ANNE **LUPFER**

Préface de **Hervé Schauer**

Gestion des risques en sécurité de l'information

Mise en œuvre de la norme ISO 27005

 ISBN : 978-2-212-12593-1

EYROLLES

Préface

La norme ISO 27001 permet d'organiser sereinement la sécurité de son système d'information sous forme d'un système de management de la sécurité de l'information (SMSI). Cette norme ISO 27001 impose une approche par la gestion des risques, et l'obligation de réaliser une appréciation des risques est une caractéristique fondamentale, en opposition avec les approches conformité. L'ISO 27001 précise en un peu plus d'une page ce que doit obligatoirement comporter une gestion des risques en sécurité de l'information. C'était un peu léger et la norme ISO 27005 est venue combler ce manque en détail, tout en allant plus loin, car l'ISO 27005 s'applique non seulement aux SMSI mais à tout type de situation, de manière autonome, tel un système embarqué, par exemple.

De nombreuses méthodologies avaient été développées tant en France qu'ailleurs, et désormais l'ISO 27005 propose une méthode structurée et normalisée, une approche qui se définit elle-même dans la norme comme systématique, c'est-à-dire une approche répétable, que l'on peut apprendre par une procédure pas à pas. L'ISO 27005 est simple à comprendre – il n'y a aucune notion très complexe, elle utilise un vocabulaire conforme au langage courant et cohérent de bout en bout –, elle est pragmatique et accessible à tout type d'organisme, adaptée à la réalité complexe des sociétés actuelles, et permet de produire un travail exploitable et utile rapidement sans aucune étape irréalisable, même si la précédente n'est pas terminée.

La gestion des risques en sécurité de l'information est une approche courante en France, mais pas partout dans le monde. Aux États-Unis, par exemple, il est plus courant de voir une gestion des risques opérationnels d'un côté et une gestion des risques purement informatiques de la DSI de l'autre (exemple : RiskIT), et moins une approche globale sécurité de l'information gérée par le RSSI (responsable de la sécurité des systèmes d'information). La méthode ISO 27005 devrait permettre une meilleure compréhension à travers le monde. L'ISO 27005 a fait des choix structurants, comme l'approche par scénario d'incidents, qui la rendent facilement accessibles à ceux qui utilisaient des méthodes françaises comme Mehari ou Ebios, alors que la norme américaine NIST SP 800-30 n'avait pas cette caractéristique.

L'ISO 27005 apporte une nouveauté fondamentale par rapport aux méthodes qui l'ont précédées : la gestion des risques dans la durée, dans le temps. Il ne s'agit plus de gérer les risques en y travaillant dur quelques semaines, puis en recom-

mençant son travail quelques années plus tard, mais de gérer les risques en sécurité de l'information au quotidien. Ce changement majeur est imposé par l'approche continue de l'ISO 27001, mais il représente le principal changement par rapport aux méthodes antérieures.

L'ISO 27005 est également la première méthode qui impose à la direction générale d'être parfaitement informée, et lui impose de prendre ses responsabilités en toute connaissance de cause, ce qui clarifie les responsabilités et facilite les arbitrages budgétaires.

L'ISO 27005 est une norme dont l'élaboration a imposé de nombreux brouillons successifs pour obtenir un consensus international. Anne Lupfer m'a suivi et m'a accompagné dans mes lectures et commentaires de ces brouillons au sein de la normalisation. Anne Lupfer est entrée chez HSC avec une expérience de gestion des risques dans l'assurance. Elle a créé la formation à la gestion des risques en sécurité chez HSC et a été l'une des premières à mettre en œuvre concrètement la méthode ISO 27005 en clientèle.

C'est à la fois son expérience sur le terrain et ses échanges avec les stagiaires que nous avons eu le plaisir de préparer à la certification « ISO 27005 Risk Manager » que vous retrouverez dans cet ouvrage. Et comme toutes les normes, l'ISO 27005 est peu didactique, payante de surcroît, et vendue plus chère que ce livre qui offre en plus une partie entière d'exemples concrets.

Hervé Schauer

Table des matières

Partie I – La norme ISO 27005

Partie II – Les études de cas

Partie III – La norme ISO 27005 et les autres référentiels

Avant-propos

La gestion des risques est une discipline pratiquée depuis fort longtemps dans l'industrie ou l'assurance. Cette dernière en a même fait son cœur de métier ! Depuis quelques années, les entreprises adoptent des méthodes de pilotage de l'activité par les risques et les écoles enseignent une nouvelle matière : la gestion du risque. Cette science, appelée science des cindyniques, reste tout de même peu accessible et peu documentée, ce qui entraîne de fortes disparités entre les entreprises et les quelques méthodes existantes. Le domaine de la sécurité de l'information ne fait pas exception et ne possède que très peu de méthodes de gestion des risques.

La publication de la norme ISO 27005 est probablement le début d'un changement majeur dans le domaine de la sécurité de l'information. Cette norme facilite la gestion des risques : en s'adaptant à tous les contextes, elle est un des meilleurs atouts pour réussir une analyse des risques.

À qui s'adresse cet ouvrage ?

Cet ouvrage s'adresse à toute personne souhaitant maîtriser les risques de son activité. Si vous êtes décideur, vous devez prendre en compte tous les risques afférents à votre champ de responsabilités. Les risques en sécurité de l'information sont donc dans votre périmètre. Grâce à ce livre, vous appréhenderez concrètement les problématiques de gestion des risques en sécurité de l'information. Vous apprendrez notamment comment les intégrer à une gestion des risques globaux.

Si vous êtes amené à convaincre votre responsable ou même la Direction de mener un projet, de réaliser des investissements ou tout simplement de prendre certaines décisions, cet ouvrage vous donnera les moyens d'accomplir votre mission. Vous découvrirez les méthodes pour faire passer des messages forts et marquants qui feront immédiatement adhérer la Direction à votre cause.

Si vous avez la charge d'identifier les risques pour votre activité, ce livre vous donnera les éléments pour y parvenir avec ou sans méthode imposée par votre hiérarchie. Vous discernerez les subtilités de la gestion des risques, vous permettant ainsi d'éviter tous les pièges et de franchir avec succès les obstacles. Cet ouvrage vous transmettra les clés de la cohésion des résultats.

De plus en plus, la gestion des risques est centralisée dans les entreprises. Tous les risques (risques juridiques, risques métier, risques informatiques, etc.) sont traités ensemble, en suivant une seule méthode, par des personnes clés de l'entreprise. Vous êtes donc acteur de ce processus. Cet ouvrage vous permettra d'identifier les risques en sécurité de l'information les plus stratégiques pour votre entreprise.

Des éléments de diverses méthodes de gestion des risques telles que Mehari et Ebios sont intégrés dans cet ouvrage de manière à vous encourager à les utiliser intelligemment. Ainsi, vous pourrez construire une méthode de gestion des risques parfaitement adaptée à votre contexte ainsi qu'à vos objectifs. Tous les éléments nécessaires à la construction de votre méthode de gestion des risques vous seront communiqués.

Par le traitement de cas réels, nous vous aiderons à répondre aux problématiques de hiérarchisation des risques et de leurs traitements. L'ouvrage porte sur la norme ISO 27005:2008 mais ne nécessite des connaissances ni des normes ISO 2700x ni de la gestion des risques.

> **Convention**
>
> L'année de parution de la norme est stipulée après la référence de la norme. Dans cet ouvrage la version publiée en 2008 est utilisée. Concernant la norme ISO 27001, la version de 2005 est employée en référence. Nous respecterons cette convention mais des écarts peuvent être faits sans remettre en cause la compréhension.

Structure de l'ouvrage

Cet ouvrage, divisé en trois parties, aborde dans un premier temps le texte de la norme. En suivant une structure identique à celle-ci et en intégrant les annexes au fur et à mesure, il facilite la manipulation du texte normatif. Bien entendu, le processus de gestion des risques en sécurité de l'information étant par nature itératif dans la pratique (ce que nous verrons par la suite), cet ouvrage fera office de guide dans les allers-retours nécessaires entre les différents éléments de la norme.

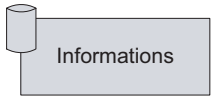
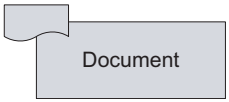
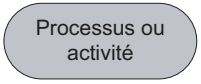
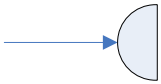
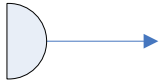
La deuxième partie est consacrée à la mise en application sur le terrain. Elle s'affranchit de la structure rigide de la démarche et permet d'aborder la gestion des risques en entreprise.

Enfin, nous n'avons pu faire l'économie d'une dernière courte partie, consacrée à la compatibilité de la norme ISO 27005 avec les autres normes ISO et la gestion des risques en général.

Pour faciliter la lecture, chaque sous-processus de la norme fera l'objet d'une présentation concise avant d'être détaillé selon la structure suivante : entrées, activités, sorties. Ces paragraphes seront agrémentés d'encadrés permettant de préciser certains éléments tels que les bonnes pratiques ou la conformité à la norme ISO 27001:2005.

Pour faciliter la compréhension des concepts, nous proposons de nombreux schémas, qui recourent aux conventions résumées dans le tableau ci-après.

Convention de lecture des schémas

Schéma	Intitulé	Description
	Informations	Ce pictogramme symbolise les informations. Ces informations peuvent se situer en entrée ou en sortie d'une activité ou d'un processus.
	Document	Ce pictogramme symbolise les documents. Les documents peuvent être utilisés en entrée d'une activité ou d'un processus et être produits en sortie d'une activité ou d'un processus.
	Processus ou activité	Ce pictogramme symbolise les processus ou les activités du processus de gestion des risques.
	Entrée	Cette flèche symbolise le sens de direction vers l'activité ou le processus. Dans ce cas, les documents ou informations sont des éléments d'entrée du processus ou de l'activité.
	Sortie	Cette flèche symbolise le sens de direction depuis l'activité ou le processus. Dans ce cas, les documents ou informations seront des éléments de sortie du processus ou de l'activité.

À propos de l'auteur

Son diplôme d'ingénieur décroché, Anne Lupfer rejoint une société de conseil spécialisée en sécurité de l'information. Après quelques missions techniques, elle s'oriente vers la gouvernance de la sécurité des systèmes d'information et la mise en œuvre de la norme ISO 27001.

La parution de la norme ISO 27005 lui permet d'approfondir le sujet passionnant de la gestion des risques en sécurité de l'information. Elle conçoit plusieurs formations et publie quelques articles sur le sujet. Non satisfaite de ne pas pratiquer pleinement, elle devient chef de projet dans une entreprise française, ce qui lui permet de gérer les risques métiers quotidiennement et de mettre ainsi en pratique la théorie.

Site web

Retrouvez Anne Lupfer pour échanger sur le livre et la gestion des risques sur le site : http://anne-lupfer.com

Chapitre 1

Une norme bien particulière

La norme ISO 27005, au contraire des autres référentiels en gestion des risques, permet de construire des résultats qui évoluent avec l'organisme. Tout changement mineur ou majeur peut être intégré dans le processus de gestion des risques. Grâce à elle, finis les résultats obtenus après des mois de dur labeur que personne n'ose faire évoluer, au risque de travailler à des éléments obsolètes !

Ce chapitre se base sur les paragraphes 5, 6 et 8.2.2 et sur l'annexe E de la norme ISO 27005.

La norme ISO 27005 se distingue des autres méthodes de gestions des risques en adoptant :

- un processus continu qui vit au fil des années ;
- une amélioration continue qui se base sur la roue de Deming mais pas uniquement ;
- un niveau de détails fortement lié au contexte et aux objectifs de la démarche ;
- un processus itératif qui vise à affiner les résultats à chaque itération.

> **Qu'est ce qu'un processus ?**
>
> Un *processus* est formé d'une action ou d'une suite d'actions utilisant des éléments en entrée et permettant la construction d'éléments en sortie. Les processus sont souvent en entrée d'autres processus, car un processus est rarement isolé : il interagit avec les autres processus. La norme ISO 27005 suit cette logique en décrivant le processus global de gestion des risques.

La gestion des risques en sécurité de l'information : un processus perpétuel

Le processus de gestion de la sécurité de l'information doit être un processus continu dans lequel le processus de gestion des risques en sécurité de l'information devra s'inscrire. Ce processus couvre la définition des objectifs, des contraintes, l'appréciation des risques et leurs traitements en utilisant un plan de traitement des risques pour mettre en œuvre les recommandations et les déci-

sions. La gestion des risques permettra d'analyser ce qui peut se produire et quelles en seront les conséquences pour l'organisme avant de décider ce qui doit être fait et de réduire les risques à un niveau acceptable défini par l'organisme lui-même.

Le processus de gestion de la sécurité de l'information doit contribuer à :

- identifier les risques ;
- estimer les risques en termes de conséquences sur le métier et de probabilité d'occurrence ;
- communiquer autour de ces conséquences et des probabilités d'occurrence ;
- s'assurer de la compréhension par chacun ;
- établir les priorités entre les actions visant à traiter les risques ;
- établir des priorités dans les actions pour réduire les occurrences des risques ;
- impliquer les parties prenantes dans les prises de décisions et les informer des niveaux des risques ;
- suivre l'efficacité des mesures de traitement du risque ;
- superviser le processus de gestion des risques ;
- sensibiliser l'ensemble des équipes à la notion de risque et aux actions à conduire pour les maîtriser.

Toutes ces actions doivent tenir compte des changements et peuvent être conduites sur l'ensemble de l'organisme ou sur un sous-ensemble.

Une amélioration continue dans la maîtrise des risques

La norme ISO 27005:2008 adopte le modèle d'amélioration continue *plan-do-check-act* (PDCA). Ce modèle est fondé sur quatre phases :

- *plan* (planifier) : prévoir ce qui doit être réalisé en fonction des objectifs ;
- *do* (faire) : mettre en œuvre les actions planifiées ;
- *check* (contrôler, vérifier) : s'assurer de la mise en œuvre des actions et de leur adéquation avec les objectifs ;
- *act* (agir) : définir les actions correctives et préventives suite aux contrôles.

Ces quatre phases s'enchaînent soit séquentiellement, soit simultanément, ce qui permet l'emploi de ce modèle sur l'ensemble d'un processus et de ses sous-processus simultanément.

Ceci présente l'avantage, pour le gestionnaire des risques, de proposer une méthode adaptée au contexte de l'entreprise tout en s'améliorant au fil du temps.

Par l'application de ce modèle, la norme ISO 27005:2008 se conforme aux exigences de la norme ISO 27001:2005 et, par conséquent, elle s'intègre pleinement dans un processus de gestion de la sécurité de l'information.

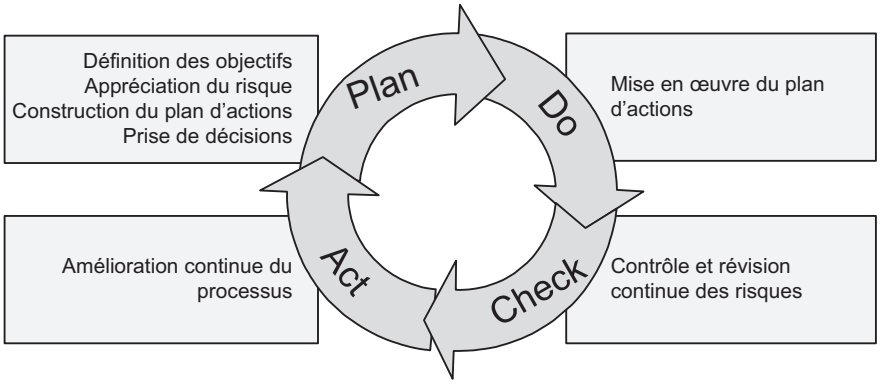


Figure 1-1 : Alignement du processus de gestion des risques dans le SMSI

De la flexibilité

La norme ISO 27005:2008 tente de s'adapter à un maximum d'organismes possédant des objectifs et des moyens variés. Pour ce faire, la démarche propose de jouer sur les niveaux de détails accordés aux résultats et aux différentes étapes. Deux grands niveaux se démarquent (aboutissant à deux démarches distinctes) : haut niveau et niveau détaillé. Ces niveaux seront employés en fonction du niveau de maîtrise de l'organisme. Tout organisme tendra progressivement vers une démarche fournissant des résultats de plus en plus détaillés. Le processus de gestion des risques décrit par la norme ISO 27005:2008 sera adapté en fonction des objectifs.

Deux éléments distinguent ces deux démarches : les résultats obtenus et les activités réalisées dans le cadre du processus de gestion des risques. Une démarche dite « de haut niveau » fournira des résultats tournés vers la stratégie de l'organisme, au détriment des aspects technologiques. Cette démarche permet d'adresser des risques génériques par domaine, activité ou processus. À l'issue de la démarche dite de haut niveau, des dispositifs de sécurité peuvent être proposés. Ils seront choisis de manière à être communs et valides à tout le système. Cette démarche consiste donc à mener une analyse par grandes lignes à l'inverse de l'appréciation détaillée des risques, qui nécessite, comme son nom l'indique, de rentrer dans les détails.

La démarche détaillée traitera des risques liés aux actifs ou à des groupes d'actifs. En fonction de la précision des résultats attendus, cette démarche

demande des efforts considérables et l'intervention d'experts. De fait, contrairement à l'appréciation de haut niveau, l'appréciation détaillée offre une garantie d'exhaustivité.

Le choix de l'une ou l'autre de ces approches sera fonction des objectifs et des moyens de l'organisme. Une appréciation des risques de haut niveau sera privilégiée pour la définition des priorités et l'ordonnancement des actions. Lorsque les moyens financiers sont limités, les deux approches sont combinées. Lorsque les délais impartis et les ressources sont disponibles, l'accent est mis sur l'appréciation de haut niveau qui permettra de mener des appréciations détaillées sur des sous-ensembles identifiés. Dans un premier temps, une appréciation de haut niveau est conduite. Dans un deuxième temps, une appréciation détaillée des risques devra être menée sur les risques identifiés comme prioritaires.

Le tableau ci-joint illustre ces propos et permet de choisir quelle démarche utiliser.

Tableau 1-1 : Choix de la démarche

	Appréciation des risques	
	haut niveau	**détaillée**
Positionnement temporel		
Décalage de temps important (supérieur à 1 an) entre le choix de la démarche et le déploiement des mesures de sécurité	1er temps	2e temps
Uniformisation des différentes démarches de l'entreprise	1er temps	2e temps
Intégration de la démarche dans d'autres projets tels qu'un plan de continuité d'activité ou un projet de sous-traitance	1er temps	2e temps
Identification des risques dans un projet		1er temps
Possibilités de la démarche		
Identification et évaluation des actifs, des conséquences sur les actifs et de leurs vulnérabilités		X
Identification de dispositifs de sécurité liés à l'organisation et au management	X	
Constitution d'un calendrier de mise en œuvre de l'organisation autour de la sécurité de l'information et du processus de gestion des risques	X	

> **Bonne pratique : choisir les outils**
>
> Dans le cas d'un projet de déploiement d'un outil de gestion d'incidents, l'identification détaillée des risques permet d'évaluer le niveau de sensibilité de la base d'incidents. Si le niveau est faible, tous les outils et solutions informatiques répondront aux contraintes de sécurité à appliquer sur la base d'incidents. En revanche, si un besoin de confidentialité fort est requis, des dispositifs de sécurité, parfois difficiles à mettre en œuvre, seront demandés.

Le tableau précédent met en avant le fait que dans la majorité des cas, le processus de gestion des risques débute par une appréciation de haut niveau. Cependant, la gestion des risques dans les projets fait exception à la règle. Dans ce cas, les risques seront immédiatement détaillés de manière à orienter rapidement le projet et à formuler les exigences sécuritaires.

> **Pour être conforme à la norme ISO 27001**
>
> La norme ISO 27001 demande de mettre en place une organisation de la sécurité de l'information au sein de l'organisme. Pour répondre à cette exigence efficacement, la meilleure solution est d'adopter une appréciation des risques de haut niveau. Ceci présente l'avantage de réaliser une première itération du processus de gestion de risques exigée rapidement par la norme et de pouvoir ainsi corriger le processus si besoin.

En règle générale, il est intéressant d'adopter une démarche en deux temps. Dans un premier temps, au cours d'un processus de haut niveau, seront identifiés les domaines pour lesquels les améliorations en termes de sécurité de l'information sont les plus nécessaires. Dans un deuxième temps, une appréciation des risques détaillée sera menée sur les domaines et les risques identifiés précédemment comme prioritaires. Cette démarche permet un gain de temps dans les phases d'acceptation de la démarche car la phase de haut niveau sera plus simple que l'appréciation détaillée des risques. Ainsi, l'appréciation des risques de haut niveau peut être adoptée comme un outil pédagogique et de communication.

Ces deux méthodes ont pour point commun la variabilité du niveau de détails des résultats. Dans la suite de cet ouvrage, cet aspect complexe de la gestion des risques sera abordé à plusieurs reprises.

Un processus qui se répète

Comme le montre le schéma global du processus de gestion des risques ci-après et le laisse entendre le paragraphe précédent, le processus de gestion des risques possède la particularité d'être itératif. Cette caractéristique est favorisée par deux points de décision intégrés au processus global de gestion des risques.

Point de décision n° 1 : si les résultats à l'issue de l'appréciation des risques ne sont pas convaincants, le processus de gestion des risques sera repris depuis l'étape d'établissement du contexte.

Point de décision n° 2 : si les résultats à l'issue du traitement des risques ne sont pas convaincants, le processus de gestion des risques sera repris soit depuis l'étape d'établissement du contexte soit depuis l'étape de traitement des risques.

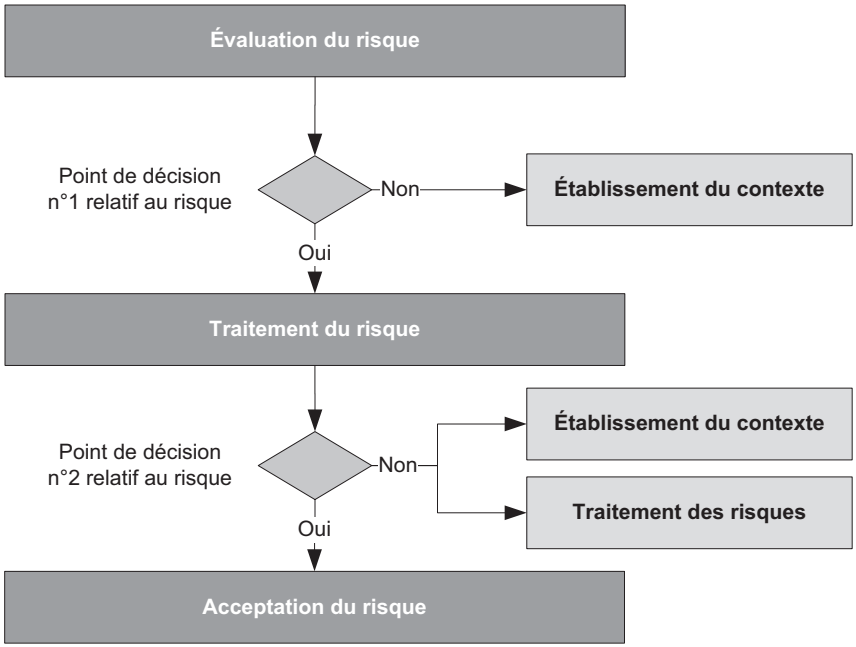


Figure 1-2 : Processus itératif – deux points de décision

Le processus peut être itératif pour l'appréciation des risques et/ou l'activité de traitement des risques. Ceci se traduit concrètement par plusieurs questions.

Au point de point de décision n° 1 :

- est-ce que l'appréciation des risques fournit des résultats satisfaisants ?

Au point de point de décision n° 2 :

- est-ce que les actions de traitement des risques sont réalisables ?
- est-ce que les risques résiduels ont été amenés à un niveau acceptable ?

> **Bonne pratique : prendre des décisions**
>
> Au risque de choquer le lecteur, si la réponse à la question précédente (« Est-ce que les risques résiduels ont été amenés à un niveau acceptable ? ») est : « non, seulement 10 % des risques ont été réduits à un niveau acceptable », deux solutions s'offrent alors au gestionnaire des risques : réduire les seuils d'acceptation des risques (phase d'établissement du contexte) ou proposer des mesures de sécurité supplémentaires (phase traite-

> ment du risque). Lors des premières itérations, la solution la mieux adaptée à la réalité est la baisse des seuils précédemment établis.
>
> Ce point, d'une forte importance philosophique, sera abordé en détails dans la suite de l'ouvrage.

La dimension itérative du processus de gestion des risques entraîne une amélioration du niveau de détail au fil des itérations, ceci permet de trouver le bon équilibre entre le temps et l'effort fournis pour identifier les mesures de sécurité, tout en s'assurant que les risques importants sont couverts. En pratique, en plus du temps, les facteurs limitatifs seront les ressources financières.

Conclusion

L'ensemble de ces concepts (processus continu, amélioration continue, niveau de détail et processus itératif) contribue à la particularité du processus de gestion des risques tel que décrit dans la norme ISO 27005:2008. Ils permettent la souplesse et la maniabilité de la norme et facilitent ainsi son adaptation et son utilisation. Grâce à ces concepts, le gestionnaire des risques maîtrise parfaitement les résultats et se trouve dans une optique différente de celle proposée par les autres méthodes. Quand d'autres méthodes sont très longues à initialiser et demandent des travaux d'inventaire pour obtenir une photographie de l'ensemble des risques sur un périmètre donné, la norme ISO 27005:2008 recommande de fournir des résultats de haut niveau permettant d'amorcer le processus et de progressivement maîtriser ses risques tout intégrant les évolutions de l'organisme. Cela se traduit, dans le cas des autres méthodes, par un tableau de gestion des risques que l'équipe ne fera pas vivre et sur lequel elle se basera. Bien que devenu obsolète, il sera utilisé pendant des années afin de rentabiliser (parfois inconsciemment) le travail fourni initialement. Avec la norme ISO 27005:2008 le gestionnaire de risques et son équipe feront au contraire vivre les résultats et pourront ainsi répondre à la stratégie de l'organisme. Nous faisons ici abstraction de la difficulté que peut comporter une méthode classique de gestion des risques dans l'évolution des résultats.

Chapitre 5

Les risques dans les projets

Souvent cité en exemple dans cet ouvrage, un cas pratique de gestion des risques dans les projets devait être présenté. Ce sera le premier cas traité dans ce chapitre. L'application de la norme ISO 27005 dans le cadre de projets est particulière du fait de la nature des projets par rapport à un processus ou une activité. En effet, un projet a, en moyenne, une durée de vie plus courte qu'une activité ou un processus. Contrairement à ces deux derniers, le projet évolue peu. Ce chapitre a pour objectif d'aider le lecteur à créer sa propre démarche de gestion des risques dans les projets.

Dans le cas présent, l'objectif est d'identifier, en amont du projet, les risques nouveaux que ce dernier est susceptible d'engendrer. Il convient donc de lister les événements pouvant se produire sur le système et causer des dommages. Malheureusement, le gestionnaire des risques a fait le choix de ne pas traiter les risques engendrés par le projet sur le reste de l'entreprise. Ces risques ne sont donc pas dans le périmètre de l'étude. Seuls des risques internes au projet sont abordés par la démarche proposée. Une autre particularité est que les mesures de sécurité sont décidées dès le lancement du projet puis déployées une fois pour toutes.

Le contexte

L'entité française d'un groupe international emploie sa propre méthode de gestion des risques depuis une dizaine d'années. Cette démarche est issue et adaptée de la méthode française Incas (Intégration dans la conception des applications de la sécurité) publiée dans les années 1990. Comme dans tout groupe international, la tendance est à l'homogénéisation des outils de travail. La méthode de l'entité française est retenue comme référentiel de gestion des risques dans les projets car elle a fait ses preuves à plusieurs reprises. Cependant, pour être adoptée mondialement, il est indispensable qu'elle fasse l'objet d'une mise à niveau. La nouvelle méthode devra respecter les principes de la

norme ISO 27005 et les exigences des normes ISO 9001 et ISO 14001. Cette conformité est un argument majeur auprès des autres pays et indispensable pour assurer l'adhésion de l'ensemble des équipes et surtout des entités américaines et japonaises déjà certifiées.

> **Bonne pratique : jouer de ses atouts !**
>
> L'adhésion des employés à la démarche choisie est le premier facteur de réussite. Pour l'atteindre, le gestionnaire des risques doit mettre tous les atouts de son côté. Ces éléments différenciateurs devront être exploités au maximum. Ils pourront par exemple être utilisés comme éléments de communication.

La Direction Générale jugeant la construction de la méthode prioritaire, elle nomme une équipe spécifiquement pour ce projet. Deux jalons sont définis : la création de la méthode et la validation de la méthode.

> **Bonne pratique : choisir les bons arguments**
>
> Souvent dans les entreprises la conformité à un référentiel est utilisée comme argument pour favoriser l'acceptation des méthodes par les employés. Dans la majorité des cas, l'adhésion ne se produit pas et, au contraire, les demandes sont perçues comme des contraintes. La bonne attitude est de promouvoir l'action et de présenter la conformité comme un avantage pour l'entreprise.

La construction de la nouvelle méthode

Dans un premier temps, l'équipe, composée du RSSI à l'origine de l'ancienne démarche et d'un consultant choisi pour sa connaissance des normes ISO, va élaborer la méthode de gestion des risques du groupe ainsi que les outils associés. Avant de s'élancer dans le travail de révision de la méthode existante et puisque l'objectif premier de la méthode est la mise en conformité à la norme ISO 27005, il convient d'identifier les points forts et faibles de la méthode existante et les écarts avec la norme ISO 27005. L'analyse débute par une prise de connaissance de la démarche Incas, ligne directrice de la méthode à moderniser. Elle se poursuit sur l'analyse de la méthode existante afin d'identifier ses forces et faiblesses. Une fois l'analyse réalisée, la nouvelle méthode peut être construite.

Analyse de la méthode Incas

Il est important ici de se servir de l'historique. Se remémorer la méthode Incas est une étape essentielle, qui favorisera la compréhension de la méthode employée permettra de s'assurer et, que les choix de modification d'Incas réalisés sont peut être toujours pertinents. Cette étape est donc susceptible d'augmenter les chances de réussite de l'équipe.

> **Le saviez-vous ?**
>
> En 1992, une démarche d'intégration de la sécurité dans les méthodes de conduite de projet (Incas.V1) est mise à disposition des chefs de projets. Elle est le résultat d'un tra-

vail de René Hanouz pour le Clusif. Puis, en 1996, cette démarche s'affranchit des méthodes de conduite de projet et devient Incas.V2. La démarche est actualisée à partir des modélisations et des standards disponibles sur le marché tels que l'approche Merise, l'approche Objet, etc.

Les critères d'évaluation des risques

Comme toute méthode, Incas s'appuie sur des critères pour attribuer des valeurs aux risques de manière à les comparer. Deux types de critères sont combinés pour obtenir une valeur unique par risque définie dans un tableau de synthèse :

- les besoins de sécurité d'un projet mesurant le niveau de sécurité requis sur le projet ;
- la gravité du risque identifié traduisant l'impact du risque sur le projet.

Mesurer les besoins de sécurité d'un projet

Incas utilise quatre critères de sécurité pour mesurer les besoins de sécurité du projet :

- **la disponibilité,** garantie de continuité de service et de performance des applications, du matériel et de l'environnement organisationnel ;
- **l'intégrité,** garantie d'exactitude, d'exhaustivité, de validité de l'information et de non-modification illicite de l'information ;
- **la confidentialité,** garantie de non-accès illicite en lecture ou de non-divulgation de l'information (papiers, clés USB, portables, etc.) ;
- **la preuve** ou **contrôle,** garantie de contrôle (au sens audit) et de non-répudiation.

Mesurer la gravité d'un risque

Incas définit une grille d'aversion au risque (voir tableau 5-1 : Grille d'aversion au risque) c'est-à-dire le ressenti vis-à-vis du risque qui a pour objectif d'estimer la gravité (ou l'importance) du risque suivant les critères d'impact et de potentialité du risque.

L'interprétation de cette matrice permet de déterminer un niveau de gravité du risque. Incas définit deux niveaux : « faible et accepté » et « inacceptable », tels que décrits dans le tableau 5-2 : Interprétation de la grille d'aversion aux risque.

Si la gravité du risque est estimée comme inacceptable, alors un plan de traitement des risques doit être établi. Ce plan de traitement des risques doit planifier le déploiement des mesures de sécurité adaptées et équilibrées à la gravité des risques et au plan économique. En d'autres termes, les mesures doivent être cohérentes. C'est-à-dire, que pour traiter un risque d'aversion de valeur « 1 », la mesure devra être peu coûteuse et demander de faibles ressources pour le déploiement et le suivi. À l'inverse, pour traiter les risques d'aversion « 4 », la mesure pourra nécessiter de forts investissements financiers, le coût étant relatif à l'entreprise. Il convient d'appliquer une règle simple : les coûts engagés doivent être relatif au niveau d'aversion du risque.

Tableau 5-1 : Grille d'aversion au risque

		Impact			
		1	2	3	4
Probabilité	0	0	0	0	0
	1	0	1	2	3
	2	0	1	3	4
	3	1	2	3	4
	4	1	2	3	4

Tableau 5-2 : Interprétation de la grille d'aversion

Aversion du risque	Gravité du risque
0 ou 1	Faible et acceptée
2, 3 ou 4	Inacceptable

Évaluer les risques

La démarche Incas propose une échelle de référence pour l'évaluation des risques. Cette échelle est reproduite ci-après :

Tableau 5-3 : Échelle d'évaluation des risques

Niveau	Description
4 – Stratégique	Tout incident susceptible de provoquer : des pertes financières inacceptables (ex : centaines de millions d'euros, et milliards) ; • des pertes immédiates d'une activité ou d'un métier de l'entreprise ; • des sanctions judiciaires au plus haut niveau de responsabilité (ex : échecs de négociations de niveau politique ou économique).
3 – Critique	Tout incident susceptible de provoquer : des pertes financières importantes (ex : quelques dizaines de millions d'euros à cent millions d'euros) ; • une nuisance grave à l'image de marque ; • une perte importante de marchés, clientèle ; • une infraction majeure à la législation ; • une nuisance organisationnelle jugée importante sur l'ensemble de l'entreprise ; • une gêne susceptible de fausser les décisions et les orientations des dirigeants.

Tableau 5-3 : Échelle d'évaluation des risques (suite)

Niveau	Description
2 – Sensible	Tout incident susceptible de provoquer : • des pertes financières significatives (quelques centaines de kilo euros à dix millions d'euros) ; • une nuisance significative à l'image de marque ; • une perte significative de clientèle ; • une nuisance organisationnelle jugée significative par l'utilisateur ; • un manquement à la réglementation comptable ou fiscale ; • la non-atteinte des objectifs visés par un projet important.
1 – Faible	Tout incident susceptible d'occasionner de faibles nuisances, interne au domaine considéré et peu gênant pour l'utilisateur.

Remarque

Les données de ce tableau devraient, bien entendu, être relatives à l'organisme et non génériques comme c'est le cas ici !

Concernant l'évaluation du risque, la démarche Incas mentionne qu'une évaluation précise et quantifiée des niveaux de risques n'est possible qu'au fur et à mesure du temps. Cette évaluation s'appuiera en effet sur l'expérience acquise et sur la comparaison entre applications.

La démarche Incas rejoint donc en quelque sorte la norme ISO 27005 puisqu'elle préconise également un processus itératif tenant compte de l'historique et des évolutions.

Les différentes étapes

La démarche Incas se décompose en étapes intervenant à chaque phase clé de déploiement du système étudié. Le schéma ci-après, extrait de la documentation sur la démarche, offre une vue d'ensemble des actions à réaliser.

Le tableau ci-après décrit chacune des étapes de la démarche et les nuance en fonction de l'état d'avancement du projet. Ces variations ne sont pas détaillées

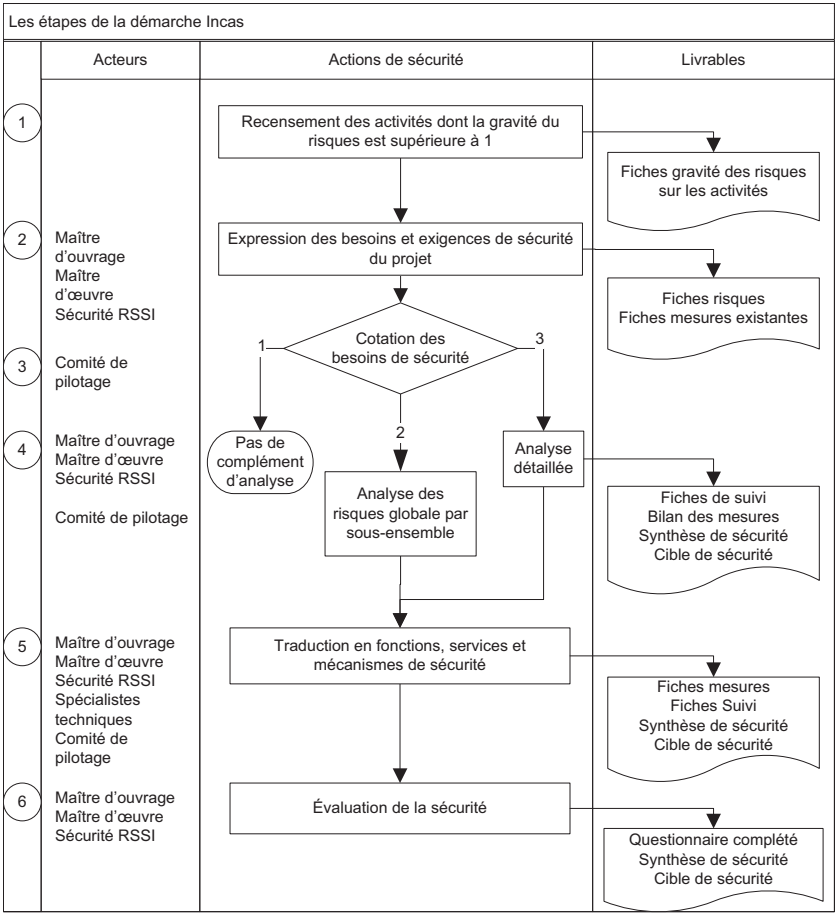


Figure 5-1 : Synoptique de la démarche Incas

dans ce chapitre. Il est conseillé au lecteur de prendre connaissance de la démarche proposée par le Clusif pour approfondir le sujet.

Tableau 5-4 : Les étapes dans la démarche Incas

Étape	Description
1	Le projet est décomposé suivant les activités. Les besoins en confidentialité, disponibilité, intégrité et preuve sont estimés. Ces éléments font l'objet d'une fiche dédiée. Une colonne de justification de la classification des critères de sécurité est prévue à ce document. Les risques survenus sur le système existant peuvent également faire l'objet d'un document.

Tableau 5-4 : Les étapes dans la démarche Incas (suite)

Étape	Description
2	Les risques sont analysés et font l'objet d'une fiche (fiche de risque) comprenant les informations suivantes : • date ; • référence du risque (sous le numéro Rxxx) ; • référence des documents support à l'analyse ; • élément à risque (objet du système d'information) ; • description du risque (accident, erreur, malveillance) ; • conséquences (pertes financières, image de marque, manque à gagner, problèmes juridiques, sociaux, surcharge ou sous charge de travail, etc.) ; • classification suivant les critères disponibilité, intégrité, confidentialité et preuve, type de préjudice, valorisation du risque ; • mesures de sécurité recommandées ; • phase du projet pour la prise en compte de la mesure, responsable de la mesure, coût des mesures de sécurité, modalités de mise en place, classification résiduelle de la gravité du risque. Une fiche permettant d'identifier les mesures de sécurité existantes est également établie. La maîtrise d'œuvre, d'ouvrage et l'équipe sécurité interviennent pour réaliser l'identification des risques et des mesures de sécurité existantes.
3	Les besoins en sécurité suivant les critères de sécurité (confidentialité, intégrité, disponibilité et preuve) sont estimés. Le comité de pilotage intervient sur le choix de traitement du risque.
4	Si les besoins en sécurité sont inférieurs à 1, aucun complément d'analyse n'est réalisé. Des exceptions peuvent être faites si le comité de pilotage le demande. Si les besoins en sécurité ont pour valeur 2, une analyse des risques globale par sous-ensemble est réalisée. Si les besoins en sécurité ont pour valeur 3, une analyse détaillée des risques est réalisée. Cette étape fait l'objet de quatre livrables : fiches de suivi, bilan des mesures de sécurité, synthèse de sécurité et cible de sécurité. Un exemple de fiche de cible de sécurité est présenté dans la suite de ce chapitre.
5	Pour chaque risque identifié, une fiche décrivant les mesures de sécurité par élément est établie. Un exemple de cette fiche est présenté dans la suite du chapitre. Cette étape fait l'objet de quatre livrables : fiches de mesures, fiche de suivi, synthèse de sécurité et cible de sécurité.
6	La sécurité est évaluée à partir d'un questionnaire. Ce questionnaire est disponible dans le manuel de la démarche. Ce questionnaire est complété, une synthèse de sécurité est réalisée et la fiche cible de sécurité est enrichie.

Les documents produits

La démarche Incas propose, en annexe, plusieurs livrables. Ces livrables sont conçus pour dérouler la méthode de bout en bout. Certains de ces documents sont décrits dans cet ouvrage. Le lecteur peut se référer à cette démarche disponible gratuitement sur Internet, s'il souhaite approfondir le sujet.

Les livrables proposés sont intéressants car ils :

- fournissent des grilles d'évaluation et des propositions de pondération ;
- sont exhaustifs et permettent d'éviter les oublis et erreurs ;
- aident à la compréhension de la démarche et par conséquent à son application ;
- présentent une mise en page claire et cohérente permettant de retrouver les informations rapidement. Des emplacements sont prévus pour la validation.

Conclusion

La méthode Incas aide à l'identification des risques dans les projets. Elle impose un niveau d'exigence fort car tous les risques de niveau 2 ou plus sur une échelle de 4 doivent être traités. À première lecture, il n'est pas aisé de la mettre en œuvre. Les exemples de livrables présentés en annexe de la méthode sont très utiles, que ce soit pour l'application d'Incas ou pour la création d'une autre démarche.

Analyse de la méthode existante

La méthode existante dans ce groupe est donc inspirée de la démarche Incas décrite ci-dessus. Dans la suite de l'ouvrage, la dénomination Incas* sera utilisée pour nommer la démarche Incas adaptée par l'entreprise.

Les critères d'évaluation des risques

La méthode utilisée par l'organisme emploie les mêmes types de critères combinés pour obtenir une valeur unique par risque :

- les besoins de sécurité d'un projet mesurant le niveau de sécurité requis sur le projet ;
- la gravité du risque identifié traduisant l'impact du risque sur le projet.

Mesurer les besoins de sécurité d'un projet

Les critères de sécurité décrits par la démarche Incas, c'est-à-dire confidentialité, intégrité, disponibilité et preuve, sont employés tels quels. Sur ce point aucune adaptation n'est réalisée.

Mesurer la gravité d'un risque

Le risque est défini comme étant un événement dont la survenance est possible et porte atteinte à l'entreprise. De la potentialité et de l'impact, définis sur une échelle de 0 à 4, est déduite la gravité du risque. La table d'aversion au risque (voir tableau 5-4 : Synopsis de la démarche existante) définie par la démarche Incas est appliquée.

Cible de sécurité

Projet :

Phase :

Date :

	Disponibilité (D)	Intégrité (I)	Confidentialité (C)	Preuve (P)	Appréciation globale
Objectif pour le futur					
Risques avant mise en œuvre des fonctions et mécanismes de sécurité					
Risques après mise en œuvre des fonctions et mécanismes de sécurité					

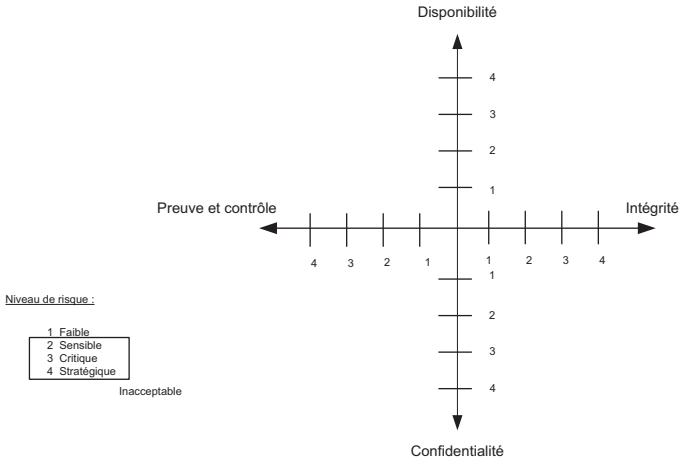


Figure 5-2 : Fiche Cible de sécurité

La valorisation des risques

Contrairement à ce que préconise la méthode Incas, les risques sont valorisés uniquement sur un critère de sécurité. Le concepteur de la méthode estime qu'un risque ne peut avoir d'impacts sur plusieurs critères de sécurité simultanément.

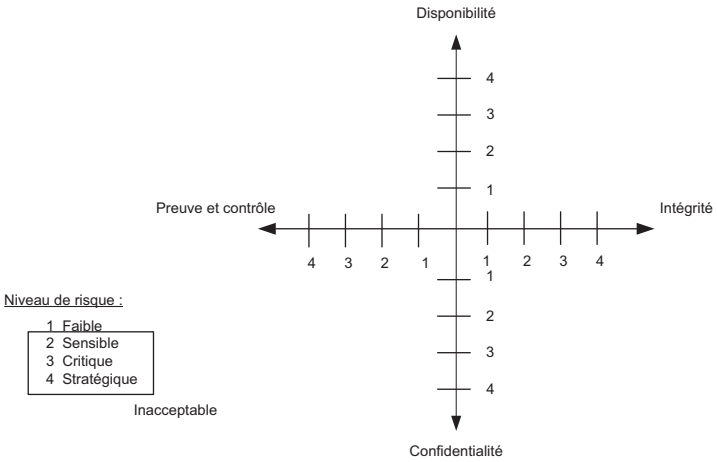
Niveau de sécurité

Projet :

Phase :

Date :

	Disponibilité (D)	Intégrité (I)	Confidentialité (C)	Preuve (P)	Appréciation globale
Risques avant mesures de sécurité					
Risques après mesures de sécurité					
Cible de sécurité du système futur					



Niveau de risque :

1 Faible
2 Sensible
3 Critique
4 Stratégique

Inacceptable

Figure 5-3 : Fiche Niveau de sécurité

> **Remarque**
>
> Cette approche est erronée et dangereuse. En effet, elle ne permet pas d'avoir une vision d'ensemble cohérente et oriente fortement le choix des mesures de sécurité. De nombreux oublis peuvent être commis.

Les risques valorisés suivant le critère de disponibilité ne sont pas intégrés dans la suite de la démarche. Ils sont donc mis de côté. En effet, l'entreprise considère que les risques de ce type entrent dans le périmètre de la continuité d'activité qui fait l'objet de projets à part.

> **Remarque**
>
> Cette approche peut être tolérée si la continuité est réellement gérée, ce qui en pratique n'est que rarement le cas. De plus, le fait de considérer que mettre un onduleur est du ressort d'un plan de continuité d'activité n'est pas viable dans le temps.

Synthèse

L'emploi des critères présente quelques différences par rapport à la méthode Incas qui à première vue sont source d'erreur.

Les différentes étapes

La démarche adoptée est prévue pour s'intégrer à la démarche de gestion de projet existante. La démarche est donc lancée dès la phase de conception du projet. Incas* comporte six étapes présentées sur le schéma ci-après.

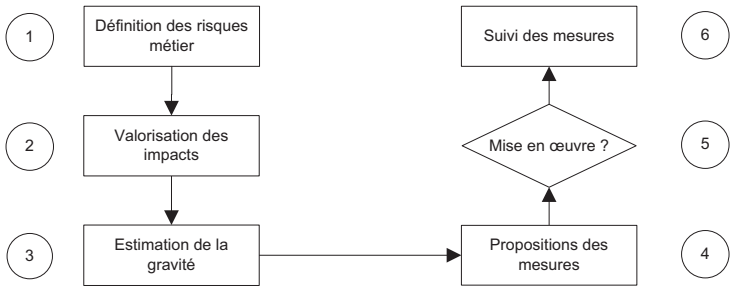


Figure 5-4 : Synopsis de la démarche existante

Les étapes sont les suivantes.

1 Définition des risques métier.

  Comme dans une analyse fonctionnelle, le projet est décomposé en grandes fonctions (limitées par la démarche de 5 à 10). Pour chaque processus, les risques métiers sont identifiés et les liens avec l'informatique mis en avant.

2 Valorisation des impacts.

  Les impacts des risques métier sont valorisés suivants les critères de sécurité.

3 Estimation de la gravité.

La gravité des risques identifiés est estimée suivant la table d'aversion au risque après que la potentialité et l'impact du risque aient été estimés.

4 Proposition de mesures.

Tous les risques inacceptables, c'est-à-dire ayant pour gravité une valeur supérieure ou égale à 2, sont analysés et des mesures de sécurité visant à en réduire l'impact ou la potentialité sont proposées. L'analyse porte sur l'identification des menaces et des vulnérabilités qui sont elles-mêmes revues avec les équipes métiers.
Chaque mesure doit faire l'objet d'une estimation budgétaire. La phase de prise en compte dans le projet ainsi que le responsable de la mesure doivent être mentionnés dans le document approprié.

5 Mise en œuvre.

Une cartographie des risques est réalisée présentant le niveau de risque sans les mesures de sécurité et avec les mesures de sécurité. La cible de sécurité est établie sur un graphique similaire à celui proposé sur la fiche « Cible de sécurité » (voir page 119).
La différence de niveau des risques est confrontée aux coûts. S'en suit une prise de décision par la Direction qui statue pour chaque risque sur le traitement et par conséquent la mise en œuvre des mesures proposées.
Les résultats amendés sont consignés par écrit.

6 Suivi des mesures de sécurité.

Une fiche de suivi des mesures de sécurité est établie. Chacune de ces fiches contient la mesure, son responsable, la phase de prise en compte dans le projet et la date de fin de déploiement. Ce document est utilisé lors de l'audit de suivi des mesures qui a lieu à différents intervalles qui sont fonction de la taille du projet. La fiche de suivi est enrichie des constats de l'auditeur et consignée dans le dossier du projet.

Les documents produits

Chacune des étapes fait l'objet d'un ou plusieurs livrables. Par exemple, chaque risque est détaillé dans une fiche qui lui est dédiée. La fiche reprend les informations suivantes : la nature du risque, le processus concerné, l'impact, la potentialité et le niveau de gravité. Cette fiche est enrichie lors de la phase d'identification des mesures de sécurité, c'est-à-dire leur coût et le niveau de gravité résiduel. Une zone pour l'amendement de la décision y est réservée.

La démarche fait elle-même l'objet d'une présentation sous forme de diaporama dans laquelle les modèles de livrables vierges sont intégrés. Celle-ci est très intuitive : elle permet aux intervenants d'identifier rapidement les tâches à effectuer. Elle intègre et rend disponible d'un simple clic tous les éléments nécessaires (guides d'entretiens, documents vierges et Incas*).

> **Bonne pratique : centraliser les résultats**
>
> Limiter le nombre de documents évite les erreurs et les incompréhensions. Attention toutefois à ne pas surcharger les documents qui peuvent devenir illisibles ou complexes à manipuler.

Conclusion

Incas* présente beaucoup de points positifs tels que la centralisation des informations (modèles de documents et démarche) dans un guide utilisateur, l'implication forte du métier et de la Direction, ainsi que le suivi des mesures. Mais, le manque de clarté dans l'utilisation des termes peut prêter à confusion pour le béotien. La simplification de la démarche et la considération que des risques métier ne tendent pas à l'obtention de résultats fiables et exhaustifs.

Cette analyse permet de conclure que certains éléments existants sont à conserver ou à améliorer et d'autres à créer.

Les éléments pouvant être conservés en l'état sont :

- les modèles de documents ;
- les critères d'évaluation et d'estimation des risques ;
- l'identification par numéro unique des risques pour un report facilité sur une matrice ;
- la définition des rôles et des responsabilités des acteurs dans les différentes étapes du processus.

Les éléments devant être améliorés sont :

- la notion d'impact ;
- les livrables de la méthode dont les plans d'actions.

Les éléments devant être ajoutés sont :

- les besoins en sécurité en relation avec les politiques de sécurité existantes ;
- des catalogues communs à l'ensemble du groupe enrichis au fil de l'eau ;
- une modélisation du processus permettant d'avoir une vision claire des éléments en entrée et sortie.

La démarche adoptée est cohérente mais présente un risque fort d'oubli d'événements liés au projet. De plus, le nombre de documents produits (un différent par étape) rend la démarche complexe à gérer, même sur des projets simples. Pour les projets nécessitant plusieurs intervenants, les risques d'erreurs sont encore plus importants. Cette démarche est bien dimensionnée pour une personne travaillant seule.

Construction de la nouvelle méthode

Pour construire la nouvelle méthode, l'équipe va fixer les objectifs à atteindre et, à partir de l'analyse précédente, proposer des mises à jour.

La définition des objectifs et des moyens

L'objectif principal de la nouvelle démarche, outre l'identification des risques dans les projets, est d'obtenir l'adhésion de tous les acteurs. Les objectifs secondaires, souhaités par le responsable de la future démarche, sont les suivants :

- démarche pragmatique ;
- simplicité d'utilisation ;
- adaptabilité aux différents projets ;

Les moyens pour y parvenir sont les suivants :

- **mise à disposition d'un outil** : ce dernier devra être simple à utiliser et permettre à chacun d'obtenir des résultats exploitables. Cet outil permettra également de comparer les résultats entre les projets afin de fixer des lignes directrices globales à l'entreprise. Pour répondre à ces exigences, l'outil sera développé sur un tableur connu, fortement utilisé dans l'entreprise. Dans l'outil, les activités sont automatisées au maximum et les champs de saisie réduits à leur minimum de manière à limiter les risques d'erreur. Le diagramme des flux est proposé en premier onglet facilitant également la navigation entre les étapes. Chaque étape fera l'objet d'un onglet dans le tableur final. À chaque onglet, un rappel des objectifs de l'étape et des moyens pour y parvenir sera réalisé ;
- **tests de la méthode :** de nombreux tests de la méthode sous la direction du RSSI seront menés sur différents projets pilotes dans l'objectif d'améliorer l'outil et la méthode. En effet, la démarche doit répondre au maximum aux attentes des utilisateurs et fournir des résultats exploitables à tous les niveaux de l'entreprise ;
- **accompagnement au déploiement de la démarche :** par expérience, toute nouvelle méthode nécessite un accompagnement par une personne expérimentée. Par conséquent, une équipe dédiée à la démarche, sous la responsabilité du RSSI, a été constituée. Cette équipe a pour missions de s'assurer de l'utilisation systématique de la démarche dans les nouveaux projets et d'accompagner les équipes projets dans son déploiement ;
- **formation des chefs de projets :** à moyen terme, des formations vont être dispensées aux chefs de projet. Ces formations présenteront la démarche dans les grandes lignes et permettront aux chefs de projet d'en tenir compte lors de l'établissement des plannings liés aux projets.

La proposition

La démarche proposée reprend les éléments décrits précédemment et tente de se conformer à la norme ISO 27005. L'équipe a choisi notamment de reprendre les grandes activités de la norme et de les présenter de manière similaire.

Étape 1 – Définition du contexte

Entrées

Méthode et outil associé, informations sur le projet notamment complexité et volumétrie.

Activités

Cette étape consiste en la définition de la méthode, principalement par l'identification d'adaptations éventuelles et par la création à partir de l'outil des documents qui seront utilisés dans la suite de son application. Au cours de cette phase, un plan d'actions déterminant principalement les personnes à rencontrer, est établi. Si le projet étudié est trop conséquent, il est alors segmenté en sous-processus pour lesquels la méthode sera déployée indépendamment.

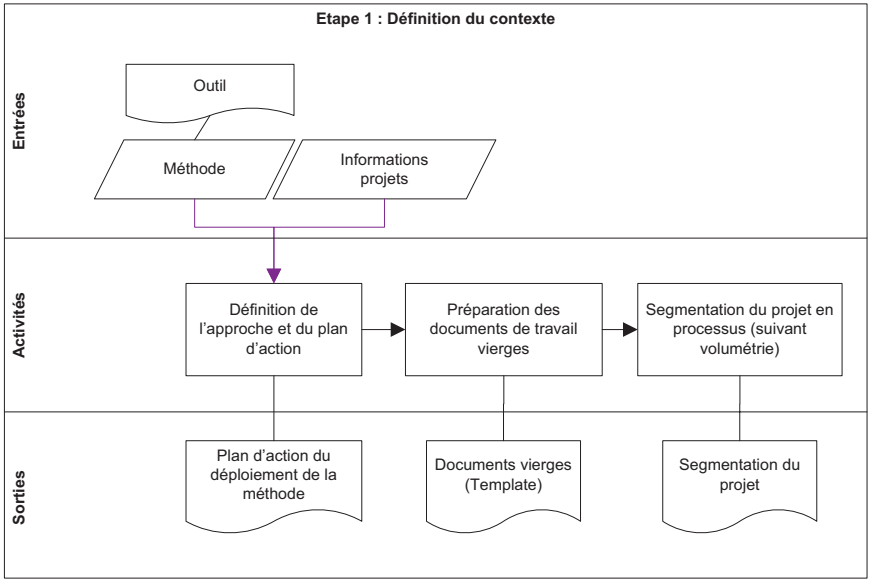


Figure 5-5 : Gestion des risques dans les projets – étape 1

Responsabilités

Le RSSI a l'entière responsabilité de cette étape. Il pourra se rapprocher du chef de projet notamment pour l'élaboration du plan d'actions.

Délais

Le temps à consacrer à cette étape est estimé à deux jours, documentation comprise.

Sorties

Les documents vierges nécessaires à la méthode (*template*) construits à partir de l'outil diffusé.

Nom du projet :	Date:
Version:	

Listes des fonctions

Astuces	Les numéros de fonctions doivent être uniques. Identifiez les grandes fonctions par projet. Masquez cette zone avant impression.

N°	Nom	Description
F1	Fonction 1	Description Fonction 1
F2	Fonction 2	Description Fonction 2
F3	Fonction 3	Description Fonction 3
F4	Fonction 4	Description Fonction 4
F5	Fonction 5	Description Fonction 5
F6	Fonction 6	Description Fonction 6
F7	Fonction 7	Description Fonction 7
F8	Fonction 8	Description Fonction 8
F9	Fonction 9	Description Fonction 9
F10	Fonction 10	Description Fonction 10

Figure 5-6 : Exemple de liste fonction

Le nom du projet, la date et la version sont renseignés automatiquement par un lien avec la page de garde de l'ensemble du classeur.

La zone « rappels » indique les tâches à effectuer, les zones à remplir (différenciées par un code couleur).

Les informations saisies dans cet onglet sont reprises automatiquement dans les onglets où elles sont nécessaires.

Les onglets sont formatés pour tenir sur une feuille A4 lors de l'impression.

Étape 2 – Identification des risques métier

Entrées

Organisation du projet et emploi du temps associé.

Activités

Cette étape consiste en l'identification des risques métier. Pour ce faire, le projet (ou les processus, si le projet le requiert) est segmenté au maximum en dix fonctions (au sens « activité »). Pour chacune de ses fonctions, sont ensuite identifiés des risques ou des incidents pouvant se produire et porter atteinte aux critères de sécurité classiques (confidentialité, intégrité, disponibilité). Dans les premiers temps de la construction de la méthode, la preuve était considérée, mais rapidement ce critère a été supprimé car peu utile dans ce contexte.