

Modèle de maturité à usage des PME/TPE

RESUME

Lié au modèle de référence de processus, le modèle de maturité présenté ici est un cadre particulier d'évaluation de processus pour aider les organisations, à développer et à renforcer leurs capacités de gestion de la sécurité de l'information avec succès, via des notions reconnues dans le monde de la qualité.

DATE

Novembre 2005

AUTEUR

M.POGGI Sébastien

<http://www.cases.lu>



LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG
Ministère de l'Economie
et du Commerce extérieur



CENTRE DE RECHERCHE PUBLIC
HENRI TUDOR
www.tudor.lu



CASES

LUXEMBOURG

CYBERWORLD AWARENESS AND
SECURITY ENHANCEMENT STRUCTURE

TABLE DES MATIERES

| | | |
|------------|---|-----------|
| I | INTRODUCTION | 5 |
| II | UN TAILORING NÉCESSAIREMENT LIMITÉ | 6 |
| | II.1 DU MODÈLE GÉNÉRIQUE AU MODÈLE SPÉCIFIQUE | 6 |
| | II.2 LE PARADOXE DE LA SÉLECTION | 6 |
| III | LA « MATURITÉ » DES PME/TPE | 7 |
| | III.1 LA MATURITÉ DES PROCESSUS ET DES ORGANISATIONS | 7 |
| | III.2 EVALUATION ET/OU AMÉLIORATION | 7 |
| | III.3 LE CADRE DE MESURAGE | 8 |
| IV | LE MODÈLE DE MATURITÉ ORIENTÉ « ORGANISATION » | 10 |
| | IV.1 PRESENTATION..... | 10 |
| | IV.2 LISTE DES NIVEAUX DE MATURITE | 11 |
| | IV.3 DESCRIPTION DES NIVEAUX DE MATURITE | 12 |
| | IV.3.1 Niveau « Zero »..... | 12 |
| | IV.3.2 Niveau « Mandatory »..... | 13 |
| | IV.3.3 Niveau « Ignition »..... | 14 |
| | IV.3.4 Niveau « Management Support »..... | 15 |
| | IV.3.5 Niveau « Communication Handling »..... | 16 |
| | IV.3.6 Niveau « Formal analysis »..... | 17 |
| | IV.3.7 Niveau « Verification »..... | 18 |
| | IV.3.8 Niveau « Business Protection »..... | 19 |
| | IV.3.9 Niveau « Follow-up »..... | 20 |
| | IV.3.10 Niveau « ISMS » | 21 |
| | IV.4 EVALUATION | 22 |
| V | LA VUE COMBINATOIRE OU LE MEILLEUR DES (DEUX) MONDES ? ... | 23 |
| VI | SYNTHÈSE | 27 |
| | ANNEXE | 28 |

GLOSSAIRE

BP

Base Practice

CMM

Capability Maturity Model

EBIOS

Expression des Besoins et Identification des Objectifs de Sécurité

GG

Generic Goal

ISMS

Information Security Management System

ISO

International Standardization Organization

NPLF

Not – Partially – Largely - Fully

PDCA

Plan – Do – Check – Act

PAM

Process Assesment Model

PRM

Process Reference Model

SG

Specific Goal

SP

Specific Practice

SSIC

Sécurité des Systèmes d'Information et de la Communication

I Introduction

A travers le PRM développé en amont, diverses activités relatives à la SSIC étaient présentées à des fins d'évaluation ou d'amélioration. La modélisation en processus, la politique de sécurité, le concept d'ISMS et son cycle PDCA constituent des outils pour parvenir à ce but. Cependant, mettre en place une démarche sécurité n'est pas chose aisée car de nombreux obstacles peuvent survenir : exhaustivité des problèmes, impératifs financiers, difficulté de mesurer le retour sur investissement, pratiques fréquemment perçues comme limitatives, résistance au changement des utilisateurs, difficulté de se positionner par rapport à ses concurrents... Le modèle de maturité ci-dessous présenté est créé pour résoudre ces problématiques en apportant un cadre de mesurage à la fois pour l'évaluation et la gestion des pratiques. Pour avoir un aperçu de ce qu'est la maturité, une présentation rapide en est faite dans le document sur la démarche d'élaboration du PRM conjointement à la première partie de ce document.

II Un tailoring nécessairement limité

II.1 DU MODELE GENERIQUE AU MODELE SPECIFIQUE

Les termes « organisation » ou « entité » employés dans cette étude ont un caractère générique. Il peut très bien s'agir de grosses ou de petites entreprises, d'administrations, d'associations, de cabinets de libéraux. En matière de sécurité, il existe également des réglementations spécifiques pour des domaines d'activité particuliers tels que le secteur médical avec l'HIPAA, le secteur bancaire avec les accords de Bâle II, les sociétés cotées en bourse avec la loi Sarbanes-Oxley et bien entendu d'autres secteurs sensibles où la sécurité est une question sine qua non tels que l'armement, le militaire, l'aérospatiale et les secteurs à très forte concurrence.

Le modèle d'approche de la SSIC développé ne tient pas explicitement compte des spécificités des organisations. Il s'agit d'un concept fondateur pour l'évaluation et la gestion de la SSIC dans les organisations. Il est donc générique par essence et pourrait être adapté à de multiples formes d'organisation, avec toutefois en tête les PME/TPE du Luxembourg puisque l'ingénierie du modèle est calquée sur leur prise en compte. Le modèle de maturité traite donc en priorité ce type d'entités.

II.2 LE PARADOXE DE LA SELECTION

Ainsi que l'a révélé l'analyse sur la structuration économique des PME/TPE au Luxembourg dans le document correspondant, il existe un peu plus de 26000 PME/TPE au Luxembourg. Leur nombre n'est pas ici la caractéristique qui mérite notre attention, mais leur nature. Que ce soit par le nombre d'employés, leur secteur d'activité, l'importance de l'informatique, la maturité de l'entreprise en terme de SSIC ; elles sont toutes différentes, chacune ayant ses spécificités. Par conséquent, le modèle de maturité ne peut pas tenir compte de l'entreprise elle-même au vu de leur pluralité, avec une exception cependant : les secteurs d'activités où la réglementation impose des exigences de sécurité. Il faut donc recourir à un autre critère de sélection pour choisir ces échelons. Toutes les organisations qui vont utiliser les outils ici développés vont le faire avec l'ambition d'évaluer et/ou d'améliorer leur SSIC, créant de fait le critère discriminant qui nous est nécessaire pour construire le modèle.

III La « maturité » des PME/TPE

III.1 LA MATURETE DES PROCESSUS ET DES ORGANISATIONS

On définit la maturité d'un processus (on a alors plutôt tendance à parler d'aptitude) comme sa capacité à atteindre le but qui lui est attribué. Plus son aptitude est élevée et plus les résultats qu'il produira seront maîtrisés, le but final étant de parvenir à une amélioration continue du processus. Il en va de même pour les organisations dans un domaine donné. Plus une organisation est mature et plus les résultats dans ce domaine seront maîtrisés et en amélioration, dans ce cas précis : la gestion de la sécurité de l'information.

Pour mesurer cette maturité, deux référentiels sont considérés comme majeurs : ISO 15504 et CMM/CMMI. Ces référentiels offrent un cadre de mesurage pour coter les processus ou les organisations. Bien que très proches, ils offrent des fonctionnements différents. ISO 15504 va mesurer exclusivement les processus selon leur aptitude sur une échelle allant de 0 à 5. Il en va de même pour CMMI dans sa version dite « continuous » (continue).

Cependant, CMMI possède une autre version, dite « staged » (étagée) qui propose un fonctionnement différent. Suivant les processus réalisés selon un cheminement déterminé, l'organisation va se voir attribuer un niveau de maturité. Le modèle fournit simultanément une séquence d'amélioration qui commence avec des pratiques basiques pour progresser à travers un chemin dont chacun des niveaux contribue à asseoir le suivant et à faire progresser l'organisation dans le domaine concerné. Par exemple, l'organisation doit voir tous les processus du niveau 2 réalisés pour accéder au niveau 3. De plus, il offre un système de notation qui résume les résultats de l'évaluation, accessoirement par rapport à une cible donnée, et du même coup permet la comparaison entre les organisations.

III.2 EVALUATION ET/OU AMELIORATION

Qu'il s'agisse de maturité de processus ou d'organisation, les modèles de maturité et les référentiels associés poursuivent deux buts distincts : l'évaluation ou l'amélioration. Dans le cas d'une évaluation ISO 15504, qui est orientée vers les processus, les résultats vont servir de base à l'amélioration des pratiques ; idem pour CMM dans sa version continue. Une évaluation sur les bases du modèle étagé de CMM est orientée davantage vers l'organisation elle-même. L'amélioration est elle conduite par le modèle lui-même qui fournit le cheminement à suivre. Les deux approches sont donc divergentes. Les différences des deux approches nous permettent cependant d'exploiter le PRM développé précédemment selon deux angles d'attaque différents.

| APPROCHE | PROCESSUS | ORGANISATION |
|----------|---------------|--------------|
| Normes | ISO 15504 | CMM Staged |
| | CMM Continous | |

Table 1- Deux philosophies divergentes...

Le premier est celui dont est issu la notion de maturité, le domaine de la qualité. En effet, l'approche processus se concentre sur les processus eux-mêmes et leurs résultats, l'évaluation portant généralement sur un nombre restreint de processus clefs à définir avec le sponsor de l'évaluation. L'amélioration se fait ensuite sur ces processus. Ultérieurement, d'autres processus peuvent être considérés. ISO 15504 et CMM continu correspondant à cette vision.

Le second angle correspond au domaine traité par le PRM, la sécurité de l'information. Il s'agit donc ici d'employer une approche organisation se focalisant sur la maturité de l'organisation dans sa gestion de la sécurité. Pour pouvoir utiliser cette approche il faut cependant développer un modèle de maturité parallèle à celui proposé par CMM concernant la sécurité. (Ce modèle fait l'objet d'un chapitre spécifique – cf IV)

| APPROCHE | PROCESSUS | ORGANISATION |
|----------|---------------|--------------|
| Normes | ISO 15504 | CMM Staged |
| | CMM Continous | |
| ANGLE | QUALITE | SECURITE |

Table 2 - ... et pourtant complémentaires...

III.3 LE CADRE DE MESURAGE

Pour procéder à l'évaluation, il est nécessaire d'utiliser ce que l'on appelle un modèle d'évaluation.

Dans le cadre de l'évaluation de la maturité des processus, il est logique de recourir à une évaluation de type ISO 15504 reprenant les règles d'évaluation proposées par la norme ISO 15504-2 car le PRM développé a été formé dans ce sens. Il formerait un PAM valide d'un point de vu normatif en lui adjoignant le cadre de mesurage de la norme.

Dans le cadre de l'évaluation de la maturité de l'organisation, il est nécessaire de se référer au [chapitre suivant](#).

| APPROCHE | | PROCESSUS | ORGANISATION |
|----------|-------------------|-----------------------------|--------------|
| Normes | | ISO 15504 CMM Continuous | CMM Staged |
| ANGLE | | QUALITE | SECURITE |
| PAM | PRM | PRM R2SIC | |
| | CADRE DE MESURAGE | ISO 15504 | Spécifique |

Table 3 - ...utilisant un modèle adapté

IV Le modèle de maturité orienté « organisation »

IV.1 PRESENTATION

Le concept retenu ici pour les niveaux de maturité est un concept proche de celui de CMM dans sa version étagée. Il s'agit de plusieurs échelons à atteindre dans un ordre fixé, chacun de ces échelons étant composé de résultats de processus à réaliser pour parvenir au niveau suivant. Les niveaux et l'ordre à suivre sont déterminés selon une logique précise. En effet, l'objectif d'une démarche sécurité étant de parvenir à un état de sécurité adapté, on va définir les échelons à franchir pour parvenir à une gestion complète de la sécurité, en partant du fait que toutes les organisations n'ont pas les mêmes besoins. La forme modulaire du PRM, décomposé en processus, nous offre cette flexibilité.

Une organisation aura atteint le niveau maximal de maturité prévu par le modèle lorsqu'elle aura mis en place un ISMS complet qui lui permettra d'améliorer continuellement ses pratiques de gestion de la sécurité, respectant de ce fait intégralement le standard BS7799-2:2002, dédié à l'organisation de la sécurité et qui propose également une démarche de certification. Les niveaux intermédiaires sont conçus en suivant un cheminement sensé de progression, permettant d'offrir aux organisations une perspective d'amélioration de leurs pratiques. En termes d'évaluation, ces échelons permettent de situer une organisation par rapport à une cible qui peut être déterminée par le commanditaire de l'évaluation ou par les conditions environnementales de l'entreprise.

IV.2 LISTE DES NIVEAUX DE MATURITE

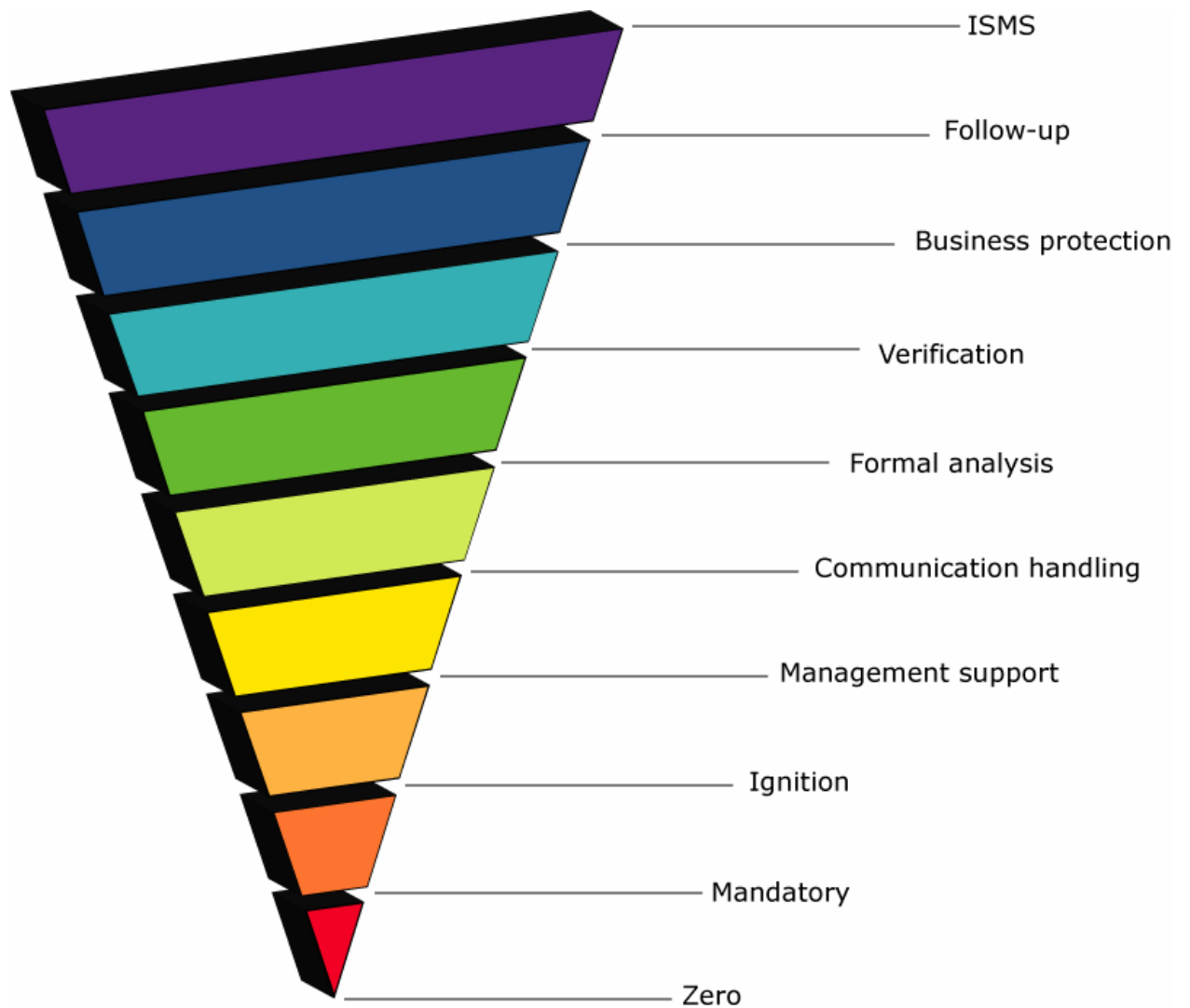


Figure 1 - Pyramide inversée des niveaux de maturité

IV.3 DESCRIPTION DES NIVEAUX DE MATURITE

IV.3.1 Niveau « Zero »

Le niveau « Zero » est le niveau le plus bas. A ce niveau, les activités sécurité sont inexistantes. Aucun processus ou aucun résultat de processus du PRM n'est atteint.

| Zero | |
|-------------------------------|--|
| Description | |
| Aucun résultat n'est réalisé. | |
| Processus et résultats | |
| Aucun | |

IV.3.2 Niveau « Mandatory »

Le niveau qui suit directement le niveau « Zero » est le niveau « mandatory » qui transcrit le strict minimum qui doit être mis en place dans toutes les organisations, notamment vis-à-vis des exigences légales. La conformité avec les lois sur la protection des données personnelles, la propriété intellectuelle, le droit en général et la réglementation concernant le métier de l'organisation sont assurées, réglementation pouvant faire référence à des niveaux supérieurs. Le respect réciproque des contrats passés avec les tiers fait partie également de ce niveau. Pratiquement, la mise en place complète des dispositions légales dans toutes les organisations est sujette à caution notamment vis-à-vis des demandes d'autorisations de traitement des données personnelles.

Ce niveau symbolise aussi la création d'un projet sécurité avec ses spécifications mais aussi l'allocation des ressources humaines, temporelles et financières nécessaires à ce projet. En l'occurrence, le projet sécurité couvre au moins les aspects légaux.

| Mandatory | |
|-------------------------------|--|
| Description | |
| | Le strict nécessaire est réalisé. A ce niveau, les exigences légales sont respectées et des ressources sont identifiées pour la démarche sécurité. |
| Processus et résultats | |
| | Processus et résultats concernés par le niveau Mandatory : <ul style="list-style-type: none">▪ CLE - Résultat 1▪ CLE - Résultat 2▪ CLE - Résultat 3▪ CLE - Résultat 4▪ CLE - Résultat 5▪ CLE - Résultat 6▪ CSE - Résultat 1▪ CSE - Résultat 2 |

IV.3.3 Niveau « Ignition »

Le niveau « Ignition » correspond à l'apparition dans l'organisation des premières mesures de sécurité. Ces mesures sont l'aboutissement d'une réflexion de haut niveau et généralement informelle sur les risques qu'encourt l'entreprise. Il s'agit de protéger les actifs les plus en vue de l'organisation. Pour ce faire des mesures de sécurité sont mises en places également appelées contre-mesures. Elles peuvent concerner aussi bien le niveau physique, réseau, application, données, ou être transverses à tous ces niveaux. Une politique de sécurité ou un équivalent est susceptible d'apparaître pour formaliser les premières mesures et décrire éventuellement la stratégie de l'organisation en termes de sécurité. Dans une configuration optimiste, la politique de sécurité est dynamique et revue au grès des améliorations.

| Ignition | |
|-------------------------------|---|
| Description | |
| | Dans ce niveau, les premières mesures de sécurité apparaissent. Elles sont issues généralement d'une réflexion de haut-niveau et informelle. Une politique de sécurité ou un équivalent est défini. |
| Processus et résultats | |
| | Processus et résultats concernés par le niveau Ignition : <ul style="list-style-type: none">▪ Ceux contenus dans le niveau Mandatory▪ ARI – Résultat 1▪ CSE – Résultat 2▪ SAF – Résultat 1▪ SAF – Résultat 2▪ SAF – Résultat 3▪ SAF – Résultat 4▪ SAF – Résultat 5 |

IV.3.4 Niveau « Management Support »

Le niveau « Management Support » transcrit l'apparition du soutien et l'implication du management, une condition sine qua non dans la réussite d'une démarche sécurité évoluée. Cela concerne donc aussi bien la contribution au projet lui-même que sa visibilité au sein de l'organisation. Le management doit par exemple afficher clairement à tous les collaborateurs son soutien. Il a aussi pour tâche de faciliter l'émergence d'une solution viable respectant les orientations stratégiques de l'organisation. La validation et la revue de cette solution rentrent également dans ses attributions tout en tenant compte du feedback de ses employés et de leurs remarques.

L'implication du management renforce la crédibilité de la démarche et sa viabilité en veillant à ce que celle-ci reste alignée avec les objectifs de l'organisation.

| Management Support | |
|---|--|
| Description | |
| Le soutien du management est un facteur crucial de réussite d'une démarche sécurité. Ce soutien doit se faire aussi bien dans le projet que hors du projet. | |
| Processus et résultats | |
| Processus et résultats concernés par le niveau Management support : <ul style="list-style-type: none">▪ Ceux contenus dans le niveau Ignition▪ ESM – Résultat 1▪ ESM – Résultat 2▪ ESM – Résultat 3▪ ESM – Résultat 4▪ PER – Résultat 2▪ PSE – Résultat 2 | |

IV.3.5 Niveau « Communication Handling »

Ce niveau met l'accent sur un des trois aspects fondamentaux de la sécurité : la communication. Ce niveau reflète l'apparition de pratiques liées à une meilleure compréhension de la sécurité de l'information en général, mais également des activités mises en œuvre au sein de l'organisation. De nombreux facteurs critiques sont contenus dans ce niveau car une sécurité efficace est liée à de nombreux facteurs dépendant de l'humain.

Une formation et une information adéquate des membres sont primordiales. La formation aux bonnes pratiques de sécurité est relative aux besoins et doit s'accompagner de la diffusion de connaissances de base. Des sources d'information sont également indispensables pour renseigner, rappeler aux utilisateurs ces bonnes pratiques et véhiculer les actualités concernant la démarche.

C'est à ce niveau qu'une gestion précise de la documentation doit être également réalisée (On pourra retrouver un descriptif d'un ensemble de documentation concernant le domaine en annexe). Cette documentation doit être accessible au plus grand nombre, notamment en ce qui concerne la politique de sécurité. En outre les architectes de la solution sécurité doivent donner un aperçu de cette dernière.

Les tiers (visiteurs, prestataires, maintenance...) doivent être inclus dans cette perspective et informés des pratiques à respecter.

| Communication handling | |
|---|--|
| Description | |
| L'apparition de pratiques liées à une meilleure diffusion des informations sécurité établit le niveau Communication handling. Il s'agit aussi bien de la sensibilisation des membres de l'organisation que de la communication au sein des activités sécurité. | |
| Processus et résultats | |
| Processus et résultats concernés par le niveau Communication handling : <ul style="list-style-type: none">▪ Ceux contenus dans le niveau Management support▪ CVE – Résultat 2▪ GRI – Résultat 3▪ PCO – Résultat 1▪ PCO – Résultat 2▪ PCO – Résultat 3▪ TIE – Résultat 3 | |

IV.3.6 Niveau « Formal analysis »

Ce niveau est un palier majeur. Il va conduire à des prises de décision solides sur base des résultats d'une analyse des risques formalisée. Cette analyse des risques peut être dite « détaillée » et ainsi basée sur une méthode reconnue telle la méthodologie proposée dans le PRM (EBIOS) , ou, reposer sur une approche dite « baseline », voire une combinaison des deux. Le but est de mener une étude réaliste qui puisse servir de base à des choix appropriés.

Ce niveau de maturité va également traiter ces choix et leur formalisation. La sélection des contre-mesures est donc de mise pour traiter les risques identifiés par l'analyse. Le transfert de certains risques fait aussi partie des activités à accomplir tout autant que les risques introduits par les interactions avec les tiers et son environnement, qui devraient également être détectés.

| Formal analysis | |
|-------------------------------|--|
| Description | |
| | L'apparition d'une analyse des risques formelle constitue une étape majeure dans la gestion de la sécurité. Les résultats de cette analyse conditionnent la suite des activités. |
| Processus et résultats | |
| | Processus et résultats concernés par le niveau Formal analysis : <ul style="list-style-type: none">▪ Ceux contenus dans le niveau Communication handling▪ ARI – Résultat 2▪ ARI – Résultat 3▪ GRI – Résultat 1▪ GRI – Résultat 2▪ PSE – Résultat 1▪ PSE – Résultat 3▪ TIE – Résultat 1▪ TIE – Résultat 4 |

IV.3.7 Niveau « Verification »

Si les mesures doivent être déployées avant ce niveau, on va ici s'attacher plus particulièrement à assurer et à vérifier leur bon fonctionnement. Elles doivent remplir parfaitement le rôle qui leur a été assigné. Cela concerne aussi bien les mesures techniques que organisationnelles.

Une administration renforcée qui puisse suivre les activités au jour le jour et détecter les incidents pouvant survenir devient nécessaire. Ce suivi permet d'adapter les configurations aux besoins ou de percevoir les améliorations à apporter. Les privilèges accordés aux utilisateurs en font partie. Ces utilisateurs doivent également participer à la vérification en s'assurant que leurs outils de traitement de l'information sont intègres.

La revue de l'efficacité des mesures de sécurité est également un des objectifs de ce niveau. Le test des mesures et des procédures mises en place devient nécessaire à ce niveau. Ce test peut être réalisé en interne par les services de sécurité et en externe par un prestataire indépendant qui puisse confirmer, ou infirmer, les résultats de l'audit interne. Le résultat de cette revue permet de savoir si les mesures sont adéquates ou si des adaptations doivent être réalisées.

| Verification | |
|-------------------------------|---|
| Description | |
| | Ce niveau traduit la mise en place d'activités qui vérifient que les mesures aussi bien techniques que organisationnelles sont mises en place |
| Processus et résultats | |
| | Processus et résultats concernés par le niveau Verification : <ul style="list-style-type: none">▪ Ceux contenus dans le niveau Communication handling▪ ADM – Résultat 1▪ ADM – Résultat 2▪ REV – Résultat 1▪ REV – Résultat 2▪ REV – Résultat 4▪ TIE – Résultat 2 |

IV.3.8 Niveau « Business Protection »

Ce niveau est dédié spécifiquement à la continuité des activités de l'organisation. A ce palier, l'organisation attache une importance toute particulière à la protection de ses activités. Les incidents sont gérés par des mesures appropriées visant à réduire les conséquences via un cheminement d'actions déterminé : détection, signalement, traitement, escalade, suivi, clôture.

Les incidents les plus graves sont traités par les plans de continuité et de recouvrement qui constituent le deuxième pan de ce niveau. La création de ces plans est précédée d'une analyse d'impact où les risques non gérés constituent une base de travail pour la réalisation de cette analyse. Une fois de plus, les plans doivent être diffusés et testés pour être connus et s'assurer de leur efficacité.

Afin de s'assurer que les activités de l'organisation sont intactes une vérification périodique des ressources disponibles depuis l'extérieur est nécessaire.

| Business protection | |
|-------------------------------|--|
| Description | |
| | Ce niveau s'attache à la continuité des activités de l'organisation. Les incidents, y compris les plus graves, sont gérés de manière appropriée. |
| Processus et résultats | |
| | Processus et résultats concernés par le niveau Business protection : <ul style="list-style-type: none">▪ Ceux contenus dans le niveau Verification▪ ADM – Résultat 3▪ GIN – Résultat 1▪ GIN – Résultat 2▪ GIN – Résultat 3▪ GIN – Résultat 4▪ GIN – Résultat 5▪ GIN – Résultat 6▪ GIN – Résultat 7▪ GIN – Résultat 8▪ PDC – Résultat 1▪ PDC – Résultat 2▪ PDC – Résultat 3▪ PDC – Résultat 4▪ PDC – Résultat 5 |

IV.3.9 Niveau « Follow-up »

Le niveau « Follow-up » met en place les canaux de retour d'information sur la qualité du système de gestion de la sécurité.

En interne des métriques (tableaux de bord) sont développées et mises en place pour fournir une appréciation du fonctionnement du système. En externe un suivi de l'actualité sécurité est opéré afin de discerner l'apparition ou l'évolution des risques affectant l'organisation. Des changements internes peuvent également entrer dans cette catégorie. Lorsque ces changements sont identifiés, qu'ils soient techniques, organisationnels ou liés à l'environnement, l'organisation et le système de gestion de la sécurité doivent s'adapter à ces nouvelles contraintes, soit par la modification de la solution sécurité, soit par l'émergence de propositions d'améliorations.

Les résultats de l'exploitation du système de gestion sont également synthétisés afin de présenter une vue rapide de son état.

| Follow-up | |
|---|--|
| Description | |
| Dans ce niveau, le dernier échelon avant de parvenir à un ISMS, l'organisation obtient un feedback sur le fonctionnement du système et du domaine de la sécurité de l'information en général. | |
| Processus et résultats | |
| Processus et résultats concernés par le niveau Follow-up : <ul style="list-style-type: none">▪ Ceux contenus dans le niveau Business protection▪ CVE – Résultat 1▪ CVE – Résultat 3▪ CVE – Résultat 4▪ PER – Résultat 1▪ TDB – Résultat 1▪ TDB – Résultat 2▪ TDB – Résultat 3▪ TDB – Résultat 4 | |

IV.3.10 Niveau « ISMS »

Ce dernier échelon correspond à l'établissement complet d'un ISMS tel que le précise la norme BS7799-2:2002. A ce niveau de maturité toutes les exigences sont respectées. Ce dernier échelon met en place la phase d'amélioration du cycle PDCA.

Les pistes d'amélioration sont identifiées sur base des métriques (établies au niveau précédent), des synthèses, des recommandations et de l'évolution des risques. Selon leur pertinence, elles sont validées, mises en places et testées pour s'assurer de leur utilité. Ces améliorations sont communiquées aux membres de l'organisation. De plus un historique est conservé afin de s'assurer de la traçabilité des mesures de sécurité et la politique de sécurité est mise à jour à chaque phase d'amélioration.

Par ailleurs une évaluation des processus est effectuée afin de déterminer la maturité du système.

| ISMS | |
|-------------------------------|--|
| Description | |
| | Ce niveau correspond à l'accomplissement total des exigences de la norme BS7799-2:2002 concernant la mise en place d'un ISMS. |
| Processus et résultats | |
| | Processus et résultats concernés par le niveau ISMS : <ul style="list-style-type: none">▪ Ceux contenus dans le niveau Follow-up▪ EIS – Résultat 1▪ EIS – Résultat 2▪ PER – Résultat 3▪ REV – Résultat 3 |

IV.4 EVALUATION

Evaluer la maturité de l'organisation sur sa gestion de la sécurité selon le modèle précédemment décrit revient à déterminer quels sont les résultats atteints parmi les processus décrits dans le PRM. Déterminer quels sont les résultats atteints repose sur la même démarche d'évaluation que celle correspondant au niveau 1 de ISO 15504. De fait, il n'est pas nécessaire d'employer une cotation à quatre niveaux NPLF, les résultats étant atteints, ou non. Comme pour une évaluation ISO 15504, le sponsor de l'évaluation détermine la cible à atteindre au sein de la pyramide. Selon le résultat de cette évaluation, le PRM et le modèle de maturité, l'organisation connaît instantanément les pratiques de base à mettre en place pour parvenir au niveau souhaité. Dans cette perspective d'amélioration le chemin proposé doit être scrupuleusement respecté afin d'obtenir une démarche cohérente et une intégration progressive des activités sécurité dans l'organisation.

V La vue combinatoire ou le meilleur des (deux) mondes ?

Pour résumer deux voies d'évaluation et d'amélioration ont été présentées, l'une en rapport avec le monde de la qualité et de l'amélioration de l'aptitude des processus, l'autre avec la gestion de la sécurité et l'amélioration de la maturité des organisations. Il est cependant possible de combiner les deux en une vue synthétique, selon la volonté de l'organisation. Pour y parvenir, il faut se rappeler que l'évaluation de la maturité de l'organisation repose sur l'évaluation des résultats de processus tout comme cela se fait dans une évaluation ISO 15504 concernant le niveau 1 d'aptitude du processus. Il est donc possible de prolonger l'évaluation en traitant les niveaux d'aptitude supérieurs et de situer à la fois la maturité de l'organisation et l'aptitude des processus en utilisant une échelle à deux dimensions.

La première dimension, horizontale, correspond à la maturité de l'organisation dans sa gestion de la sécurité (cf. Figure 2 - Exemple d'analyse de la maturité de l'organisation dans la gestion de la SSIC). La seconde, verticale, interprète l'aptitude des processus (cf. Figure 3 - Exemple de l'analyse de l'aptitude des processus de gestion de la SSIC). Les carrés rouges représentent les résultats de processus non atteints (niveau 0 pour l'ISO 15504) ; les verts représentent ceux qui le sont (niveau 1 à 5 pour l'ISO 15504). On peut ainsi dégager un profil pour l'organisation d'un point de vue processus (vue qualité) et d'un point de vue organisationnel (vue sécurité), ou une vue combinée (cf. Figure 4 - Exemple de résultat d'une analyse combinée qualité et sécurité).

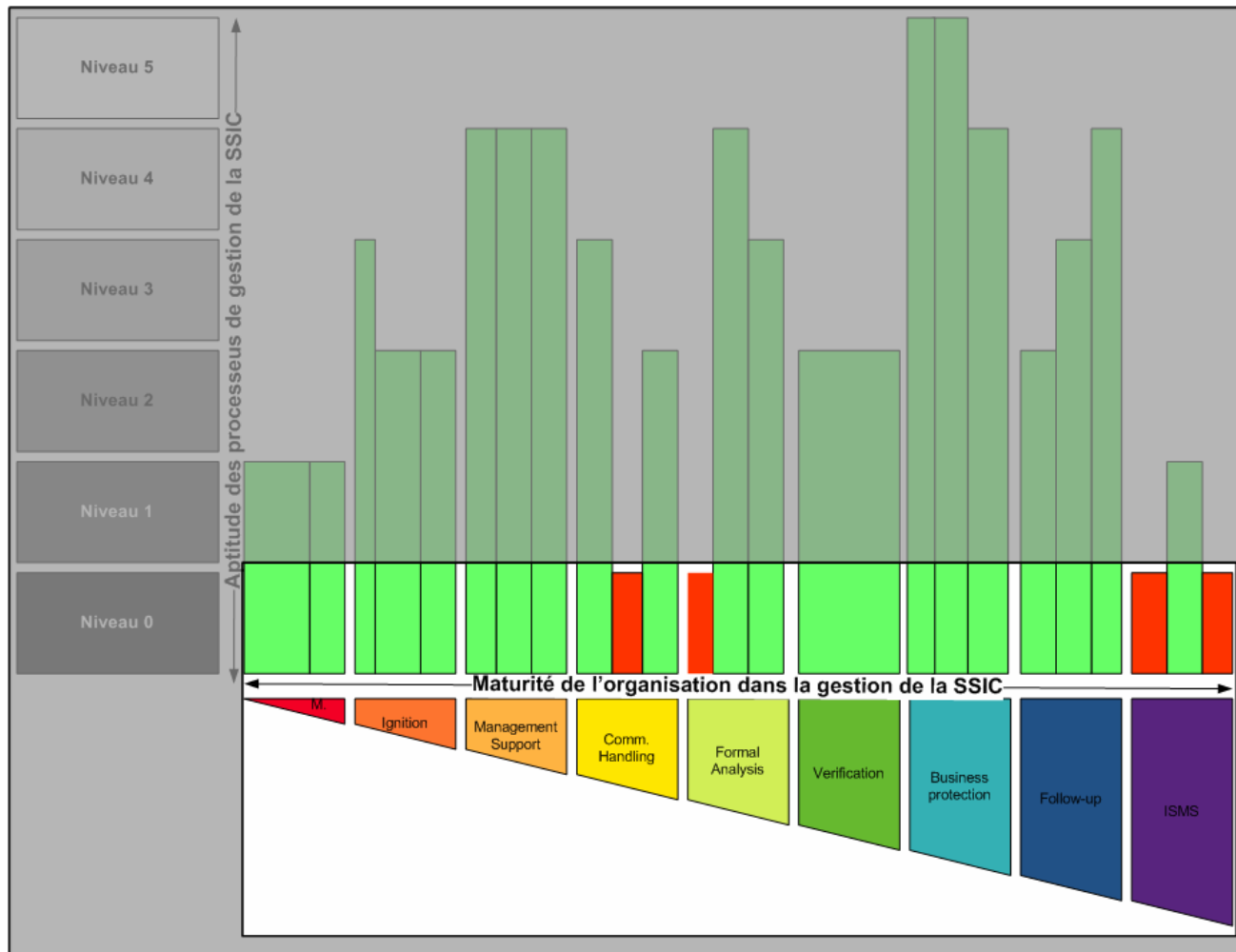


Figure 2 - Exemple d'analyse de la maturité de l'organisation dans la gestion de la SSIC

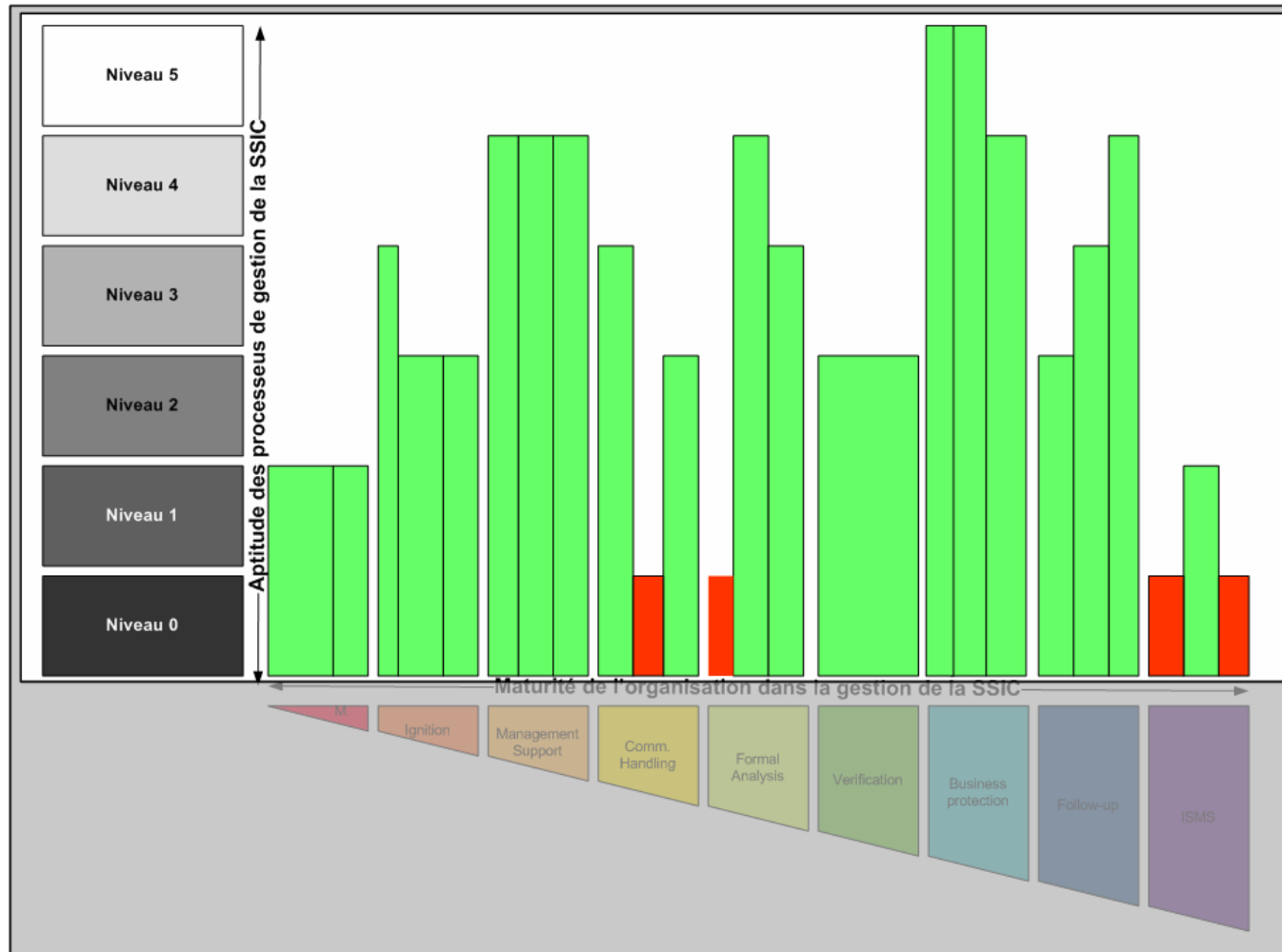


Figure 3 - Exemple de l'analyse de l'aptitude des processus de gestion de la SSIC

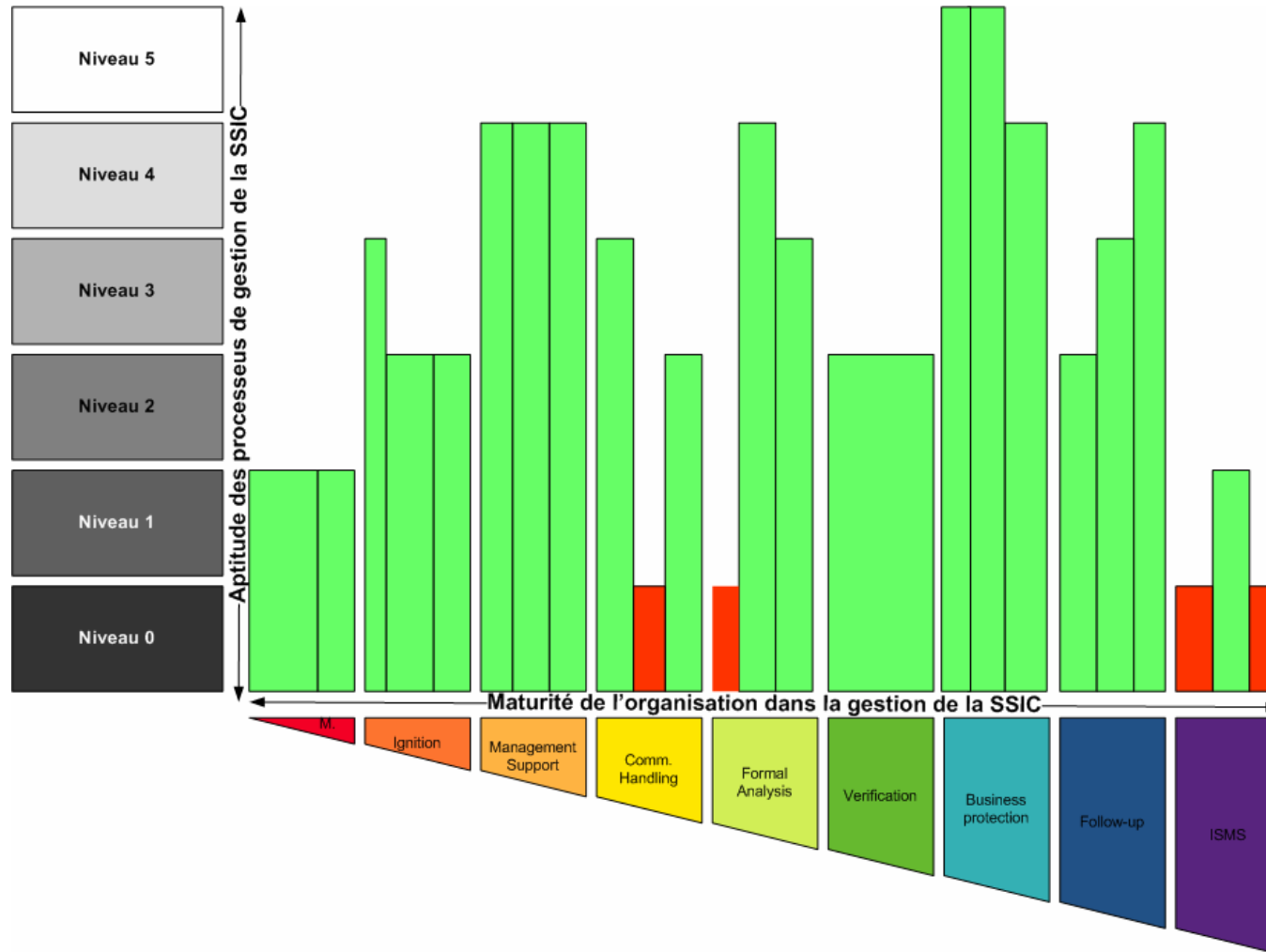


Figure 4 - Exemple de résultat d'une analyse combinée qualité et sécurité

VI Synthèse

Le modèle de maturité proposé ici constitue une échelle de mesure pour l'évaluation et la gestion progressive de la sécurité. Ce modèle traduit également la tentative de réunir non seulement les activités sécurité, mais également de dresser un pont entre le milieu de la sécurité et celui de la qualité, aussi bien au niveau du concept que des outils employés. La combinaison possible entre les deux vues et l'utilisation de l'ISO 15504 sur une base d'exigences proposé par la norme sécurité BS7799-2:2002 illustre cette perspective. La conséquence en est l'intégration progressive de la sécurité de l'information dans le champ des activités communes de l'organisation ; on peut alors parler de gouvernance.

Annexe

ENSEMBLE DE DOCUMENTATION

Afin de construire un système de gestion de la SSIC robuste, il est nécessaire à partir d'une certaine maturité visée, d'en documenter les spécifications, les tenants et les aboutissants.

Pour y parvenir, une documentation doit comporter les éléments suivants :

- Un dossier de projet consacré à la démarche sécurité
- La politique de sécurité
- Les résultats de l'analyse des risques
- Le plan de traitement des risques
- La liste des objectifs de contrôle
- Les procédures documentées

Des pratiques de gestion de cette documentation sont aussi indispensables pour disposer le plus facilement des informations pertinentes tout au long de leur cycle de vie. Cela concerne aussi bien la dénomination, l'emplacement, la version, le référencement, le cycle de validation de ces dits documents.

ABREVIATION DES PROCESSUS CONTENUS DANS LE PRM

- ADM Administration des contre-mesures
- ARI Analyse des risques
- CLE Conformité avec la législation
- CSE Coordonner la sécurité
- CVE Activités de veille
- EIS Amélioration de l'ISMS
- ESM Engagement et soutien du management
- GIN Gestion des incidents
- GRI Plan de gestion des risques
- PCO Plan communication
- PDC Plan de continuité
- PER Perspectives
- PSE Définition du plan de sécurité
- REV Revue
- SAF Mise en place des contre-mesures
- TDB Tableaux de bord
- TIE Considération des Tiers

TABLE DES FIGURES

| | |
|--|----|
| Figure 1 - Pyramide inversée des niveaux de maturité..... | 11 |
| Figure 2 - Exemple d'analyse de la maturité de l'organisation dans la gestion de la SSIC | 24 |
| Figure 3 - Exemple de l'analyse de l'aptitude des processus de gestion de la SSIC 25 | |
| Figure 4 - Exemple de résultat d'une analyse combinée qualité et sécurité | 26 |

TABLE DES TABLES

| | |
|---|---|
| Table 1- Deux philosophies divergentes... .. | 8 |
| Table 2 - ... et pourtant complémentaires... .. | 8 |
| Table 3 - ...utilisant un modèle adapté..... | 9 |

POUR POURSUIVRE

BSI, British Standard 7799-2 : 2002, Information Security Management Systems – Specification with guidance of use

CMMI Product Team, Capability Maturity Model® Integration (CMMISM), Version 1.1, Continuous Representation, *Carnegie Mellon Software Engineering Institute*, 2002

CMMI Product Team, Capability Maturity Model® Integration (CMMISM), Version 1.1, Staged Representation, *Carnegie Mellon Software Engineering Institute*, 2002

Code civil et code pénal du Luxembourg, disponibles sur <http://www.legilux.lu>

Chardonnet A. et Thibaudon D., Le guide du PDCA de Deming - Progrès continu et management, *Editions d'Organisation*, 2003

ISO, ISO 15504-2 : Information technology - Process assessment -- Part 2 : Performing an assessment, 2003

OCDE, Lignes directrices de l'OCDE régissant la sécurité des systèmes et réseaux d'information - Vers une culture de la sécurité, 25 juillet 2002

<http://www.oecd.org/dataoecd/16/22/15582260.pdf>

Picard M. et Lejeune V., Modélisation des processus ITIL à l'aide d'autres approches qualité, *Facultés Universitaires Notre-Dame de la Paix – Institut informatique de Namur*, 2004

Viral S., Costs and Benefits of using Smaller Assessment Models for Software Process Assessment and Improvement in Small Software Organizations, *Proceedings of the 5th International SPICE Conference on Process Assessment and Improvement*, 2005