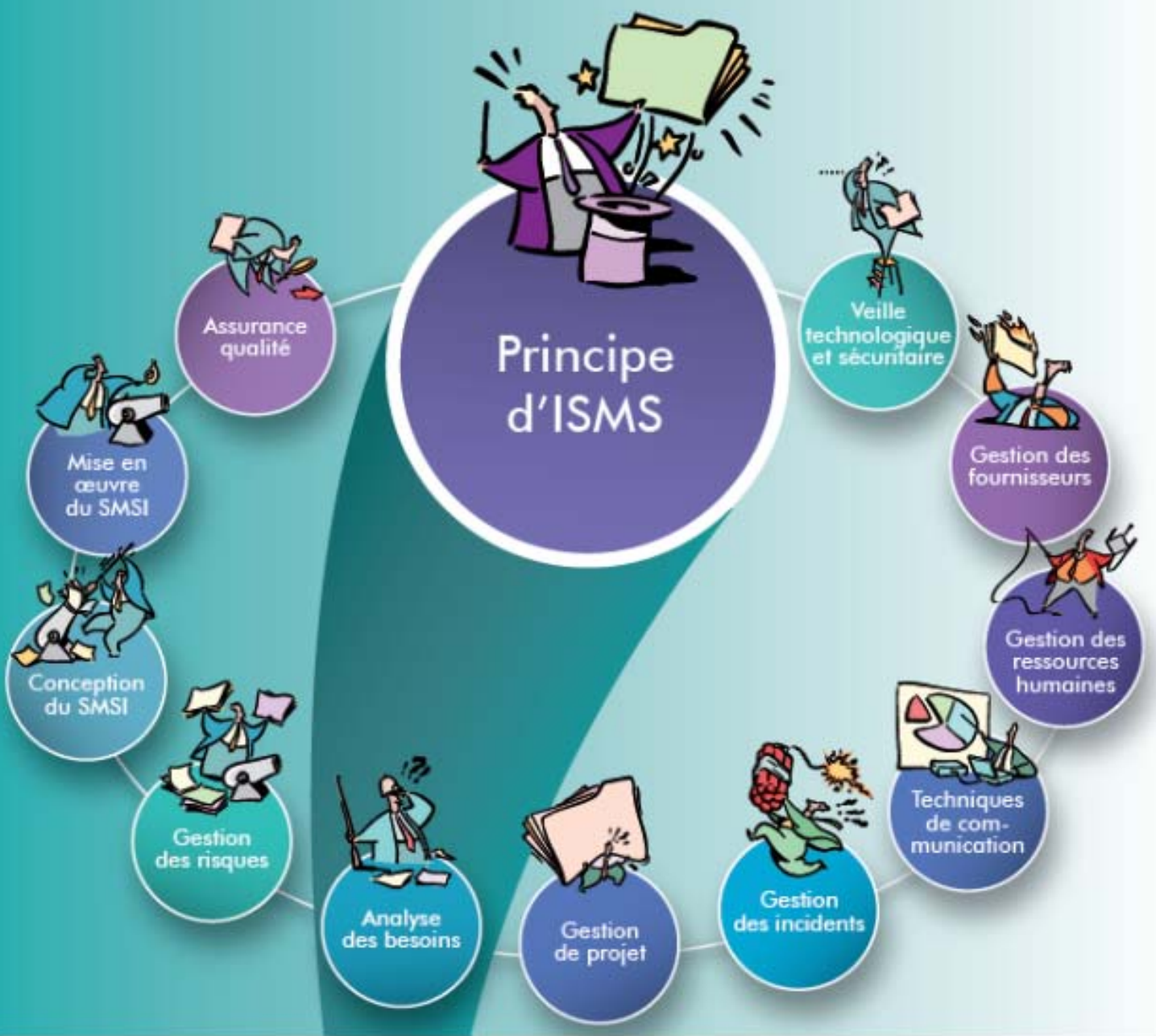
IDEC école supérieure d'informatique

ICT Security Expert

Les bases pour construire un ISMS



Sommaire

Chapitre 1
De la stratégie à l'ISMS en passant par le management de processus

1.1 Introduction

Dans tous les domaines, la sécurité ne devient une préoccupation qu'après une série de catastrophes ayant clairement démontré qu'elle n'est pas une option à ajouter uniquement quand on en a les moyens mais qu'elle doit être intrinsèquement présente dès la conception. L'aéronautique, l'automobile et de manière plus générale, toutes les industries qui ont eu une influence majeure sur l'économie et la société sont déjà passées par les phases d'expérimentation, de déploiement, de standardisation et de sécurisation.

Les spécialistes s'accordent pour affirmer que la dernière révolution industrielle en date est celle de l'information. De fait, nous ne pouvons que constater chaque jour que l'information porte dorénavant une valeur économique essentielle. La richesse même de l'individu ou des nations n'est plus tangible : l'argent que vous possédez n'est qu'un enregistrement dans une base de données, de même que votre identité et votre nationalité. Les états eux-mêmes, qui garantissaient auparavant leur monnaie sur la base de l'or qu'ils possédaient, empruntent aujourd'hui sur la base de la valeur accordée à leur économie et leur croissance, c'est-à-dire purement et uniquement de l'information produite par des experts.

Pourtant, ce monde de l'information n'a pas encore atteint sa maturité industrielle. La standardisation et la sécurisation sont à l'ordre du jour mais les exigences du marché et de la législation en la matière ne font qu'émerger, au fil des pertes bien tangibles que subissent les uns et les autres à cause d'informations perdues ou, au contraire, transmises à des entités qui n'auraient pas dû en avoir connaissance et s'en sont servi pour nuire.

La mission d'un ICT Security Expert consiste à garantir que son entreprise traite l'information conformément à ses propres besoins de sécurité mais également à ceux de ses clients et partenaires ainsi qu'aux exigences de la réglementation en vigueur. L'intitulé du poste étant souvent RSSI, pour « responsable de la sécurité du système d'information », nous emploierons le plus souvent ce terme pour désigner l'ICT Security Expert.

Ce premier chapitre présente les concepts et le vocabulaire nécessaires à l'acquisition des compétences d'un RSSI. Ces concepts seront développés de manière plus approfondie dans la suite de ce livre ou dans d'autres livres de la collection ICT Security

Expert. Chacun de ces livres sera également présenté, avec son rôle vis-à-vis de la mission du RSSI.

Le but de ce premier chapitre est d'offrir une vision générale du domaine de la sécurité de l'information et de sa place dans l'économie et la gestion des organisations.

Tout au long des ouvrages de la collection, nous voyagerons en compagnie de deux entreprises fictives mais réalistes qui ont toutes deux pour objectif la certification ISO[1] de leur système de management de la sécurité de l'information (SMSI ou ISMS pour *Information Security Management System*).

La première est une petite entreprise qui développe des logiciels de *serious games*, des jeux à vocation éducative destinés à la formation en entreprise. Son fondateur, propriétaire et directeur se nomme David Vinssant et il a créé son entreprise après plusieurs années de carrière en tant que consultant en sécurité des systèmes d'information. Durant ses loisirs, David a conçu plusieurs jeux gratuits qui ont obtenu un honorable succès sur les plateformes de téléchargement. L'idée lui est alors venue de conjuguer son hobby et sa profession afin de réaliser un *serious game* de sensibilisation à la sécurité de l'information. Il a donc fondé David Vinssant Développement Logiciel (DVDL) tout en conservant à temps partiel son activité de consultant. Une grande association patronale s'est montrée très intéressée par son projet et lui a commandé un premier module mais elle souhaite que DVDL fasse preuve d'exemplarité en matière de sécurité des systèmes d'information

[1] Tous les mots soulignés en pointillés sont définis dans le lexique, page 145 et suivantes.

(SSI) et obtienne la certification ISO 27001 avant de signer le mandat pour la totalité du projet.

A l'opposé, la seconde entreprise est bien loin de la PME puisqu'il s'agit d'une banque présente dans toute la Suisse. La banque Koffr-Faure emploie près de 10'000 collaborateurs dans un réseau qui comprend quasiment un millier d'agences. Face à la méfiance grandissante des clients vis-à-vis de la cybercriminalité et de l'usage de leurs données personnelles, la banque souhaite se positionner comme un partenaire de confiance en démontrant sa conformité à la norme de sécurité internationale ISO 27001.

L'une, la banque, dispose déjà d'un système de management de la sécurité de l'information mais il a été élaboré au fur et à mesure que les besoins apparaissaient et, bien qu'il ait été audité et testé de nombreuses fois, sa conformité à une norme n'a encore jamais été vérifiée. L'autre vient tout juste de débuter son activité, ce qui lui offre l'opportunité de pouvoir intégrer la sécurité quasiment dès le début de son activité. DVDL va pouvoir pratiquer le fameux « *secured by design* » que prônent les experts comme seule manière d'obtenir des systèmes sûrs.

Chacune sera confrontée à des difficultés bien différentes qui nous permettront d'illustrer la diversité des implémentations d'ISMS dans les organisations. La conception et la réalisation d'un système de management de la sécurité de l'information, comme tout projet impactant l'ensemble d'une organisation, présente en effet son lot de difficultés et elles sont loin d'être négligeables.

La première d'entre elle, sans doute l'une des plus importantes, est le manque de conviction des dirigeants et des collaborateurs lorsqu'il s'agit de dépasser le discours sécuritaire et de mettre

réellement en œuvre la sécurité de l'information. Le chapitre qui suit en aborde les causes.

1.2 Sécurité et efficience : des objectifs concurrents

L'efficience, c'est la capacité à réaliser une tâche à l'aide de la juste quantité de ressources. Quand l'efficacité se contente d'atteindre les objectifs, par exemple répondre correctement à la demande d'un client dans un court délai, l'efficience y ajoute une contrainte : les ressources consommées pour ce faire doivent être le minimum nécessaire pour atteindre l'objectif. Parmi ces ressources, on trouve le matériel, les infrastructures, les personnes et les moyens financiers. Quand les ressources sont essentiellement d'ordre financier, on parle souvent de rentabilité. Tout comme l'efficience, la rentabilité est un objectif concurrent à celui de la sécurité. En effet, la sécurité se matérialise la plupart du temps sous forme :

- ☹ d'opérations supplémentaires, comme s'authentifier afin d'être autorisé à réaliser une opération ou encore catégoriser chaque information produite pour indiquer son niveau de confidentialité,

- ☹ de logiciels et matériels de protection qu'il faut acquérir, tester, déployer, mettre à jour et surveiller aussi bien que les logiciels de production,

- ☹ de restrictions sur l'usage de ressources qui nécessitent parfois l'intervention de personnes supplémentaires pour valider une opération ou simplement l'autoriser,

- ☹ de personnes embauchées ou mandatées pour contrôler si la sécurité est adéquate et effective.

Tout ceci a un coût, direct (l'achat des solutions de protection et les salaires des personnes en charge de la sécurité) ou indirect (le ralentissement des opérations dû aux contraintes supplémentaires).

Or toutes les organisations ont un impératif d'efficience voire de rentabilité :

- les entreprises commerciales, bien sûr, qui doivent produire un bénéfice afin de rémunérer leurs actionnaires ou de rembourser le capital emprunté,
- mais aussi les organisations de type communal, cantonal ou fédéral qui doivent offrir à l'électeur-contribuable le service qu'il attend au meilleur coût,
- et jusqu'aux organisations non gouvernementales qui doivent consacrer les fonds de leurs généreux contributeurs à la cause qu'ils déclarent servir avec des frais de fonctionnement réduits au minimum.

Ainsi, l'efficience est une condition élémentaire de survie de toute organisation.

Comment s'étonner alors que, face au surcoût engendré par la sécurité, les dirigeants préfèrent allouer un budget à des opérations au résultat garanti plutôt qu'à des mesures destinées à les protéger d'événements qui n'auront peut-être jamais lieu ?

Comment s'étonner que les collaborateurs des organisations, auxquels on demande l'efficience dans chacune de leurs tâches, se préoccupent avant tout d'atteindre les objectifs fixés par leur hiérarchie et s'efforcent d'ignorer ou de contourner toutes les contraintes qui peuvent les en empêcher ?

C'est un fait : la sécurité ne fait pas partie de ce que les organisations jugent utile. Elle appartient au domaine de la garantie, comme le décrit le prochain chapitre.

1.3 Utilité et garantie dans la fourniture de services

Née sous forme de recueil de bonnes pratiques, l'ITIL s'est progressivement imposée comme référence dans la fourniture de services informatiques aussi bien chez les fournisseurs IT que dans les entreprises dont l'informatique n'est pas le métier. Sa vision des composantes d'un service illustre bien la difficulté à trouver un soutien pour la mise en œuvre du « *secured by design* ».

Rappelons tout d'abord ce qui constitue un service tel que le définit l'ITIL : « *un moyen d'apporter de la valeur aux clients en les aidant à obtenir les résultats qu'ils souhaitent sans en supporter les coûts et les risques spécifiques. Un service IT est composé d'une combinaison d'informatique, de personnes et de processus.* »

La manière dont ces composants s'organisent en relation avec la stratégie et les processus figure en annexe, page 140.

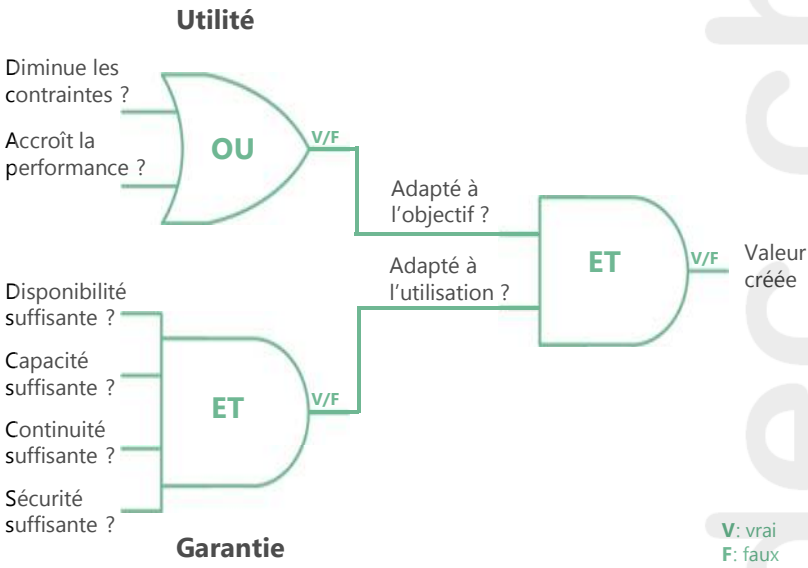


Figure 1 : utilité et garantie (adapté de ITIL, Service Strategy 2011)

Représenté sous forme de portes logiques comme dans l'ingénierie des processeurs, ce schéma ramène à sa plus simple expression les caractéristiques qu'un service doit offrir afin d'être générateur de valeur.

Du côté de l'utilité, qui est la partie la plus visible du service, soit le service permet à son utilisateur d'améliorer sa performance dans la réalisation d'une tâche, soit il lève des contraintes qui gênaient la réalisation de cette tâche. Chez Koffr-Faure, les deux dernières applications livrées illustrent bien ces aspects. La première permet au chargé de compte de consulter d'un clic de souris toutes les demandes du client, quel que soit le canal emprunté pour les formuler, ce qui élimine le temps de recherche. Cela constitue un gain de temps appréciable et rend le chargé de compte plus