LES DOSSIERS TECHNIQUES

LES METRIQUES DANS LE CADRE DE LA SERIE 27000

mai 2009

Groupe de Travail Série 27000

CLUB DE LA SECURITE DE L'INFORMATION FRANÇAIS

30, rue Pierre Sémard, 75009 PARIS

Tél. : +33 1 53 25 08 80 – Fax : +33 1 53 25 08 88 – e-mail : clusif@clusif.asso.fr
Web : http://www.clusif.asso.fr

REMERCIEMENTS

Le CLUSIF tient à mettre ici à l'honneur les personnes qui ont rendu possible la réalisation de ce document, tout particulièrement :

Nicolas ANDREU	**Devoteam**
Régis BOURDONNEC	**BNP Paribas Assurance**
Anne COAT	**SEKOIA SAS**
Henri CODRON	**SCHINDLER**
Jean-Marc DELTEIL	**France Telecom**
Frédéric HUYNH	**Ernst & Young**
François JOLIVET	**Société Générale**
Laurent MARECHAL	**Hapsis**
Fred MESSIKA	**SEKOIA SAS**
Gérard REMY	**Devoteam**
Paul RICHY	**France Telecom**
Hervé SCHAUER	**HSC**

ainsi que les personnes ayant participé à la relecture.

TABLE DES MATIERES

NOTE AUX LECTEURS

La langue anglaise comprend plusieurs mots « control », « measure », « measurement », « security measure » qui se traduisent généralement en français par le mot « mesure » ; il convient donc de préciser le périmètre et la définition retenue pour chacun de ces mots dans la suite du document, afin d'éviter les ambiguïtés de traduction. Ainsi, pour la suite, nous utilisons les correspondances suivantes :

- « Control » = **mesure de sécurité** : doit se comprendre comme un ensemble de dispositions à mettre en œuvre. Ce sont les « mesures à prendre » pour mettre en œuvre une politique de sécurité ; « Control » ne se rattache donc pas directement à la notion de métrique ;

- « Measure » = **valeur mesurée** : est défini comme « la valeur » de la mesure ; il s'agit donc d'une valeur quantitative, résultat de la « mesure de la mesure de sécurité » ;

- « Measurement » = **mesurage** : est explicité dans le glossaire (cf. §2.2), comme étant le « processus de mesurage » ; il s'agit à un niveau, soit élémentaire, soit plus global de la « mise en œuvre de métriques » ; « measurement » couvre donc la définition, le choix, le déploiement et l'évaluation d'indicateurs.

- « Security measure » = **mesure de sécurité** (voir la définition de « Control »).

Dans ce document, le terme « mesure » employé seul désigne le résultat de l'action de mesurer et ne correspond donc pas à « mesure de sécurité ».

1. INTRODUCTION

L'un des objectifs suivis lors de la mise en œuvre, au sein d'un organisme, d'une politique de sécurité du système d'information est d'apporter ou de renforcer la confiance en celui-ci. Cette confiance traduit l'une des exigences des différents acteurs (internautes, clients, fournisseurs, actionnaires, …) ou de l'organisme lui-même (entreprise, administration, ONG, tiers de confiance, ...) lors d'une transaction commerciale, du développement de son activité, pour la conservation de données numériques, …

La notion de « niveau de sécurité » est souvent utilisée, par abus de langage, pour « étalonner » cette confiance. Cela pour signifier que l'on veut être « sûr » de son SI, ou pour « garantir » que des mesures de sécurité ont été mises en œuvre et qu'elles permettent de réduire l'exposition aux risques à un niveau « acceptable ».

L'appréciation de l'atteinte des objectifs de sécurité ainsi que la pondération à affecter aux différentes thématiques de sécurité (plan de continuité, sécurité physique des infrastructures, gestion des identités, …) demeurent des questions d'actualité. Il est difficile d'indiquer parmi différentes mesures de sécurité déployées celles qui auront le plus de valeur ajoutée sur le niveau de protection du système d'information.

La confiance accordée à la sécurité du système d'information se mesure notamment par rapport à une politique, constituée par des processus et des objectifs, suivant une démarche formalisée pour les atteindre. Le respect de ces conditions permet de se positionner dans une perspective de maîtrise du *système de management de la sécurité de l'information (SMSI)* ou d'évaluation des mesures de sécurité mises en place.

La norme ISO/IEC 27004 fournit une réponse structurée et normalisée pour « mesurer » la performance d'un SMSI dans le cadre de l'ISO/IEC 27001:2002.

1.1 Objectif de ce document

Lors de ses précédents travaux sur les normes de la série 27000, le CLUSIF a développé de quelle manière :

- la norme ISO/IEC 27001:2005 permet le Management de la sécurité de l'information par une approche normative ;
- la norme ISO/IEC 27002:2005 fournit les mesures de sécurité permettant de répondre à ses exigences.

L'objectif de ce document est de présenter au lecteur, des concepts généraux pouvant être utilisés pour définir des indicateurs et une métrique permettant les « mesurages » (voir définition au §2.2) du système de management de la sécurité de l'information.

Ce document ne porte pas de jugement sur la qualité de la norme. Ce n'est pas non plus un document sur la métrologie ou l'élaboration de tableaux de bord. Il traite des fondamentaux sur les métriques et leurs utilisations, afin de mieux appréhender le contenu de la norme ISO/IEC 27004.

Enfin, les annexes proposeront différents exemples de métriques selon l'ISO/IEC 27004 qui permettraient le mesurage d'un SMSI normé par l'ISO/IEC 27001:2005.

1.2 Lectorat

Les documents du CLUSIF sont généralement à destination des RSSI et des DSI.

L'élargissement du périmètre au mesurage de l'ensemble du SMSI nous incite à proposer une cible sensiblement plus large incluant tous les professionnels de la sécurité de l'information, mais aussi toutes les entités de contrôle permanent ou de gestion des risques.

Comme tout texte, l'utilité de la norme doit être évaluée en fonction du contexte de mise en œuvre. Ce document ayant été rédigé plus particulièrement pour un public de « non-initiés » afin de leur permettre de mieux appréhender le contenu de la norme, les personnes au fait de cette dernière n'y trouveront peut être pas de développement nouveau.

2. LES METRIQUES

2.1 Panorama des référentiels et des bonnes pratiques

La norme ISO/IEC 27002:2005, connue précédemment sous la référence ISO/IEC 17799:2005 a pour titre « *Code of practice for information security management* ». Elle met l'accent sur le fait que, désormais, l'information est une ressource essentielle de l'entreprise ; c'est-à-dire que l'information, au même titre que d'autres actifs, doit être prise en considération, évaluée et protégée.

La sécurité de l'information vise entre autres à garantir la continuité de l'activité, à réduire les risques, à optimiser le retour sur investissements ainsi que les opportunités d'action pour l'organisme.

Cette norme traduit une évolution tendancielle des normes traitant de la sécurité de l'information. Au départ, il y a une quinzaine d'années, ces normes étaient plutôt techniques et contenaient surtout des prescriptions relatives aux systèmes ou aux réseaux informatiques.

Vers le milieu des années 90, des travaux d'origine britannique ont conduit à élaborer des documents dont le champ s'étendait aux systèmes d'information et orientés vers les responsabilités managériales et l'organisation des entreprises.

Le plus connu de ces documents est le standard britannique BS 7799 dont la partie 1 (*Code of practice for information security management*) a servi de base à l'ISO/IEC 27002 (anciennement ISO/IEC 17799), et la partie 2 a servi de base à l'ISO/IEC 27001, dans laquelle on trouve la notion de SMSI (*Système de Management de la Sécurité de l'Information).*

Lors d'une réunion de l'ISO, il a été décidé de regrouper les principales normes traitant du SMSI dans une « série ISO/IEC 27000 » un peu comme la qualité fait l'objet de la « série ISO 9000 » ou l'environnement de la « série ISO 14000 ». Il est d'ailleurs à noter que ces trois familles de normes sont cohérentes entre elles quant à l'approche managériale et organisationnelle des thèmes traités. Il est prévu de disposer à terme des normes suivantes (liste non limitative) :

- ISO/IEC 27000, *Principles and Vocabulary*,
- ISO/IEC 27001, *Information Security Management Systems – Requirements*, basée sur la BS 7799-2 et orientée vers la certification,
- ISO/IEC 27002, *Code of practice for Information Security Managemen*t, anciennement ISO/IEC 17799,
- ISO/IEC 27003, *ISMS Implementation*,
- ISO/IEC 27004, *ISMS, Measurements and metrics*,
- ISO/IEC 27005, *ISMS, Information security risk management*,
- ISO/IEC 27006, *Information technology — Security techniques — Requirements for bodies providing audit and certification of information security management systems.*

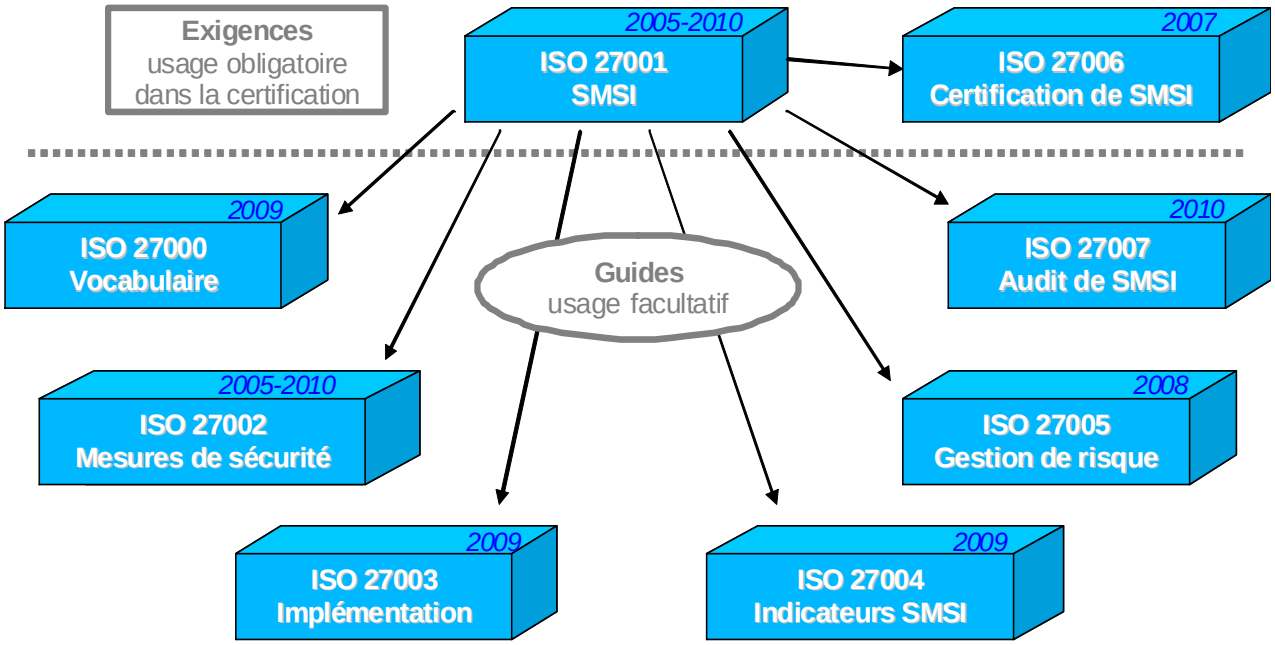

Schéma 1 : La série ISO/IEC 27000

Bien sûr, d'autres normes techniques continueront de traiter de la sécurité des systèmes d'informations. En particulier, nous pouvons mentionner :

- ISO/IEC 27031, *Specification for ICT Readiness for Business Continuity*,
- ISO/IEC 27032, *Guidelines for Cybersecurity*,
- ISO/IEC 27033, de 1 à 8, *IT network security* (ex : ISO/IEC 18028),
- ISO/IEC 27034, *Guidelines for Application Security*,
- ISO/IEC 27035, *Information Security Incident Management.*
- ISO/IEC 18043, S*election, deployment and operation of intrusion detection systems (IDS).*

D'autres référentiels, eux aussi en cours d'évolution, sont susceptibles d'être utilisés pour améliorer la sécurité de l'information. Ils peuvent ainsi se trouver en concurrence avec tout ou partie des normes précitées. Ils peuvent aussi introduire de nouvelles contraintes qui seront à prendre en compte dans leur mise en œuvre.

Le plus connu est le CoBIT (Control Objectives of Information and related Technology), élaboré par l'ISACA (*Information Systems Audit and Control Association*). Il convient également de mentionner les documents émanant du COSO (*Committee of Sponsoring Organisations of the Treadway Commission*) ou de différents organismes gouvernementaux (NIST aux USA, DTI au Royaume Uni, …).

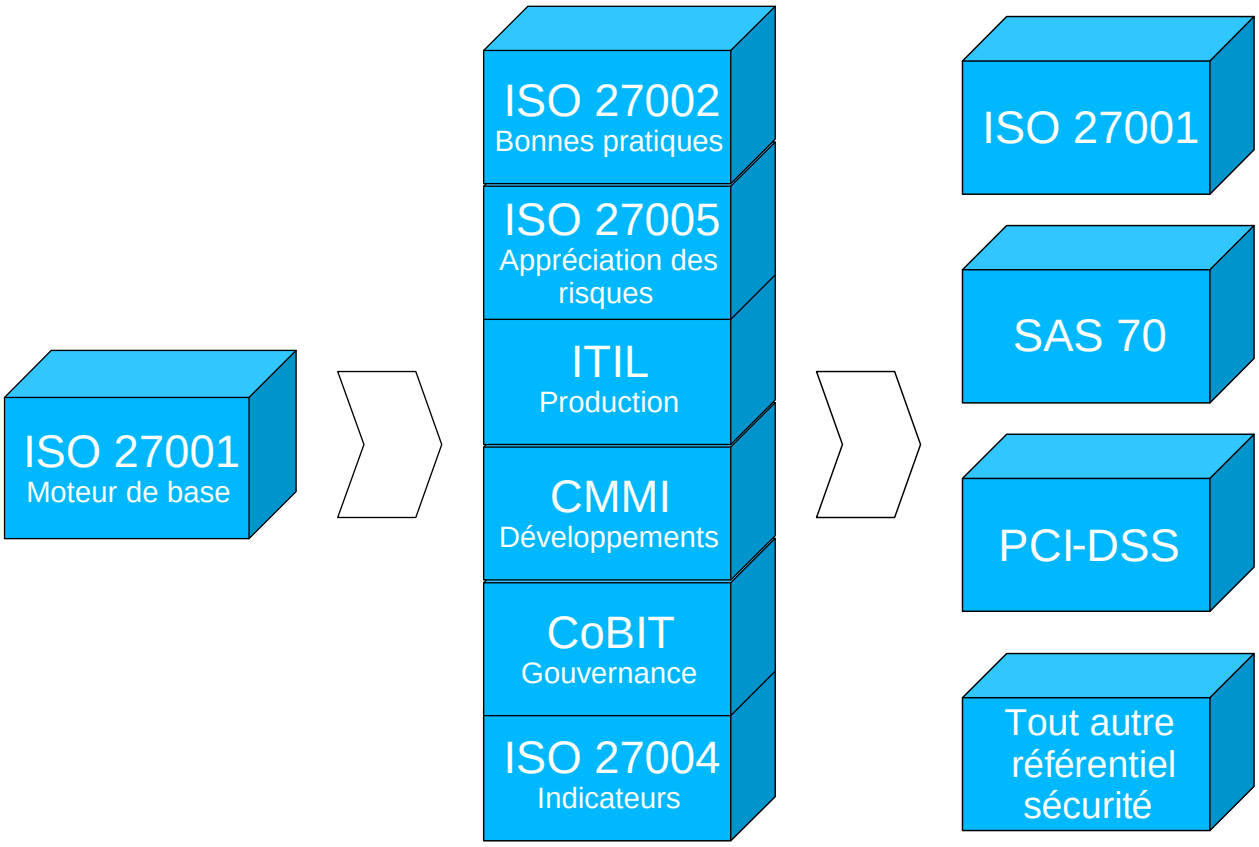

Schéma 2 : La série ISO/IEC 27000 et les autres référentiels

De la même façon, les lois et les règlements concernant la sécurité de l'information (informations nominatives, gestion de l'identité, rétention de données, chiffrement, …) sont actuellement en évolution dans la plupart des pays.

De nouvelles conditions de traitement, de conservation ou de destruction des informations sont ainsi à mettre en œuvre de façon impérative et de façon d'autant plus complexe que les mesures de sécurité peuvent varier d'un pays à l'autre.

Des impératifs législatifs ou sectoriels peuvent aussi voir le jour et entraîner des conséquences importantes. Par exemple la loi Sarbanes-Oxley Act pour les entreprises cotées sur les marchés américains, la Loi sur la Sécurité Financière pour les entreprises françaises, Bâle II pour les établissements financiers ou Solvency II pour les assurances.

2.2 Terminologie

Le terme « métrique » n'existe pas dans la langue française au sens où il est utilisé dans ce document.

Le terme anglais « metrics » (a system of related measures that facilitates the quantification of some particular characteristic) est utilisé pour métrologie, parfois « traduit » par métrique.

Pour mémoire, la métrologie est la science qui s'intéresse aux côtés théoriques et pratiques de la mesure, dans tous les domaines de la science et de la technologie. Plus spécifiquement, la métrologie touche l'utilisation des unités, la réalisation des étalons, les méthodes, les techniques et les appareils de mesure, ainsi que la précision obtenue.

Les différentes normes en rapport avec le sujet fournissent les définitions suivantes :

- Attribut : propriété ou caractéristique d'un objet qui peut être distingué quantitativement ou qualitativement par des moyens humains ou automatiques [ISO/IEC 15939:2007]

- Mesurage : processus d'obtention d'information relative à l'efficacité d'un SMSI et de mesures de sécurité, à l'aide d'une méthode d'évaluation, d'une fonction d'évaluation, d'un modèle analytique et de critères de décision [ISO/IEC 27004]

- Indicateur : résultat de l'application d'un modèle analytique à une ou plusieurs variables en relation avec les critères de décision ou un besoin d'information. [ISO/IEC 27004]

Un indicateur est la base de l'analyse et de la prise de décision.

Compléments aux définitions proposées dans ce document :

- Métrique : ensemble d'éléments permettant de fournir une évaluation qualitative ou quantitative représentative d'une situation.

- Indicateur : donnée objective qui présente une situation du strict point de vue quantitatif. Un indicateur est pertinent s'il est directement relié à une zone d'action (il indique où il faut agir). Les indicateurs peuvent être regroupés dans un tableau de bord, outil de synthèse et de visualisation des situations décrites.

2.3 Positionnement des métriques dans le modèle de fonctionnement

La figure ci-dessous positionne les termes « attribut », « métrique » et « indicateur ».

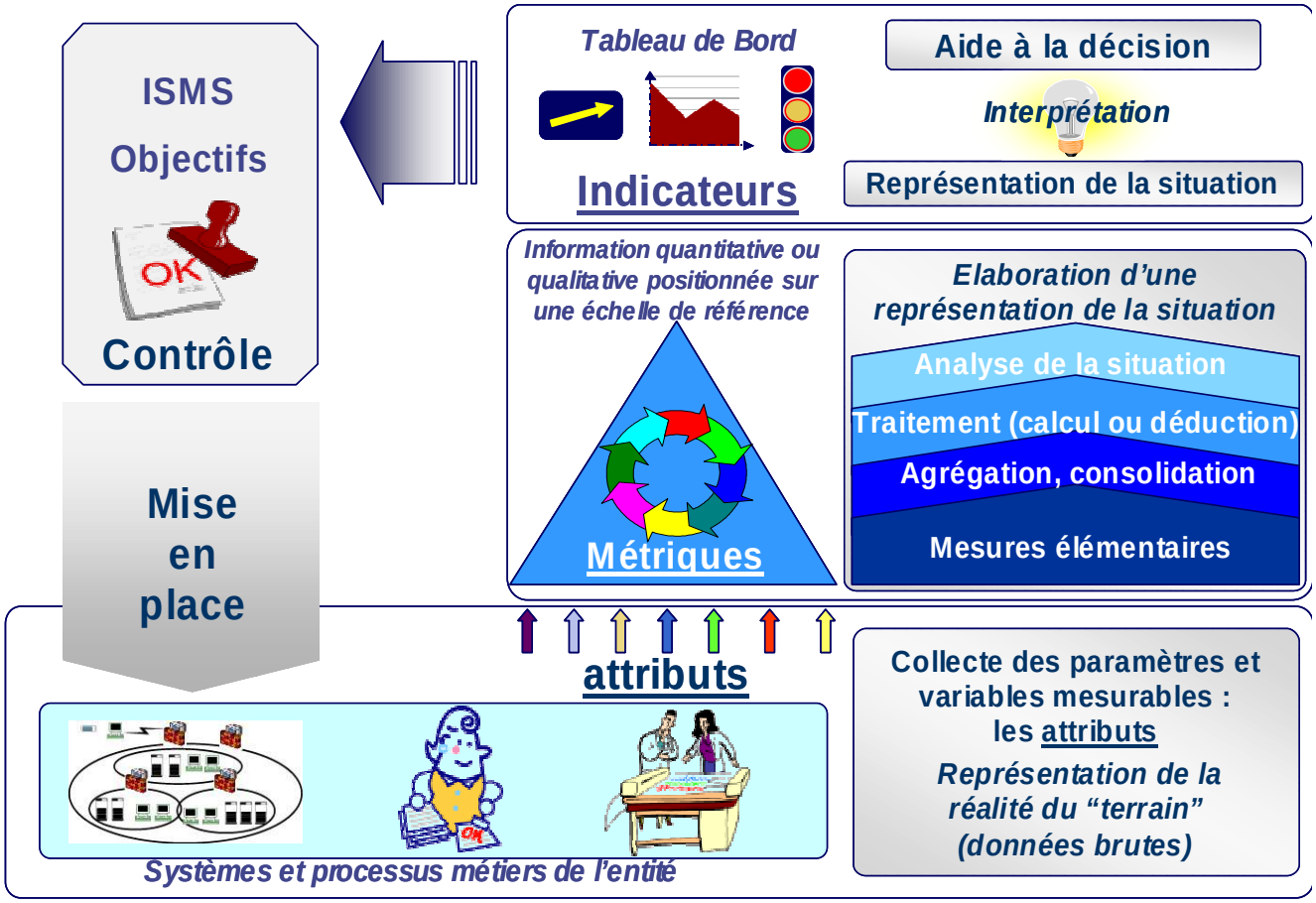

Schéma 3 : Représentation d'après le document ISO/IEC 27004

Exemple dans le domaine des antivirus :

- Nombre de postes équipés d'un antivirus : **attribut**
- Pourcentage du nombre de postes équipés sur le total : **métrique**
- Nombre de postes équipés d'un antivirus dont l'antivirus a été mis à jour : **attribut**
- Pourcentage de postes dont l'antivirus a été mis à jour : **métrique**

A partir de l'exemple ci-dessus, en regroupant les deux métriques nous pouvons constituer un **indicateur** représentant à la fois le niveau de protection viral des postes de travail et la maîtrise du processus antiviral sur ces postes.

Les indicateurs, intimement liés à la situation que nous voulons représenter peuvent être de nature différente et avoir des finalités également différentes :

- constater une situation dans le domaine que l'on veut observer ;
- mesurer l'écart entre le niveau existant et le niveau de l'objectif défini ;
- suivre l'évolution des domaines gérés et analysés ;
- anticiper et/ou déclencher la mise en œuvre de plans d'actions de sécurité (à partir du franchissement d'un seuil) ;
- communiquer à partir de données analysées ;
- piloter les projets ;
- apprécier le respect des lois et réglementations ;
- auditer.

Dans le contexte de la mise en œuvre d'un SMSI et du respect du principe de la Roue de Deming (cycle PDCA), les critères de choix des indicateurs doivent intégrer le souci d'amélioration permanente de la sécurité par la vérification de l'efficacité des mesures de sécurité validées et déployées. Ainsi, il est toujours souhaitable d'avoir en mémoire que l'objectif d'un indicateur de sécurité dans le SMSI est d'évaluer l'efficacité des mesures de sécurité.

Dans la suite du document, le choix a été fait d'illustrer uniquement les méthodes de mise en œuvre d'indicateurs pour les SMSI. En effet, le suivi de l'efficacité de tout système de management est réalisé à partir de ces indicateurs (cf. schéma 3).

2.4 Éléments pour la mise en œuvre des indicateurs

Afin de satisfaire les objectifs assignés, les indicateurs doivent respecter des conditions particulières et être dotés de qualités spécifiques, notamment :

- être issus des objectifs retenus dans la politique de sécurité ;
- être aisément quantifiables (construits à partir d'informations ou de processus générant des informations quantifiables) afin de permettre des comparaisons (entre systèmes ou entre périodes). Il s'agit le plus souvent de pourcentage, de taux, de ratio, de moyenne et/ou de nombres « bruts » ;
- les informations nécessaires à l'élaboration de la mesure doivent être faciles à obtenir et/ou collecter. En effet, il faut s'assurer que les ressources mises en œuvre pour obtenir les données ne sont pas disproportionnées par rapport à celles concourant à la réalisation du processus mesuré ;
- s'appuyer sur des processus « stables » et aisément « reproductibles » ;
- permettre la mesure des évolutions suite à des actions correctives ;
- être fiables sur la durée et autoriser une analyse des écarts.

Ces caractéristiques sont regroupées dans certaines démarches sous l'acronyme « SMART » qui signifie :

- Specific : il correspond à ce qui est analysé et met en avant la spécificité de l'attribut.
- Measurable : il peut être mesuré et cette mesure est objective.
- Attainable : il est obtenu dans des conditions satisfaisantes de coût et de délai.
- Repeatable : sa mesure est reproductible.
- Time dependent : la mesure dépend de la fenêtre de temps utilisée.

Les caractéristiques de la mesure définies dans l'Annexe A de l'actuel projet de norme ISO/IEC 27004 doivent être définies pour chaque indicateur.

2.5 Exemples d'indicateurs

Quelques exemples d'indicateurs sont donnés ci-après. La liste fournie n'est pas exhaustive. Il est intéressant de constater que certains indicateurs sont de nature opérationnelle ou stratégique, voire opérationnelle et stratégique.

Contrôle d'accès

- pourcentage d'utilisateurs dont le mot de passe respecte les principes de construction ;
- pourcentage de systèmes accessibles depuis l'extérieur et comprenant un IDS à jour.

Contrôle des codes malveillants :

- nombre annuel d'attaques réussies par défaut de mise à jour de la base virale ;
- délai de retour à la normale sur attaque virale ;
- fréquence de mise à jour de la base antivirus ;
- fréquence d'évaluation de la conformité des politiques antivirales « locales » avec la politique « globale ».

Mise en œuvre du SMSI :

- pourcentage de déclinaisons des principes de la politique de sécurité de l'organisme en procédures opérationnelles ;
- nombre mensuel d'incidents de sécurité non résolus ;
- pourcentage de comités de pilotage de sécurité tenus en accord avec le planning ;
- pourcentage d'actions correctives non menées à terme.

Maîtrise des dépenses :

- dépenses liées à la sécurité selon différents critères : nombre d'alertes, d'incidents, etc.

Formation :

- pourcentage du budget global de formation consacré à la sécurité des systèmes d'information ;
- pourcentage de participants en fonction de la population cible à des sessions relatives à la sécurité des systèmes d'information ;
- taux de fréquentation des formations aux procédures d'alerte par les personnes clés des cellules de crise.

Sécurité des logiciels / applications :

- nombre de correctifs de sécurité validés après analyse ;
- taux de correctifs de sécurité validés mis en œuvre dans les délais prévus.

Sécurité réseau :

- nombre d'audits et de tests de vulnérabilité réalisés sur la période.

Disponibilité des services :

- taux de disponibilité DNS, accès internet, messagerie.

3. LES DIFFERENTS USAGES DES INDICATEURS

3.1 Évaluer

Ces indicateurs peuvent être répartis dans les grandes familles suivantes :

- Les indicateurs « de conformité » décrivent le niveau d'exigence souhaité (ou constaté) sur une mesure de sécurité. Par exemple en ce qui concerne la mesure de sécurité « Réalisation de sauvegardes », un indicateur de conformité de sécurité peut être la fréquence des sauvegardes ou le ratio du nombre de bandes externalisées par rapport au nombre total de bandes ;
- Les indicateurs « d'efficacité » décrivent l'état du fonctionnement de la mesure de sécurité. Sur le même exemple de la « Réalisation de sauvegardes », un nombre élevé de tests de restaurations défectueux peut démontrer un mauvais fonctionnement des sauvegardes ;
- Les indicateurs « d'efficience » visent à rapprocher l'efficacité de la mesure de sécurité au regard de l'importance des moyens mis en œuvre.

3.2 Piloter

Toute activité (production, projet, processus, etc.) implique la détermination d'indicateurs de pilotage. Ces derniers permettent :

- d'apprécier l'avancement correct du projet ;
- d'évaluer une situation ;
- de détecter un risque ;
- de déclencher une alerte.

Le choix des indicateurs peut dépendre des objectifs de l'activité (coûts, délais, performance, etc.) mais aussi être lié à des processus transverses (management, support, etc.).

Nous pourrons ainsi avoir les indicateurs suivants, sur différentes échelles de temps, année, mois, semaine, jour :

- nombre de machines infectées par des virus / nombre de machines ;
- nombre de messages infectés par des virus / nombre de messages ;
- nombre de machines à jour / nombre de machines ;
- temps moyen et maximum de mise à jour du parc ;
- nombre d'attaques virales identifiées / bloquées / exécutées ;
- impact de ses attaques en heures de travail perdues / financier ;
- raison des infections : mise à jour non effectuée / sécurité non appliquée / malveillance… ;
- variation du taux d'infection et tentatives d'infection sur les 12 derniers mois ;
- etc.

Ces indicateurs peuvent aussi être élémentaires ou plus synthétiques. Par exemple, l'agrégation de certains indicateurs informatiques avec les indicateurs économiques. Le « Ratio du nombre annuel d'accords de confidentialités (NDA – Non disclosure agreement) signés par rapport au nombre de prestataires présents dans l'organisme » en est un exemple.

3.3 Communiquer

Des indicateurs sont aussi utilisés pour communiquer, en interne ou en externe. Leur nature sera différente en fonction des acteurs visés, et de leur objectif de communication (sensibiliser, faire passer des idées, justifier…).

Par exemple pour communiquer autour de la lutte antivirale :

- nombre d'heures de travail perdues suite à une attaque virale ;
- variation du taux d'infection sur les douze derniers mois (justification du budget) ;
- nombre d'attaques virales provenant d'un support externe.

3.4 S'autoévaluer

Cette évaluation peut être réalisée en interne par l'équipe en charge de la fonction comme par l'équipe d'audit ou de contrôle interne.

Elle se situe par rapport à un référentiel interne ou externe ou par rapport à un objectif arbitraire, ou résultant d'une expérience passée et déjà mesurée.

Les indicateurs cités comme exemple dans les paragraphes précédents peuvent notamment servir dans le cadre d'une autoévaluation.

3.5 Contribuer à l'obtention d'une certification

Ces indicateurs servent à :

- apprécier l'avancement dans le processus de certification ;
- obtenir la certification ;
- et surtout la conserver.

Sans être obligatoire pour l'obtention de la certification ISO/IEC 27001:2005, la mise en place d'indicateurs simplifie grandement le cheminement vers celle-ci.

3.6 Répondre à un audit

Les indicateurs servent à informer l'auditeur, à justifier des mesures de sécurité mises en place et des correctifs en cours.

Les indicateurs présentés lors d'audits contribuent à l'analyse de risque et s'apprécient par rapport à un référentiel externe.

4. LES TRAVAUX NORMATIFS EN COURS (ISO/IEC 27004)

Ce document a été rédigé alors que la norme ISO/IEC 27004 n'était pas stabilisée (version CD); il est toutefois permis de penser que l'intérêt du document justifie les travaux entrepris ci-après, sous réserve de possibles évolutions.

Ce projet de norme, au sein de la série 27000, constitue un guide [à usage facultatif], de « Mesurage et métriques », dans le cadre d'un SMSI (Système de Management de la Sécurité de l'Information) tel que défini dans l'ISO/IEC 27001:2005.

Les domaines suivants sont abordés :

- présentation du processus de mesurage ;
- rôles et responsabilités ;
- conception des indicateurs ;
- production et mise en forme des indicateurs ;
- analyse et reporting ;
- amélioration du processus de mesurage.

Une première annexe présente un modèle commenté d'une fiche d'indicateur (cf. Annexe A). La seconde annexe présente plusieurs exemples d'attributs, de métriques ou d'indicateurs (cf. Annexe B).

4.1 Concepts de métriques

Un processus de mesure a pour but de vérifier que les objectifs de sécurité, fondés notamment sur l'analyse de risque et la conformité aux dispositions légales et réglementaires, sont atteints.

Il se compose de phases de collecte d'informations et d'analyse. Par comparaison à des critères de décision, ces phases permettent l'obtention d'informations de sécurité et l'amélioration continue du management de la sécurité.

Les mesures peuvent être élémentaires ou dérivées :

- une mesure **élémentaire**[1] est la valeur d'un « attribut » obtenue par une méthode de calcul ;
- une mesure **dérivée** est la valeur issue d'un traitement d'une ou plusieurs mesures élémentaires.

Pour chaque type de mesure (élémentaire ou dérivée) il convient de faire en sorte que des objectifs de conformité ou de performance soient mis en évidence.

Le modèle du processus de mesure proposé comprend un processus de remontée de mesures élémentaires et de mesures dérivées qui contribuent à la fabrication d'indicateurs, lesquels seront comparés individuellement à leur critère de décision. L'efficacité du système

1 Une mesure élémentaire peut, dans certains cas, correspondre directement à un indicateur.

de management s'apprécie en comparant les résultats issus des mesures effectuées avec leurs objectifs initiaux.

Dans le projet de norme, les précisions suivantes sont apportées :

- les objectifs du processus de mesure sont clairement établis (évaluer, fournir des données, faciliter l'évolution, communiquer). En revanche le périmètre sur lequel s'applique ce processus ainsi que la méthodologie d'implémentation restent à l'initiative de chacun ;
- l'implication du management dans le processus de mesure est soulignée notamment sur son engagement, ses responsabilités et les ressources à mettre en œuvre ;
- les différents rôles qui devraient être assignés par le Management concernant le processus de mesure sont précisés : le fournisseur, le client, le collecteur, le communicateur, le ré-examinateur (cf. définitions dans l'annexe A du présent document). Ces différents rôles devront faire l'objet de procédures d'habilitation prenant en compte les contraintes de séparation des tâches et les compétences techniques nécessaires.

4.2 Concevoir des métriques

Des métriques doivent être créés pour évaluer l'efficacité du SMSI, contrôler l'atteinte des objectifs, identifier, valider et améliorer les mesures de sécurité spécifiques.

Pour cela, il faut pour chaque métrique, à partir d'une analyse de risque et de l'état initial :

- identifier et choisir des objectifs ;
- documenter et planifier l'activité de mesurage (l'annexe A du présent document présente un modèle de fiche sur ce thème) en particulier concernant la méthode de collecte, de stockage, d'archivage, de vérification et d'analyse des données ainsi que la mise en place du processus de mesurage ;
- définir les principaux acteurs et les ressources nécessaires ;
- s'assurer de la pertinence des mesurages qui devraient vérifier les critères SMART (Specific, Measurable, Attainable, Repeatable, Time dependant).

4.3 Mettre en place des métriques

La mise en place permanente de la collecte, de la conservation et de l'analyse des données a pour but d'assurer la compréhension et l'amélioration du SMSI. Ce processus doit accompagner les évolutions du SMSI.

Cette rubrique, dans le projet de norme, constitue un guide pratique opérationnel qui précise les conditions de :

- collecte des données (en spécifiant la date, l'heure, le propriétaire…) ;
- validation ;
- traitement ;
- diffusion ;
- conservation.

Il importe que les résultats des indicateurs servent à évaluer l'efficacité des dispositifs de sécurité (de prévention, détection, correction ou récupération) en place. Dans un second temps, cette base d'indicateurs constituée permettra de soutenir un processus de décision dans le choix de nouveaux dispositifs.

4.4 Utiliser, communiquer et améliorer les métriques

L'analyse des données et leur interprétation consistent à les rapprocher des critères de décision préalablement définis (Annexe A).

Le but de l'analyse est de pouvoir identifier les écarts entre la performance attendue et celle réalisée. Les causes de non-conformité et de mauvaise performance pourront être ainsi identifiées en fonction des dispositifs de sécurité qui :

- ne sont pas opérationnels ;
- sont implémentés mais ne fonctionnement pas correctement ;
- sont implémentés, fonctionnent correctement, mais ne couvrent pas les menaces estimées ;
- sont implémentés, fonctionnent correctement, mais toutes les menaces ne sont pas couvertes.

Les conclusions des analyses devraient être revues par toutes les parties prenantes – dans le sens « *stakeholders* » – pour assurer la bonne interprétation de la donnée. A cette fin, les résultats des analyses devraient être suffisamment documentés.

La consolidation de ces résultats devra intervenir dans des tableaux de bord pour une communication à qui de droit.

Les mesures peuvent être utilisées à diverses fins :

- évaluer l'efficacité des dispositifs de sécurité ;
- critiquer les appréciations et les traitements des risques ;
- démontrer les progrès ;
- se comparer au sein ou entre organisations.

4.5 Améliorer le processus de mesure

L'efficacité du processus de mesure doit être examinée périodiquement afin de l'améliorer. Néanmoins, les données de base doivent faire l'objet de sauvegardes régulières et pérennes afin de pouvoir recalculer les métriques en fonction de leurs différentes évolutions.

Des évolutions peuvent être envisagées quand l'organisation introduit de nouveaux objectifs de mesure, points de mesure, de nouvelles méthodes ou fonctions de mesure.

Le processus de mesure devrait être évalué en termes d'utilité et réexaminé à chaque fois que l'organisation change. Il importe de s'assurer que les mesures reflètent un état à jour de la sécurité et de vérifier que les données sous-jacentes sont encore valides. Il est également important de valider la pertinence des hypothèses.

Il s'agit aussi d'évaluer l'utilité de la mesure, et le coût du processus de mesure afin de déterminer la pertinence de sa modification ou de sa suppression.

5. CONCLUSION

L'ISO/IEC 27001:2005 insiste sur l'importance de mesurer l'efficacité des processus du SMSI, des mesures de sécurité mises en œuvre et du processus de mesurage lui-même[2] .

Cependant, cette norme ne précise pas comment mesurer cette efficacité. Elle se contente d'indiquer qu'une méthode est à définir.

A cette fin, le présent document apporte un éclairage aux RSSI, auditeurs internes, acteurs du contrôle permanent et managers, dans la définition et la mise en œuvre des indicateurs adaptés à leurs exigences selon des processus qui devraient figurer dans la norme ISO/IEC 27004.

L'ISO/IEC 27004 est un guide qui complétera l'ISO/IEC 27001:2005 en fournissant des lignes directrices et des conseils sur :

- la conception,
- la mise en œuvre,
- l'analyse et la communication des résultats,
- l'amélioration du processus de mesurage d'un SMSI.

Cette future norme devrait être publiée prochainement. La série ISO/IEC 27000 a été complétée de l'ISO/IEC 27005:2008 et de l'ISO/IEC 27003 (prévue en 2009) qui traitent respectivement de la gestion du risque et de la mise en œuvre d'un SMSI.

[2] cf. clauses 0.2.c, 0.2.d, 4.2.2.d, 4.2.3.c, 4.3.1.g, 7.2.f et 7.3.e

ANNEXE A : FICHE DESCRIPTIVE

Modèle de fiche descriptive d'une mesure

Cette fiche est inspirée de l'ISO/IEC FCD 27004.

Identification de la mesure	
Nom de la mesure	Nom de la mesure
Identifiant de la mesure	Identifiant numérique unique spécifique à l'organisme.
Objectif de la mesure	Décrit l'objectif de la mesure de sécurité à mettre ou déjà mise en œuvre (référence à la mesure de sécurité de l'annexe A de la norme ISO 27001).
Mesure de sécurité (1)	Facultatif : Décrit la mesure de sécurité à mettre ou déjà mise en œuvre (référence à la mesure de sécurité de l'annexe A de la norme ISO 27001).
Mesure de sécurité (2)	Facultatif : Décrit d'autres mesures de sécurité (à mettre ou déjà mise en œuvre) faisant l'objet, le cas échéant, de la même mesure (référence aux mesures de sécurité de l'annexe A de la norme ISO 27001).
Objectif de la mesure	Définit le but de la mesure.
Ré examinateur	Personne ou unité organisationnelle qui examine et valide que les critères d'évaluation de la mesure sont appropriés pour vérifier l'efficacité des mesures de sécurité et des processus du SMSI.
Objets du mesurage et attributs	
Objet du mesurage	Objet qui doit être mesuré et qui est caractérisé par la mesurabilité de ses attributs. Les objets peuvent comprendre des processus, des systèmes ou des composants de systèmes.
Attributs	Propriété ou caractéristique d'un objet qui peut être distinguée quantitativement ou qualitativement par des moyens humains ou automatiques.
Spécification des mesures élémentaires (pour chaque mesure élémentaire [2…n])	
Mesures élémentaires	Une mesure élémentaire est définie en fonction d'un attribut et de la méthode de mesurage spécifiée pour le quantifier (par exemple, le nombre de personnel formé, le nombre de sites, le coût cumulé à ce jour). Au moment où la donnée est collectée, une valeur est affectée à une mesure élémentaire.
Méthodes de mesurage	Suite logique d'opérations qui permettent de quantifier un attribut selon une échelle.
Echelle	Ensemble ordonné de valeurs ou de catégories utilisées pour la mesure élémentaire.
Spécification de la mesure dérivée	
Mesure dérivée	Une mesure dérivée est la valeur issue d'un traitement d'une ou plusieurs mesures élémentaires.
Fonction de mesurage	Suite logique d'opérations qui permettent de calculer la mesure dérivée. Pour les mesures dérivées, la fonction par laquelle les mesures dérivées, fondées sur des mesures élémentaires correspondantes et la précision cumulative résultante, sont agrégées.
Echelle	Ensemble ordonné de valeurs ou de catégories utilisées pour la mesure dérivée.
Spécification de l'indicateur	
Description d'indicateur et exemple	Présentation d'une ou plusieurs mesures (élémentaires ou dérivées) qui fournit une estimation ou une évaluation d'attributs spécifiés résultant d'un modèle analytique en ce qui concerne des besoins de l'information définis. Un indicateur est souvent présenté à l'aide d'un graphique ou d'un diagramme. Inclure un croquis de l'indicateur.
Modèle analytique	Algorithme ou calcul combinant une ou plusieurs mesures élémentaires et/ou dérivées avec les critères de décision associés.

Critère de décision	Seuil, cible, ou modèle utilisé pour déterminer la nécessité d'une action ou un complément d'enquête, ou pour décrire le niveau de confiance dans un résultat donné.
Interprétation d'indicateur	Description de la façon dont l'indicateur exemple (voir la figure exemple dans la description de l'indicateur) devrait être interprété.
Effets / impact	Définition des effets et de l'impact issu des résultats obtenus par la mesure.
Causes d'écart	Définition des causes possibles à l'origine d'écarts des résultats.
Valeurs positives	Déclaration expliquant si les valeurs en « croissance » indiquent des tendances positives (bon résultat) ou si les valeurs en « décroissance » doivent être considérées comme des tendances positives.
Format de restitution	Le format de la restitution devrait être précisé et documenté. Il décrit les observations que l'organisation ou le propriétaire de l'information peut vouloir sur l'enregistrement. Les formats de rapport décriront visuellement les mesures et fourniront une explication verbale des indicateurs. Ils devraient être personnalisés en fonction du « client de l'information » (*ce terme est défini ci-après*).
Procédure de collecte des données **Complétez cette section pour chaque mesure élémentaire**	
Fréquence de collecte des données	Fréquence à laquelle les données sont collectées.
Fournisseur de l'information	Personne ou unité organisationnelle qui détient l'information pour créer les mesures élémentaires. *Celui qui va contribuer à la métrique / produire l'information pour le calcul de la métrique.*
Collecteur de l'information	Personne ou unité organisationnelle en charge de collecter, enregistrer et stocker les informations. *Celui qui va obtenir la métrique.*
Outils utilisés dans la collecte des données	Liste les outils utilisés dans la collecte des données (par exemple, un scanner de vulnérabilité).
Conservation des données collectées	Liste les outils où les données sont conservées après avoir été collectées (par exemple, une base de données).
Date de collecte	Date à laquelle la donnée devrait être obtenue.
Procédure d'enregistrement des données	Définit la procédure d'enregistrement des données (lien vers la procédure correspondante).
Validité de la mesure	Date de révision (date d'expiration ou de validité de renouvellement) de la mesure.
Période d'analyse	Définit la période mesurée.
Procédure d'analyse des données (pour chaque Indicateur)	
Fréquence de la restitution des données	Fréquence à laquelle les données sont restituées (cette fréquence peut être inférieure à celle de collecte).
Communicateur de l'information	Personne ou unité organisationnelle responsable de l'analyse de l'information et de la communication des résultats des mesures. *Celui qui va analyser la métrique.*
Source d'information pour l'analyse	Liste les sources d'information utiles pour l'analyse de résultats (documents, journaux, entretien, etc.)
Outils utilisés dans l'analyse	Liste les outils utilisés pour l'analyse (par exemple, des outils statistiques).
Client de l'information	La personne ou l'unité organisationnelle qui demande ou requiert les mesures pour les besoins de son activité. *Celui qui va utiliser la métrique.*
Information complémentaire	
Conseils d'analyse Complémentaires	Fournit des conseils complémentaires sur les variations de cette mesure.
Considérations de mise en œuvre	Liste les processus ou les exigences de mise en œuvre qui sont nécessaires pour la réussite de la mise en œuvre.

Exemple d'utilisation de la fiche

Identification de la mesure	
Nom de la mesure	Revue des droits d'accès des utilisateurs aux systèmes et aux applications.
Identifiant de la mesure	R1-A11.2.4
Objectif de la mesure de sécurité	A11.2.4 [27001:2005]
Mesure de sécurité (1)	Les managers doivent, dans leur périmètre, réexaminer les droits d'accès des utilisateurs à intervalles réguliers par le biais d'un processus formel.
Mesure de sécurité (2)	Revue des accès au réseau informatique.
Objectif de la mesure	Mesurer le pourcentage de manager déclarant avoir effectué des contrôles sur les droits d'accès utilisateurs de leur périmètre, ce qui permet d'évaluer : • la prise de conscience des managers vis-à-vis des risques d'accès non fondés, frauduleux ou obsolètes aux SI • l'implication du management dans le processus de maîtrise et de gestion du risque informatique.
Ré examinateur	Direction des Risques
Objets du mesurage et attributs	
Objet du mesurage	Processus de revue des droits d'accès des utilisateurs aux systèmes et aux applications.
Attributs	Attestation de réalisation de revue des droits d'accès des utilisateurs.
Spécification des mesures élémentaires (pour chaque mesure élémentaire [2…n])	
Mesures élémentaires	Existence d'une attestation de réalisation de revue des droits d'accès des utilisateurs par chacun des managers.
Méthodes de mesurage	Tous les trimestres les managers enverront un email standardisé au Département Sécurité des SI attestant que les accès des utilisateurs ont été revus pour leur périmètre.
Echelle	Numérique
Spécification de la mesure dérivée	
Mesure dérivée	Taux d'attestations retournées par les managers sur le trimestre étudié.
Fonction de mesurage	Taux d'attestations retournées par les managers sur le trimestre étudié = (nombre d'attestations retournées par les managers / Total d'attestations attendues dans le trimestre) * 100
Echelle	Ratio : pourcentage
Spécification de l'indicateur	
Description d'indicateur et exemple	Courbe montrant l'indicateur sur plusieurs périodes de restitution.
Modèle analytique	Satisfaisant si : % >= 90% Globalement satisfaisant si : 80% < % < 90% Moyennement satisfaisant si : 70% <= % <= 80% Insatisfaisant si : % < 70%
Critère de décision	Seuil min 80%
Interprétation d'indicateur	Un résultat insatisfaisant indique un manque d'engagement des managers dans la gestion des risques liés à la sécurité des SI.
Effets / impact	Si résultats insatisfaisants l'indicateur est remonté à la Direction Générale pour action.

Causes d'écart	Les réorganisations fonctionnelles de l'entreprise.
Valeurs positives	Des valeurs croissantes indiquent des tendances positives.
Format de restitution	Tableau Excel standardisé.
Procédure de collecte des données **Complétez cette section pour chaque mesure élémentaire**	
Fréquence de collecte des données	Trimestrielle
Fournisseur de l'information	Chaque manager
Collecteur de l'information	Le RSSI
Outils utilisés dans la collecte des données	Mail, courrier
Conservation des données collectées	Répertoire spécifique du disque réseau.
Date de collecte	Pour le 15 de chaque début de trimestre.
Procédure d'enregistrement des données	E://…/NOV08/R1-A11-2-4.XLS
Validité de la mesure	Annuelle
Période d'analyse	Du 1er janvier au 31 décembre de l'année en cours
Procédure d'analyse des données (pour chaque Indicateur)	
Fréquence de la restitution des données	Trimestrielle
Communicateur de l'information	Le RSSI
Source d'information pour l'analyse	Rapports d'entretiens
Outils utilisés dans l'analyse	Excel
Client de l'information	Direction des Risques
Information complémentaire	
Conseils d'analyse Complémentaires	N/A
Considérations de mise en œuvre	N/A

ANNEXE B : EXEMPLES D'ATTRIBUTS, DE METRIQUES ET/OU D'INDICATEURS

L'objet de cette annexe est d'apporter au lecteur un début de réflexion sur la mise en œuvre d'indicateurs. Elle fournit une liste non exhaustive d'attributs, de métriques et/ou d'indicateurs. Ces éléments de réflexions sont à adapter au contexte de l'organisme et du périmètre du SMSI.

Pour illustrer ces exemples, seuls les articles 8 « Sécurité liée aux ressources humaines », 9 « Sécurité physique et environnementale » et 15 « Conformité » de l'annexe A de l'ISO/IEC 27002:2005 ont été retenus.

Mesures de sécurité de l'ISO/IEC 27001 (annexe a)	Attributs, métriques et/ou indicateurs
A.8 Sécurité liée aux ressources humaines	
A.8.1 Avant le recrutement	
A.8.1.1 Rôles et responsabilités	Taux (granulométrie) de rôles ayant un impact sur la sécurité
A.8.1.2 Sélection	Taux de dossiers ayant fait l'objet d'une vérification des documents fournis par le candidat
A.8.1.3 Conditions d'embauche	Présence des règles de sécurité dans le contrat de travail ou dans le règlement intérieur
A.8.2 Pendant la durée du contrat	
A.8.2.1 Responsabilités de la direction	Existence d'un plan de communication sur la sécurité
A.8.2.2 Sensibilisation, qualification et formations en matière de sécurité de l'information	Nombre de personnes formées / an
A.8.2.3 Processus disciplinaire	Nombre annuel de sanctions disciplinaires Perte annuelle due à des pratiques à risque
A.8.3 Fin ou modification du contrat	
A.8.3.1 Responsabilités en fin de contrat	Existence d'une procédure de gestion des fins de contrat
A.8.3.2 Restitution des actifs	Coût des biens non rendus en fin de mission
A.8.3.3 Retrait des droits d'accès	Taux de retraits des droits hors délai
A.9 Sécurité physique et environnementale	
A.9.1 Zones sécurisées	
A.9.1.1 Périmètre de sécurité physique	Nombre d'actifs sensibles localisés dans des zones non sécurisées
A.9.1.2 Contrôles physiques des accès	Nombre d'intrusions physiques identifiées (y compris les dépassements d'horaires de personnes autorisées)
A.9.1.3 Sécurisation des bureaux, des salles et des équipements	Nombre annuel de disparition de biens informatiques dans les locaux
A.9.1.4 Protection contre les menaces extérieures et environnementales	Nombre de non conformités constatées lors des visites des organismes de contrôle.
A.9.1.5 Travail dans les zones sécurisées	Nombre d'écarts constatés par rapport aux consignes de sécurité applicables en vigueur.

Mesures de sécurité de l'ISO/IEC 27001 (annexe a)	Attributs, métriques et/ou indicateurs
A.9.1.6 Zones d'accès public, de livraison et de chargement	Nombre d'intrusions / vols / dans des aires de livraison
A.9.2 Sécurité du matériel	
A.9.2.1 Choix de l'emplacement et protection du matériel	Nombre d'équipements localisés dans des zones dont la sécurité n'est pas cohérente avec leur sensibilité
A.9.2.2 Services généraux	Durée mensuelle cumulée d'indisponibilité des énergies (électricité, climatisation, eau)
A.9.2.3 Sécurité du câblage	Nombre annuel d'accidents d'origine électrique Réalisation de contrôle annuel de conformité par des organismes indépendants
A.9.2.4 Maintenance du matériel	Taux d'équipements sensibles couverts par un contrat de maintenance adapté et honoré
A.9.2.5 Sécurité du matériel hors des locaux	Nombre d'équipements mobiles disparus pendant un déplacement
A.9.2.6 Mise au rebut ou recyclage sécurisé(e) du matériel	Nombre de destruction des données ou des équipements sensibles
A.9.2.7 Sortie d'un actif	Nombre de tentatives de sortie sans autorisation ; Nombre de demandes d'autorisation délivrées
A.15 Conformité	
A.15.1 Conformité aux exigences légales	
A.15.1.1 Identification de la législation en vigueur	Charge annuelle de la veille réglementaire
A.15.1.2 Droits de propriété intellectuelle (DPI)	Nombre de non-conformités sur les licences
A.15.1.3 Protection des enregistrements de l'organisme	Nombre de non-conformités constatées
A.15.1.4 Protection des d nées et confidentialité des informations relatives à la vie privée	Nombre annuel de non conformités dans le traitement des données personnelles (diffusions indues, refus de diffusion, …)
A.15.1.5 Mesure préventive à l'égard du mauvais usage des moyens de traitement de l'information	Nombre d'équipements détectés comme non-conformes
A.15.1.6 Réglementation relative aux mesures cryptographiques	Charge annuelle de la veille réglementaire spécifique
A.15.2 Conformité avec les politiques et normes de sécurité et conformité technique	
A.15.2.1 Conformité avec les politiques et les normes de sécurité	Nombre de non-conformités constatées
A.15.2.2 Vérification de la conformité technique	Nombre de non conformités identifiées lors d'audits techniques Nombre de non-conformités aboutissant dans des actions d'amélioration
A.15.3 Prises en compte de l'audit du système d'information	
A.15.3.1 Contrôles de l'audit du système d'information	Taux de réalisation du programme d'audit
A.15.3.2 Protection des outils d'audit du système d'information	Nombre d'incidents liés à l'utilisation non-autorisée.

L'ESPRIT DE L'ÉCHANGE

CLUB DE LA SÉCURITÉ DE L'INFORMATION FRANÇAIS

30, rue Pierre Sémard

75009 Paris

✆ 01 53 25 08 80

clusif@clusif.asso.fr

Téléchargez les productions du CLUSIF sur

www.clusif.asso.fr