

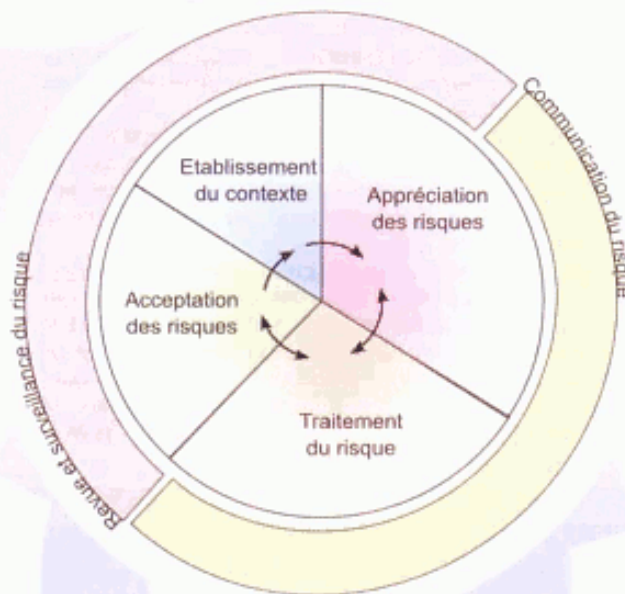
NORME

L' « ABÉCÉDAIRE » DE LA NORME ISO 27005

Par Anne Lupfer, Cabinet HSC



La cindynique, appelée science du danger, est la discipline qui étudie les risques. Cette activité se développe et évolue depuis une vingtaine d'années dans des secteurs variés tels que la finance, l'environnement, la santé, etc. La norme ISO 27005, inspirée de ces travaux antérieurs, décrit le processus de gestion des risques en sécurité de l'information et permet une clarification du vocabulaire. Un cindynicien y retrouvera donc ses repères conceptuels et lexicaux pour partie. Pour les néophytes, il est important d'apporter des clarifications quant aux concepts et au vocabulaire pour leur faciliter la compréhension et la maîtrise de la norme.



*Def : Ensemble d'activités corrélées ou interactives qui transforme des éléments d'entrée en éléments de sortie. ISO 9000:2005 3.4.1

La norme ISO 27005:2008 décrit le processus* de gestion du risque de sécurité de l'information comme un processus itératif et non linéaire. Six sous-processus, eux-mêmes divisés en activités, sont identifiés : établissement du contexte (context establishment), appréciation des risques (risk assessment), traitement du risque (risk treatment), acceptation du risque (risk acceptance), revue et surveillance du risque (risk monitoring and review) et communication du risque (risk communication). Chacun de ces sous-processus peut être considéré individuellement bien que sa sortie constitue une entrée pour le processus suivant. Les deux derniers (revue et supervision du risque et

communication du risque) sont transverses et interviennent donc tout au long du processus de gestion du risque. Les sous-processus « traitement du risque » et « acceptation du risque » sont itératifs et permettent de mesurer et approuver les résultats des processus précédents.

La gestion du risque de sécurité de l'information doit donc être établie et suivie suivant un processus continu. Ce processus doit définir le contexte, apprécier et traiter les risques en utilisant un plan de traitement pour implémenter les recommandations et les décisions. La gestion du risque analyse les éventualités et les conséquences plausibles, avant de décider les actions à mener et leur ordonnancement, afin de réduire les risques à un niveau acceptable.

Appréciation des risques

Une différence notable avec les méthodes de gestion du risque connues est l'appellation « appréciation des risques » que l'on dénomme habituellement, en langage commun, « analyse de risque ». Au sens de la norme ISO 27005:2008, le sous-processus « appr-

Appréciation des risques

Analyse du risque

Identification des risques

Estimation des risques

Evaluation des risques



ciation des risques » a pour objectifs, l'identification, la quantification ou la qualification et la priorisation des risques par rapport aux critères de leurs évaluations et des objectifs pertinents pour l'organisme. Cette appréciation, noyau dur du processus de gestion du risque, regroupe donc « l'analyse des risques » et « l'évaluation des risques ». L'analyse des risques est également composée de deux activités : « l'identification des risques » et « l'estimation des risques ».

Actif primordial et actif en support

Les actifs*, centre d'intérêt du processus de gestion du risque, sont, dans la norme ISO 27005:2008, ordonnés en deux catégories : actifs primordiaux (primary assets) et actifs en support (supporting assets).



Sous la dénomination « actif primordial » sont regroupés les processus métiers (et sous processus), les activités et l'information. Les « actifs en support » sont de différents types : matériel, logiciel, réseau, personnel, site, structure. Les actifs

primordiaux reposent sur les actifs en support ou sur un groupe d'actifs en support. Cela signifie qu'à un processus (actif primordial) sont rattachés des actifs (actifs en support) qui permettent le bon fonctionnement de ce processus. La sécurité de l'information repose essentiellement sur la sécurité des différents actifs en support pris individuellement et globalement. Ainsi, le gestionnaire du risque identifiera les risques qui pèsent sur les actifs en support et non sur les actifs primordiaux. Le gestionnaire du risque portera une vigilance particulière à ce que son équipe ne fasse pas de confusion entre actif primordial et actif essentiel ou capital pour l'entreprise. Tout processus même superflu, toute information même de faible valeur, toute activité même secondaire sont des actifs primordiaux. La valorisation des actifs primordiaux et des actifs en support est réalisée dans un second temps et influera sur le niveau de risque et les choix de traitement du risque.

Risque

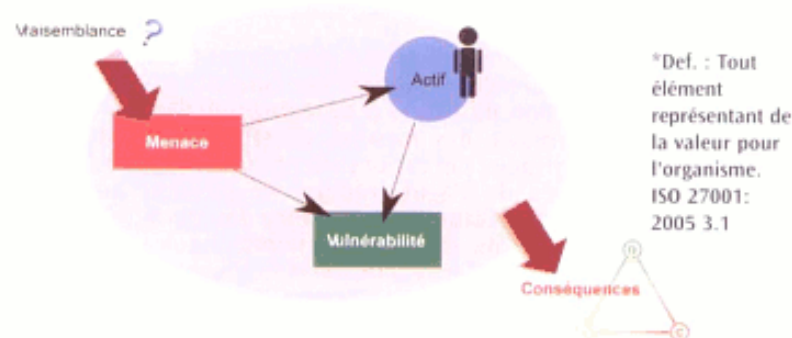
Le risque se définit comme la possibilité (éventualité) qu'une menace donnée exploite une ou plusieurs vulnérabilités d'un actif ou d'un groupe d'actifs et, ainsi, cause des préjudices à l'organisme.

Le risque se mesure en termes de combinaison de la vraisemblance (probabilité d'occurrence) et de ses conséquences.

Likelihood : la probabilité d'une occurrence

Likelihood est un terme scientifique anglophone décrivant

une fonction statistique. Ce terme ne possède pas d'équivalent direct en langue française. Le BS-25999-1 le définit ainsi : « possibilité que quelque chose se produise, pouvant être définie, mesurée ou estimée objectivement ou subjectivement avec des termes descriptifs généraux (tels que rare, improbable, probable, possible, certain), sous forme de fréquence ou de probabilités mathématiques. » Les francophones ont tendance à traduire likelihood par probabilité d'occurrence. Cependant, il semble plus cohérent de retenir le terme



*Def. : Tout élément représentant de la valeur pour l'organisme. ISO 27001: 2005 3.1

« vraisemblance »**. En effet, le gestionnaire du risque et ses acolytes pourraient être influencés par l'a priori mathématique du mot probabilité tandis que la « vraisemblance » se réfère à quelque chose de plausible où le subjectif intervient plus aisément. Lorsque la vraisemblance d'un événement est estimée par les participants à l'appréciation du risque, aucun élément ne doit être négligé. Il conviendra de prendre en compte les mesures de sécurité implémentées ou planifiées, les événements et incidents passés propres à l'organisme mais également publiés dans la presse, le contexte particulier de l'organisme, les comportements des employés, etc. Une grande part subjective entre donc en jeu dans l'estimation de la vraisemblance. Ce subjectif est essentiel pour tendre vers la réalité de l'entreprise

**Def. : la vraisemblance peut être exprimée qualitativement ou quantitativement.

STANDARDS ISO 27005 FROM A TO Z

ANNE LUPFER, HSC



Risk analysis (sometimes referred to as cindynics) is the science of risk probability and evaluation. This activity has been developing over the last 20 years in areas such as finance, environment, health, etc. The ISO 27005 standard, which is based on previous work in this area, describes the risk management process for information security systems and defines the terms used. Risk analysis experts will find some of their familiar terms and concepts but further clarification is required to allow newcomers to fully understand and master the new the standard.

NORME

afin de répondre le plus parfaitement possible aux besoins de l'entreprise. C'est pourquoi, les résultats des appréciations des risques diffèrent d'un organisme à un autre. Ainsi, un même risque pourra être réduit par un organisme et accepté par un autre.

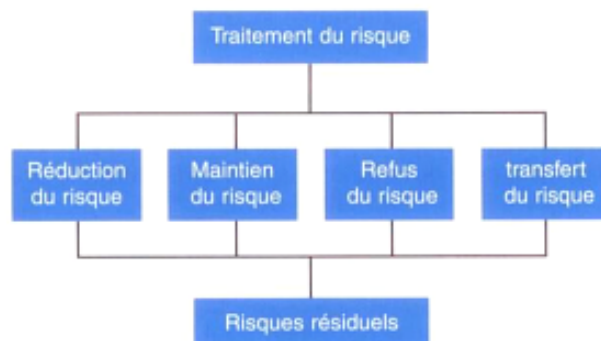
De la réduction au transfert du risque

Bien que les organismes soient libres quant au traitement du risque, quatre choix s'imposent à eux: réduction du risque, maintien du risque, refus du risque et transfert du risque.

Ces choix sont effectués suivant des critères établis par l'organisme lui-même et dictent une conduite à tenir :

- La réduction du risque (risk reduction) consiste à mettre en œuvre des mesures de sécurité afin de réduire les risques. Ces actions visent soit à réduire les vulnérabilités de l'actif (réduire l'exposition aux menaces), soit à limiter la survenance des menaces.

- Le maintien du risque (risk retention) consiste à prendre le risque. C'est-à-dire que le risque est accepté et la situation inchangée. Malgré les apparences, maintenir le risque n'est pas une action passive mais nécessite de tenir fixe un risque, voire une situation.



- Le refus du risque ou évitement du risque (risk avoidance) consiste à supprimer l'élément qui engendre le risque. Dans le cas où un nouveau projet crée des risques trop importants, le projet est abandonné.

- Le transfert du risque (risk transfer) consiste à faire appel à une assurance ou un tiers possédant des compétences spécifiques. Le risque est supporté par l'assureur ou le tiers via un contrat, mais la responsabilité légale ne peut être transférée.

Impact et conséquence

Lors de la phase d'établissement du contexte, les critères de base sont établis. Ces critères comprennent, en particulier, les critères d'impact. Ces derniers doivent être développés et spécifiés en termes de degré de dommages ou de coûts sur l'organisme causés par un événement de sécurité de l'information.

Lors de l'analyse de risque, les conséquences (en termes de perte de confidentialité, intégrité et disponibilité) sur les actifs doivent être identifiées. Elles peuvent être temporaires ou permanentes. Par exemple, l'indisponibilité d'un actif dû à une panne mineure sera temporaire tandis qu'une destruction sera permanente.

De manière générale, il est indispensable de formuler, de manière claire et compréhensible par tous, les conséquences et les impacts. Une ou deux phrases illustrent parfaitement les conséquences d'un événement. Cette explication facilite la communication avec la direction, avec les utilisateurs et les parties prenantes. De plus, elle facilite l'amélioration du processus. En effet, expliciter clairement et succinctement les faits permet de comprendre les résultats et les décisions prises ultérieurement. Une bonne appréciation des risques doit pouvoir être comprise et mise à jour par n'importe qui.

Mesures de sécurité suivant l'acception anglaise de « control »

En anglais, le terme control possède plusieurs significations. La première définition, qui induit en erreur les personnes francophones, est la notion de surveillance et de mesure. La seconde, plus appropriée dans la gestion du risque, est l'action de réduire l'envergure de quelque chose. Dans la majorité des cas, dans la norme ISO 27005:2008, « control » est employé dans ce sens. Dans le domaine de la sécurité de l'in-



formation, l'action de réduire un risque est réalisée par l'implémentation de dispositifs de sécurité. Ces derniers, de différentes natures, sont plus couramment appelés mesures de sécurité (controls). Dans le cas de la gestion du risque, control est donc un faux ami. L'utilisation du terme contrôle est à prendre avec vigilance d'autant que dans la norme, ce terme est parfois employé sous son premier sens de vérification. Les mesures de sécurité (controls) permettant de réduire les risques, dont fait référence la norme ISO 27005:2008, émanent de l'annexe A de la norme ISO 27001:2005. Ces mesures de sécurité sont ordonnées par thèmes et regroupées sous des objectifs de sécurité.

Les risques résiduels doivent être acceptés par les DG

Pour la norme ISO 27001:2005, les risques résiduels doivent être acceptés par la direction générale. Ce principe est appliqué dans la norme ISO 27005. Ces risques, bien souvent oubliés lors d'une appréciation des risques, sont essentiels pour la validation du plan de traitement du risque avant son implémentation. En effet, le risque résiduel (risque qui reste après l'implémentation de mesures de sécurité) est calculé suivant la même méthode que le risque initial. Les résultats obtenus sont alors comparés. Si le niveau de risque résiduel atteint un niveau acceptable, la pertinence des mesures de sécurité est validée. Autrement, il convient d'analyser à nouveau la situation.

La norme ISO 27005:2008, décrivant le processus de gestion des risques dans sa globalité, apporte de nombreux éclaircissements lexicaux et n'interdit pas à chacun de continuer à utiliser son propre vocabulaire. Maîtriser son système prime avant tout. Il est primordial que les équipes se comprennent et parlent le même langage. Cependant, adopter le vocabulaire normatif facilite les échanges entre les organismes et les individus à grande échelle. Il favorise la compréhension des documents officiels, il accorde chacun sur

les activités à réaliser lors de chaque processus et il limite les interprétations personnelles dues à un vocabulaire mal choisi. ■ ■ ■

Tableau récapitulatif

Asset	Actif
Primary asset	Actif primordial
Supporting asset	Actif de support
Avoid	Éviter (ou refuser)
Basic criteria	Critère de base
Conséquence	Conséquence
Context establishment	Établissement du contexte
Control	Mesure de sécurité ou contrôle
Impact	Impact
Likelihood	Vraisemblance (ou probabilité d'occurrence)
Risk	Risque
Risk acceptance	Acceptation du risque
Risk analysis	Analyse du risque (ou analyse des risques, analyse de risque)
Risk assessment	Appréciation du risque
Risk avoidance	Évitement ou refus du risque
Risk criteria	Critère de risque
Risk estimation	Estimation du risque
Risk evaluation	Évaluation du risque
Risk identification	Identification du risque (ou identification des risques)
Risk management	Management du risque ou gestion de risque ou gestion du risque
Risk monitoring and review	Surveillance et réexamen du risque
Risk reduction	Réduction du risque ou réduction des risques
Risk retention	Maintien du risque
Risk transfert	Transfert du risque
Vulnerability	Vulnérabilité