

NORME

ISO/CEI 27005 :

LA NORME DU CONSENSUS



Le 4 juin 2008, l'ISO a publié la première norme de gestion de risque ISO/CEI 27005 (document daté du 15 juin). Le groupe de normalisation internationale ISO SC27 WG1 avait d'ores et déjà accepté une version préliminaire en novembre 2007. Depuis sa publication, elle a beaucoup circulé, mais sa version définitive était très attendue. Compte tenu de son importance, la traduction de l'ISO 27005 en français a d'ores et déjà été lancée par l'AFNOR.

PAR HERVÉ SCHAUER, CABINET HSC



Hervé Schauer, Cabinet HSC

La norme ISO 27005 explique en détails comment conduire l'appréciation des risques et le traitement des risques, dans le cadre de la sécurité de l'information. Tout en définissant une méthodologie de gestion de risques strictement conforme à la norme ISO

27001, la norme ISO 27005 demeure utilisable dans toutes les situations, de manière autonome, par exemple pour l'appréciation des risques dans un projet, dans un PCA, sans lien avec l'ISO 27001. La norme ISO 27005 applique à la gestion de risques le cycle d'amélioration continue PDCA utilisé dans les normes de systèmes de management, comme l'ISO 27001 en sécurité de l'information. Cela lui permet une souplesse et un pragmatisme pour être utilisée en toutes circonstances et notamment dans des entreprises où tout change sans arrêt. Elle constitue un guide qui s'adapte à tous types d'organismes et de situations.

ISO 27005, une norme synthétique et consensuelle

La norme ISO 27005 est un très rare exemple de vérifiable norme. Une norme se doit d'être le consensus entre les points de vues des différents acteurs du mar-

NORME



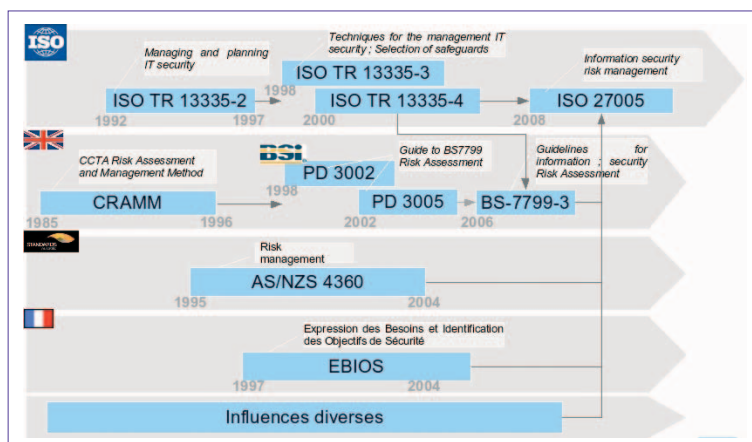
ché et des différents pays. Elle se doit d'offrir des garanties aux utilisateurs, notamment aux consommateurs, et de permettre une rationalisation et une multiplication des échanges. Or en SSI, une grande majorité de normes ne servent à rien, sont de piètre qualité, et existent car un consultant trouve du financement quand il est volontaire pour être rédacteur en chef d'une norme. La norme ISO 27005 est l'exemple même de la norme synthétique et consensuelle qui répond à ce que devrait être une norme. Elle reprend tout ce qui avait été fait sur le sujet. L'ISO 27005 est principalement issue :

- De la norme internationale ISO 13335 qui a modélisé la gestion de risque en sécurité des systèmes d'information dès le lancement de la normalisation en SSI en 1992.
- De la méthode EBIOS v2 de la DCSSI en France, dont notamment le principe du découpage du processus d'appréciation des risques en activités et sous-activités élémentaires avec des entrées, un travail à accomplir et un résultat à obtenir, a été repris dans l'ISO 27005 ;
- De la norme australienne et néo-zélandaise AS 4360 dont est issue le schéma ordonnant les tâches de la gestion de risques ;
- De la norme britannique BS7799-3, qui avait été éditée par le BSI dans la lignée de la norme BS7799-2 qui est devenue l'ISO 27001 ;
- De nombreuses autres sources diverses dont je n'ai pas forcément repéré la filiation dans l'ISO 27005, que leurs auteurs m'en excuse.

La norme ISO 27005 présente la gestion de risque en utilisant un vocabulaire courant, que l'on retrouve dans les autres métiers, ce qui facilite sa compréhension et sa lecture. Un prochain article dans cette rubrique fera un point sur le vocabulaire. La norme ISO 27005 applique les critères de risques (appelés aussi critères de sécurité) : confidentialité, intégrité, disponibilité, sur l'ensemble du patrimoine informationnel de l'organisme, selon les objectifs de sécurité du processus métier, les obligations légales, les contraintes réglementaires, les aspects financiers et opérationnels, la technologie et les facteurs sociaux et humains.

Elle va ainsi plus loin que les méthodes basées sur les menaces et vulnérabilités visant les ressources informatiques. L'ISO 27005 met les ressources informatiques comme actifs de soutien aux actifs primordiaux que sont l'information et les métiers de son organisme.

La norme ISO 27005 est fondamentale car trop d'organismes ont pris pour argent comptant la norme ISO 27002 (anciennement ISO 17799), malheureusement disponible avant l'ISO 27001, qui définit le processus par lequel la SSI est gérée dans le temps. Ainsi, de nombreux organismes utilisent l'ISO 27002 dans une approche conformité, à la SoX et autres référentiels



innombrables. Cependant, développer une approche conformité par rapport à l'ISO 27002 en SSI donne des résultats catastrophiques. Elle engendre des actions inutiles et coûteuses, vous fait vous mettre à dos les services de production informatique qui doivent être vos alliés, oblige les gens à prendre l'habitude de mentir en cochant des cases alors que les actions ne sont pas faites et dégoûte l'ensemble des utilisateurs de la sécurité. Il n'y a que les auditeurs peu compétents qui y trouvent leur compte.

Une approche par la gestion de risque

La norme ISO 27005 permet de revenir à une approche de la sécurité de l'information par la gestion de risque. Or seule une approche de ce type permet de justifier ce qui est fait ou non dans le déploiement des dispositifs de sécurité. L'ISO 27005 utilise une évaluation des risques par scénarios, mais pas une analyse des risques par scénarios, cependant elle recommande l'utilisation de scénarios pour expliquer et justifier dès l'identification des risques.

Avant de parler de la



TITRE

BY XXXXXX

Texte

NORME

Contents	Page
Foreword	v
Introduction	1
1 Scope	1
2 Normative references	3
3 Terms and definitions	3
4 Structure of this International Standard	3
5 Background	4
6 Overview of the information security risk management process	7
7 Context establishment	7
7.1 General considerations	7
7.2 Basic criteria	9
7.3 The scope and boundaries of information security risk management	10
7.4 Organization for information security risk assessment	10
8 Information security risk assessment	14
8.1 General description of risk assessment	14
8.2 Risk analysis	17
8.2.1 Risk identification	17
8.2.2 Risk estimation	19
8.3 Risk evaluation	20
9 Information security risk treatment	20
9.1 General description of risk treatment	20
9.2 Risk reduction	21
9.3 Risk retention	21
9.4 Risk avoidance	21
9.5 Risk transfer	21
10 Information security risk communication	22
11 Information security risk monitoring and review	23
12 Information security risk management	25
12.1 Monitoring and review of risk factors	25
12.2 Risk management monitoring, reviewing and improving	25
Annex A (informative) Defining the scope and boundaries of the information security risk management process	28
A.1 Study of the organization	28
A.2 List of the constraints affecting the organization	28
A.3 List of the legislative and regulatory references applicable to the organization	28
A.4 List of the constraints affecting the scope	28
Annex B (informative) Identification and valuation of assets and impact assessment	31
B.1 Examples of asset identification	31
B.1.1 Identification of primary assets	31
B.1.2 List and description of supporting assets	31
B.2 Asset valuation	35
B.3 Impact assessment	36
Annex C (informative) Examples of typical threats	40
Annex D (informative) Vulnerabilities and methods for vulnerability assessment	42

norme ISO 27002, parlez d'abord de l'ISO 27005. Elle vous permettra de choisir, en amont, les mesures de sécurité appropriées de l'ISO 27002, là où c'est justifié.

La norme ISO 27005 détaille le processus de gestion de risque dans les chapitres 6 à 12. Elle est complétée de 6 annexes de référence A à F, nécessaires à la mise en oeuvre de la méthode. Ces annexes permettent d'alléger le corps de la

norme tout en permettant d'avoir les approfondissements, les explications détaillées, les tableaux et les listes.

Le chapitre 6 explique le processus de gestion de risque dans son ensemble et la manière dont il se positionne dans un cycle PDCA.

Le chapitre 7 précise l'établissement du contexte, afin que l'on spécifie son périmètre de l'appréciation des risques, que l'on établisse tous les critères de base, que l'on décrive son environnement, et organise ses processus.

Le chapitre 8 définit l'appréciation des risques, qui se décompose en l'analyse des risques et l'évaluation des risques. Le paragraphe 8.2 définit l'analyse de risques, qui consiste, d'une part, à identifier et valoriser ses actifs sensibles, identifier les menaces et les vulnérabilités, ainsi que les mesures de sécurité existantes, et, d'autre part, à estimer la probabilité d'occurrence des risques identifiés, quantifier les conséquences potentielles, au final, calculer le risque. L'estimation des risques peut être qualitative ou/et quantitative. La norme n'impose aucune méthode de calcul particulière et en propose 3 en annexe. Le paragraphe 8.3 décrit l'évaluation des risques afin de prioriser et ordonner les risques par rapport aux critères d'évaluation des risques. Ces critères préalablement établis par les objectifs de sécurité imposés par les métiers de l'organisme et identifiés

par les parties prenantes permettent de déterminer le seuil au-delà duquel le risque devra être traité.

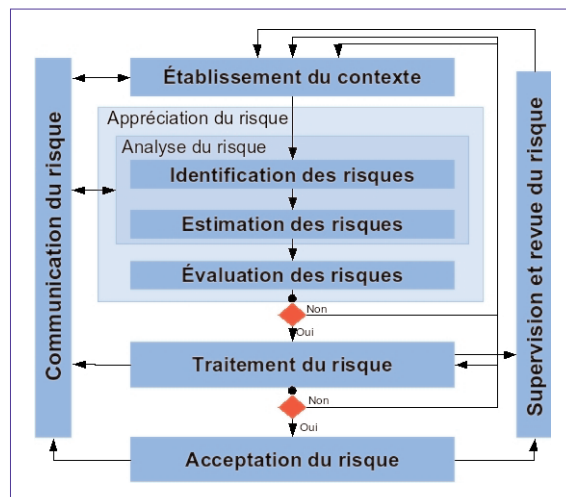
Le chapitre 9 spécifie le traitement du risque. Les quatre choix du traitement du risque sont :

- 1) Le refus ou évitement : le risque est trop élevé, il n'y a pas de mesure de sécurité réaliste pour le réduire, l'activité est supprimée ;
- 2) Le transfert vers un assureur ou un sous-traitant qui saura mieux le gérer ;
- 3) La réduction par l'application des mesures de sécurité ;
- 4) Et la prise de risque : le risque est accepté tel quel sans qu'aucune action soit prise.

A ce stade, la norme dit d'intégrer les coûts notamment dans le choix des mesures de sécurité.

Le chapitre 10 détermine l'acceptation du risque. Il faut calculer le risque résiduel qui sera obtenu une fois que le traitement du risque sera mis en oeuvre. La direction générale doit accepter les risques résiduels, donc accepter le plan de traitement du risque dans son ensemble. Cette décision est formellement documentée et enregistrée, et si par exemple des contraintes de budget ou de temps ne permettent pas à la direction de déployer, c'est elle qui en prend la responsabilité, pas la RSSI.

Le chapitre 11 décrit la communication du risque. Cette communication est un partage régulier d'informations entre le gestionnaire des risques SSI (en général, le RSSI), les décisionnaires, et les parties prenantes concernant la gestion du risque. Ses buts sont de donner confiance à la direction générale et aux parties prenantes, collectionner les informations concernant





les risques encourus, faire connaître les plans de traitement du risque, obtenir le support et les moyens pour la mise en oeuvre du traitement du risque, impliquer la responsabilité des décisionnaires, améliorer les compétences de gestion du risque, et sensibiliser l'organisme à la prévention du risque.

Le chapitre 12 décrit la surveillance et le réexamen des risques. La surveillance constante du processus de gestion des risques est nécessaire pour s'assurer que le processus reste pertinent et adapté aux objectifs de sécurité des métiers de l'organisme, que chaque risque traité n'est pas surestimé ou sous-estimé, et que ses coûts de gestion sont adaptés à la dimension du risque et aux besoins de sécurité. Il faut aussi identifier les changements nécessitant une réévaluation du risque ainsi que les nouvelles menaces et vulnérabilités.

L'annexe A liste toutes les contraintes qui peuvent affecter votre processus de gestion des risques.

L'annexe B aide à identifier et valoriser les actifs à considérer dans son appréciation des risques, et aide à estimer les impacts.

L'annexe C répertorie les menaces classées par type : dommages physiques, pertes de service essentiel, altération d'informations, etc. La liste n'est pas exhaustive mais complète.

L'annexe D liste les vulnérabilités, les moyens de recherche de vulnérabilités et des exemples de menaces qui pourraient exploiter ces vulnérabilités.

L'annexe E décrit trois méthodes de calcul de risque, qui permettent de réaliser l'appréciation des risques, dans l'activité estimation des risques. Les méthodes estiment l'impact potentiel d'un risque par rapport à la valeur de l'actif, à la facilité d'exploitation des vulnérabilités par les menaces, à la probabilité d'occurrence, etc.

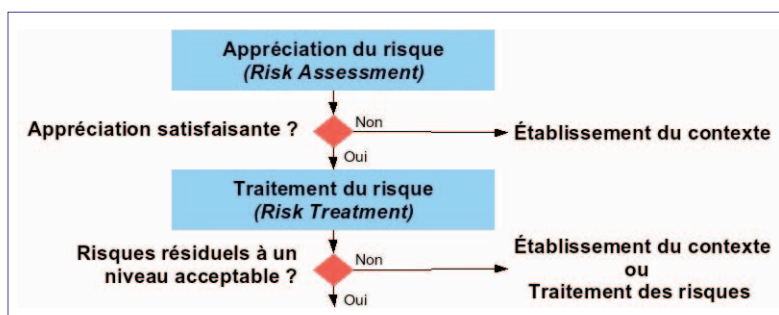
L'annexe F précise toutes les contraintes à intégrer lors de la réduction des risques, notamment lorsque l'on sélectionne des dispositifs de sécurité.

La gestion de risque dans l'ISO 27005 est un processus continu et itératif. Un RSSI qui démarre son appréciation à partir d'une feuille blanche ne commence pas par décider des échelles alors qu'il ne maîtrise pas encore tous les principes. Les critères de valorisation des actifs, d'évaluation des risques, éventuellement les critères d'impact, et les critères d'acceptation des risques, sont explicités dans l'établissement du contexte (chapitre 6) de la norme mais il sont construits au fur et à mesure des processus itératifs et pas séquentiellement au début.

**La norme ISO 27005,
déjà incontournable
au niveau international**

La norme insiste sur deux points de décisions, soit le

travail est satisfaisant, soit il faut réitérer. Cette approche itérative améliore la finesse de l'analyse à chaque itération, fournit une bonne répartition entre le temps et l'effort fourni pour identifier les



mesures de sécurité, permet de traiter les risques en fonction des ressources et moyens disponibles, facilite les liens entre les risques et les conséquences sur les métiers, permet d'avancer lorsque les interlocuteurs sont absents, en facilitant la gestion des susceptibilités et des aspects politiques entre interviewés. L'approche itérative de l'ISO 27005 permet à la gestion de risques de tendre progressivement vers une maîtrise des risques de haut niveau et conforme aux besoins de l'organisme.

L'ISO 27005 fait entrer la gestion des risques pour la SSI dans la gestion de risques en général. Toute direction générale doit mettre en oeuvre une gestion globale des risques pour atteindre les objectifs de l'organisme. Avec l'ISO 27005, la gestion des risques en sécurité de l'information se rapproche des risques opérationnels, industriels, financiers, etc.

Cette nouvelle norme est une méthode complète de la gestion du risque de la sécurité de l'information. Elle est cohérente avec les autres normes ISO de la famille 2700x. Elle permet une gestion simple, pragmatique et adaptée aux besoins de sécurité de tous les métiers ; il n'y a pas de processus linéaire à suivre et peu d'obligations dans le formalisme. Elle est neutre sur les méthodes d'évaluation qualitative et quantitative. Cette norme est supportée par de nombreux produits commerciaux, déjà plus d'une dizaine sur le papier, cependant le tableur demeure l'outil le plus performant et le plus utilisé. En France, l'organisme de certification LSTI propose une certification individuelle "ISO 27005 Information Security Risk Manager" et plusieurs entreprises comme HSC ont annoncé la formation correspondante. Enfin l'ISO 27005 est recommandée pour la mise en place d'un SMSI selon la norme ISO 27001, et elle est d'ores et déjà incontournable au niveau international.