

2/ L'autre pilier de la méthode : service delivery

5 processus types le composent :

Service Level Management

Ce Processus permet de définir, négocier, documenter et contrôler les services et les niveaux de service, en collaboration avec le représentant des utilisateurs (clients) chargé de cette activité et les prestataires de services internes ou externes (ou leurs responsables) chargés de fournir le service.

Il permet d'établir un catalogue des services, d'évaluer l'expression de besoins utilisateur et de valider les niveaux de service requis (Service Level Requirement – **SLR**), de négocier et formaliser les contrats de service (Service Level Agreements – **SLA**), les engagements de prestations en interne (Operational Level Agreements – **OLA**) ou en externe avec les contrats de sous-traitance (Underpinning Contract – **UC**) et enfin de rédiger et mettre en œuvre le Plan Qualité (Service Quality Plan – **SQP**).

Availability Management

La gestion de la disponibilité (Availability Management) est le processus permettant de mettre en œuvre une méthode et des outils qui permettent de mesurer et de piloter la disponibilité des composants du SI pour s'assurer que la disponibilité des services est conforme aux engagements pris dans les SLAs (Service Level Agreements).

Capacity Management

La gestion des capacités est le processus permettant de prendre en compte :
- la stratégie de l'entreprise : les services que l'on souhaite pouvoir délivrer dans le futur (Business Capacity Management).
- l'organisation de la production : La façon dont les services sont actuellement fournis (Service Capacity management).
- l'infrastructure : les moyens à mettre en œuvre pour pouvoir fournir les services (Resource Capacity Management).

Il permet aussi de s'assurer que tous les aspects actuels et futurs en terme de ressources et de performance sont pris en compte.

IT Service Continuity Management

Le service Continuity Management est le processus permettant de définir, tester et mettre à jour régulièrement, les plans et/ou procédures, afin de prévenir toute interruption des services critiques pendant une longue période.

Financial Management for IT Services

C'est un processus qui permet de :

- déterminer la rentabilité des actifs et des ressources utilisées pour la fourniture des services,
- expliquer entièrement les dépenses sur des services et attribuer ces coûts aux services fournis aux clients de l'organisation,
- aider à la prise de décision sur les investissements

Pour en savoir plus : http://www.itil.co.uk et http://www.itsmf.com

Conclusions générales :

En améliorant leurs processus de gestion de leurs infrastructures et de leurs services informatiques, réseaux et Télécoms tout en s'appuyant *sur les conseils de BlasCom IT*, les entreprises peuvent :

- Disposer d'une base d'informations centralisée
- Améliorer le taux d'utilisation des ressources
- Améliorer l'efficacité des équipes informatiques
- Limiter la duplication de certaines tâches
- Réduire les coûts des services de support et d'assistance aux utilisateurs
- Garantir le respect des délais pour les projets informatiques
- Fournir les services dont l'entreprise a réellement besoin
- Documenter les processus, le rôle des différents acteurs
- Automatiser certains processus clés
- Etc…

Contact :
27 rue du Président Edouard Herriot
69002 LYON – France
Tel : +33(0)4 27 11 56 31 Fax : +33(0) 4 78 28 39 33

Web : www.BlasCom.com

Email : blascom@blascom.com