SIGMA
PARTNERS

Publication SIGMA Partners

Norme ISO 31000 :

Apports de la norme
dans le management des risques des entreprises

Janvier 2021

SOMMAIRE

SIGMA PARTNERS

INTRODUCTION

- *Pourquoi une norme internationale sur le management des risques ?*
- *Le processus de normalisation*
- *Qui a participé à la révision de la norme ISO 31000 en 2018 ?*

SIGMA PARTNERS

ORIGINE DE LA NORME ISO 31000

QU'EST-CE QUE LA NORME ISO 31000?

La norme ISO 31000 est une **norme internationale sur le management du risque** publiée en 2009 par l'Organisation internationale de normalisation [1]

La norme ISO 31000 désigne une **famille de normes de gestion des risques organisées et codifiées**

Elle vise à **fournir des principes et des lignes directrices du management des risques** ainsi que les **processus de mise en œuvre** aux niveaux stratégique et opérationnel

Elle cherche à **harmoniser la multitude d'approches, de standards et de méthodologies existantes** en matière de management des risques

POURQUOI UNE NORME INTERNATIONALE SUR LE MANAGEMENT DES RISQUES ?

- La **nécessité de créer un standard commun à tous les secteurs d'activité** se fait sentir dans les années 1990.
- **L'Australie et la Nouvelle Zélande** sont les premiers pays à publier un standard en management des risques (As/NZS 4360) en 1995. Elle sera utilisée par le Japon, la Chine et le Canada qui publiera sa propre norme en 1997.
- **La FERMA**[2] publie en **2004** son **cadre de référence de la gestion des risques** tandis que les **États-Unis** publient la même année leur référentiel des bonnes pratiques pour le contrôle interne : le COSO2 [3] prenant en compte l'ERM [4] **.**
- **En 2005,** sous l'impulsion de ces différents membres de l'ISO[2], il est décidé d'**harmoniser le management des risques** par la norme ISO 31000.

(1) L'Organisation internationale de normalisation est une organisation internationale non gouvernementale, indépendante, dont les 165 membres sont les organismes nationaux de normalisation

(2) Federation of European Risk Management Associations

(3) Committee Of Sponsoring Organizations of the Treadway Commission

(4) Entreprise Risk Management

SIGMA PARTNERS

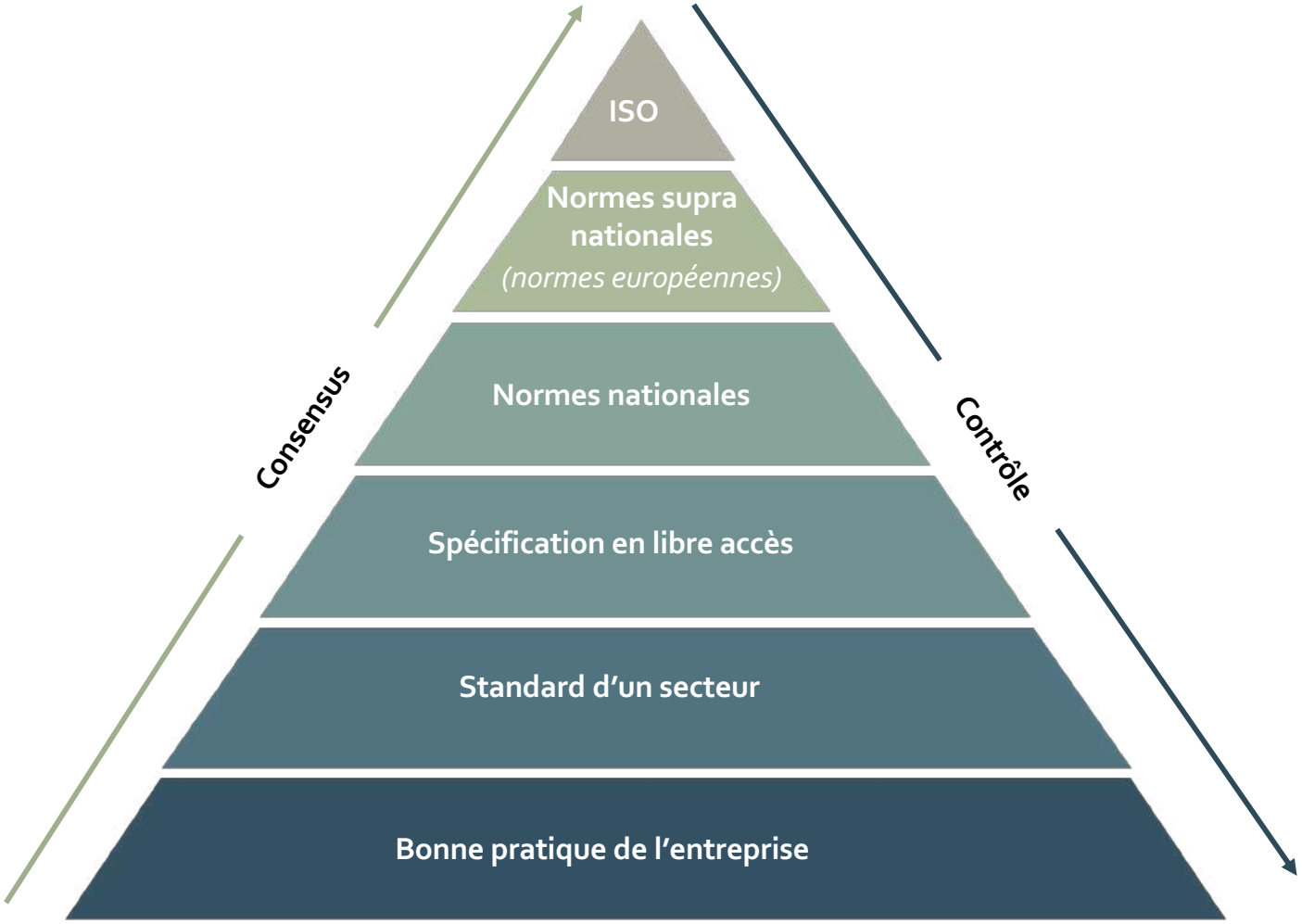
LE PROCESSUS DE NORMALISATION

6 ETAPES

Une norme ISO se construit en six étapes :

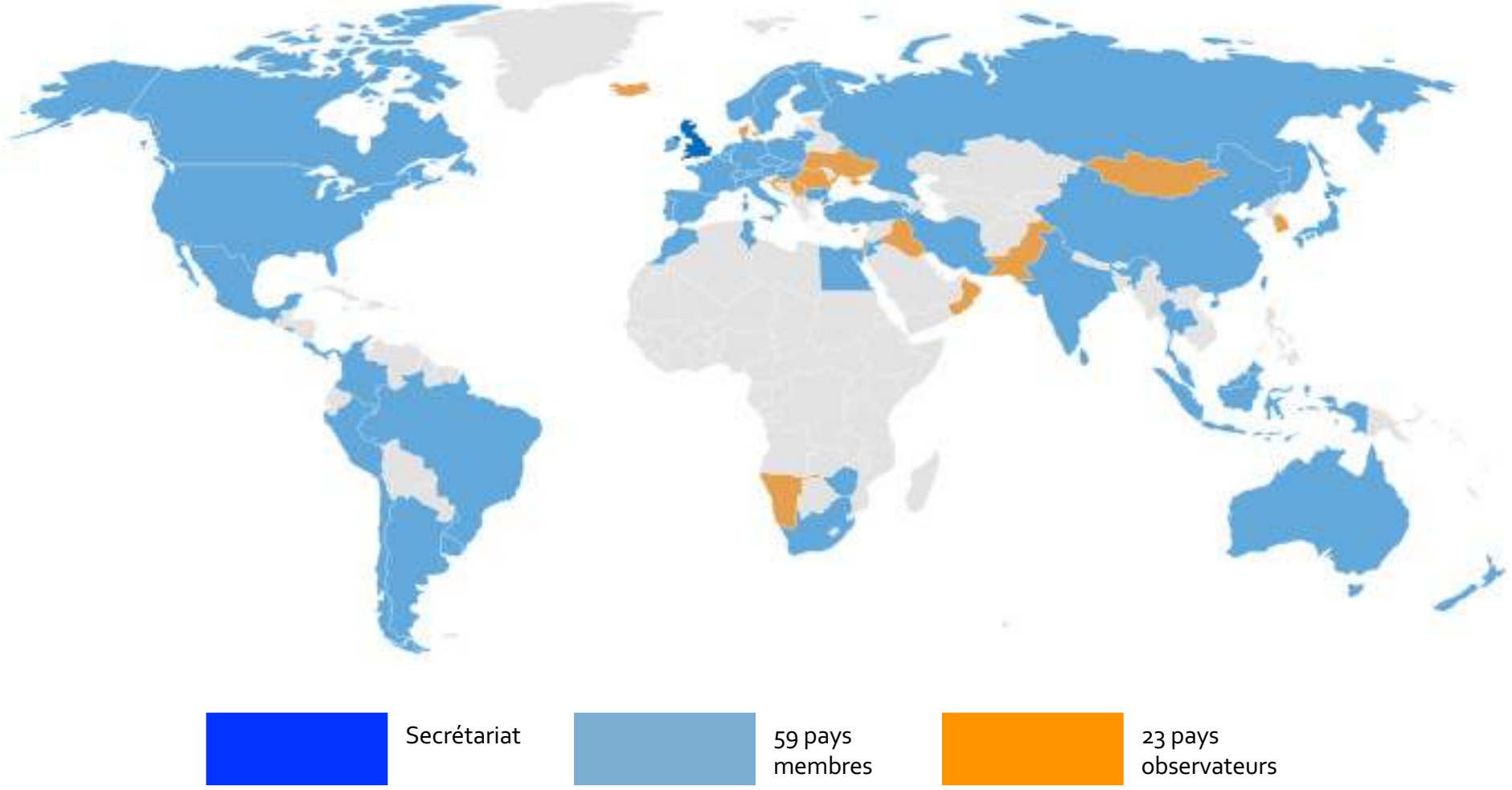
1. **La proposition** qui consiste à confirmer qu'il existe un besoin
2. **La préparation** durant laquelle un groupe de travail est mis en place pour préparer le projet
3. **Le comité** qui rédige la norme au format ISO
4. **L'enquête** durant laquelle le projet de norme est soumis aux divers comités
5. **L'approbation** qui valide le projet final de la norme internationale est soumis au vote
6. **La publication du** texte par le Secrétariat Central de l'ISO

La normalisation à l'échelle internationale se fait par consensus (qui n'est pas l'unanimité), il ne s'agit donc pas de trouver un compromis entre l'opinion de tous les experts de chaque pays qui y contribuent, mais de définir le dénominateur commun sur un sujet.



QUI A PARTICIPE À LA RÉVISION DE LA NORME ISO 31000 EN 2018?

LES PAYS AYANT PARTICIPE A LA REVISION DE LA NORME EN 2008



UNE NORME
POUR TOUTES LES ORGANISATIONS

- *L'ISO 31000, une norme chapeau*
- *Domaines d'application*
- *Les 3 volets de la norme ISO 31000*
- *Un standard mondialement reconnu*
- *Les débuts difficiles de l'ISO 31000 en France*

SIGMA PARTNERS

L'ISO 31000, UNE NORME CHAPEAU

DE MULTIPLES NORMES

Il existe de multiples normes construites sur un modèle commun (HLS 1) afin de maîtriser les risques propres à certains domaines :

- ISO 90xx : Management de la qualité
- ISO 140xx : Management environnemental
- ISO 550XX : Management gestion d'actifs
- ISO 270xx : Management des technologies de l'information

SPECIFICITES DE L'ISO 31000

La norme ISO 31000 permet d'aborder le management global des risques dans tout type d'organisme en s'appliquant à toutes les autres normes volontaires de management par sa vision transversale et par une harmonisation des différentes approches, standards et méthodologies en matière de management des risques.

UNE NORME FAITIERE

La norme ISO 31000 est la norme faitière d'une famille de normes régulièrement révisées :

31010	Management des risques – Technique d'évaluation des risques
31022	Management des risques – Lignes directrices relatives au management du risque juridique
31030	Gestion des risques liés aux voyages – Recommandation pour les organismes
31050	Guidance for managing risks to enhance resilience [5]
31070	Management des risques – Lignes directrices sur les concepts clés [6]
31073	(Anciennement guide 73) Risk management – Vocabulary [5]

[5] *En cours de conception*

[6] *Consultation en cours*

SIGMA PARTNERS

OBJECTIFS DE LA NORME

1 PARTAGER UN LANGAGE COMMUN

L'objectif premier de la norme ISO 31000 est de **proposer un langage commun et unifié sur les risques** en se positionnant comme un **cadre de référence** avec un niveau d'abstraction élevé. Avant sa diffusion, le langage sur les risques était dépendant des risques traités et des secteurs d'activité.

2 PROPOSER UN REFERENTIEL UNIQUE

La norme ISO 31000 vise à **s'appliquer à toute organisation,** i.e à « tout public, toute entreprise publique ou privée, toute collectivité, toute association, tout groupe ou individu ».

Elle propose un **référentiel unique** pour les organisations de tout secteur et de toute taille

3 HARMONISER LES PROCESSUS DE MANAGEMENT DES RISQUES

La norme est **adaptable et suffisamment flexible pour harmoniser les processus de management** de tous les types de risques faisant peser une incertitude sur l'atteinte des objectifs de l'entreprise.

4 EVITER LA GESTION DES RISQUES PAR « SILOS »

L'approche proposée par la norme ISO 31000 permet de **formaliser les pratiques de management des risques**, tout en permettant aux entreprises de **mettre en place un cadre ERM** (Enterprise Risk Management) évitant ainsi une approche de management des risques par « silos ».

**La norme ISO 31000 ne vise en aucun cas à uniformiser les pratiques,
ni à créer un système de management parallèle.
Elle n'a pas vocation à servir de base à une certification mais se définie plutôt comme un guide méthodologique**

SIGMA PARTNERS

LES 3 VOLETS DE LA NORME ISO 31000

Des principes

- L'ISO 31000 met en avant des principes de management des risques qui visent à définir son utilité
- Ces principes précisent notamment que le management des risques crée de la valeur ou à minima préserve la valeur de l'organisation

Un cadre organisationnel

- Elle explique comment intégrer, par le processus itératif de la roue de Deming (Plan-Do-Check-Act), le management des risques dans la stratégie de l'organisation (conduite stratégique)
- Elle vise à permettre à l'organisation de s'adapter en permanence à son contexte externe et interne

Un processus

- Elle précise **comment intégrer le management des risques au niveau opérationnel** de la stratégie de l'organisation (conduite opérationnelle)
- Le processus vise, en suivant des **étapes clairement définies** à **rendre les risques acceptables** au vue de critères choisis et définis par l'entreprise

La norme ISO 31000 propose un référentiel unique pour les organisations de tout secteur et de toute taille.

Elle est adaptable et suffisamment flexible pour harmoniser les processus de management de tous les types de risques.

LES 11 PRINCIPES DU MANAGEMENT DES RISQUES

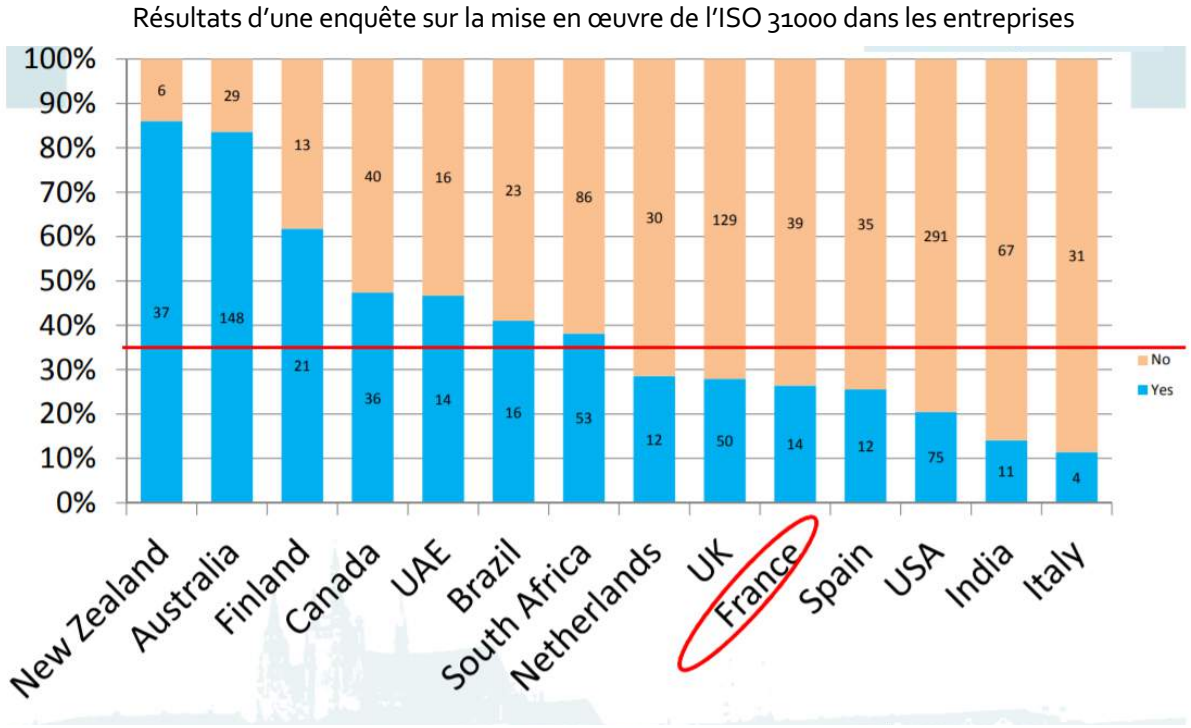
LES 11 PRINCIPES DU MANAGEMENT DES RISQUES SELON LA NORME ISO 31000

- Il crée de la valeur et la préserve
- Il est intégré aux processus d'organisation
- Il est intégré aux processus de prise de décision
- Il traite explicitement de l'incertitude
- Il est systématique, structuré et utilisé en temps utile
- Il s'appuie sur la meilleure information disponible
- Il est adapté à chaque organisation
- Il intègre les facteurs humains et culturels
- Il est transparent et participatif
- Il est dynamique, itératif et réactif au changement
- Il facilite l'amélioration continue de l'organisation

SIGMA PARTNERS

UN STANDARD MONDIALEMENT RECONNU

MISE EN PLACE DE LA NORME ISO 31000 DANS LES ENTREPRISES



Source: Global-survey-ISO-31000-results-final-version4-CARM 5juin12 ((1338 réponses)

DE LA DEFINITION A LA MISE EN OEUVRE

- Chaque norme est rédigée puis régulièrement révisée par un comité d'experts composé d'une trentaine de nationalités différentes
- Puis chaque délégation nationale vote les différentes recommandations proposées par le groupe d'experts
- L'intérêt est de fournir un cadre commun, un vocabulaire commun et une approche commune du management du risque, de façon à permettre une harmonisation des bonnes pratiques à l'échelle planétaire
- Depuis sa publication, cette norme a été adopté par la plupart des grands pays dans le monde (EU, USA, Chine, Inde, Brésil, Turquie, Canada, Australie, …)
- Ce sondage réalisé en 2012, auprès de 1400 entreprises réparties dans 111 pays, établie à 36% le pourcentage d'entreprises engagées dans la démarche ISO 31000
- De très fortes disparités sont tout de même à noter entre des pays largement engagés (NZ, Autiche, Finlande, Canada) et le reste du monde, et demeurent aujourd'hui.

SIGMA PARTNERS

LES DÉBUTS DIFFICILES DE L'ISO 31000 EN FRANCE

UNE CONNAISSANCE DE LA NORME HISTORIQUEMENT TRÈS INÉGALE

- Initialement, la vision Européenne et Américaine de la gestion des risques préconisait des réponses techniques d'atténuation des risques (risque zéro), allant à l'encontre des nouveaux principes de management préconisés par cette norme.
- La norme ISO 31000 s'appuie plutôt sur la vision Japonaise, Australienne et Néozélandaise du traitement des risques : le risque est partout, il faut le traiter, vivre avec et transformer les opportunités qu'il peut engendrer.
- Ainsi, il aura fallu quelques années en France pour que cette norme soit reconnue et acceptée de tous.

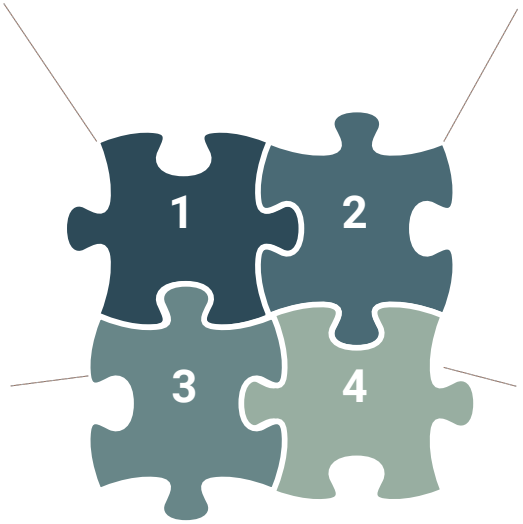
POURQUOI?

INCOMPRÉHENSIONS

La nouvelle définition du risque[7] a perturbé la communauté des managers des risques, notamment ceux travaillant sur les aspects techniques du risque.

DIFFUSION

La diffusion de la norme se fait en France uniquement par l'AFNOR [8], qui compte peu d'experts en management des risques parmi les formateurs agréés. L'ISO 31000 est donc peu valorisée et enseignée.



CONCURRENCE AVEC D'AUTRES STANDARDS

Chaque secteur utilise des standards bien établis pour gérer ses risques, il peut s'agir de normes de management déjà existantes comme l'ISO 9001 ou de référentiels de bonnes pratiques comme le COSO 2.

MÉTIERS À DÉVELOPPER

Le métier de manager global des risques n'est pas encore bien reconnu dans nombre de secteurs. Il est encore vu soit comme un financier, soit un assureur, ou un spécialiste d'un risque donné.

AUJOURD'HUI, LA CONNAISSANCE DE LA NORME PROGRESSE FORTEMENT

- La communauté des risques commence à se structurer dans de nombreux secteurs d'activité. Les métiers de manager des risques, qu'ils soient orientés vers la finance, la conformité ou la sécurité / sûreté, acceptent aujourd'hui que la norme ISO 31000 structure et oriente l'ensemble de leurs activités.
- Grâce aux formations se multipliant autour du sujet de la gestion globale des risques, la norme se démocratise d'année en année.

(7) Cf. page 15 de la publication
(8) AFNOR : Association française de normalisation

SIGMA PARTNERS

LES APPORTS DE LA NORME ISO 31000

- *Une nouvelle définition du risque*
- *Le développement d'un management global des risques*
- *Le traitement de l'incertitude*
- *La mise en place d'un processus de management du risque*
- *Un outil efficace de partage d'une culture commune*
- *Implémenter le management des risques en entreprise en 4 étapes*

UNE NOUVELLE DÉFINITION DU RISQUE

UNE NOUVELLE DÉFINITION

- La norme ISO 31000 introduit la définition d'un risque comme l'**effet de l'incertitude sur les objectifs** d'une organisation.
- Cette définition transforme un management des risques historiquement technique et sectorisé vers une **définition universelle et applicable à tous systèmes de management des risques** par une méthodologie commune.
- L'efficacité dans la maîtrise des risques se situe dorénavant dans le **cadre organisationnel** donné pour la gestion des risques et non plus dans une expertise technique.
- La **notion d'incertitude** introduite **dans la réalisation des objectifs** permet maintenant de voir les risques comme des menaces et/ou des opportunités afin d'englober tous les cas de figure rencontrés dans chaque organisation.

SES APPORTS

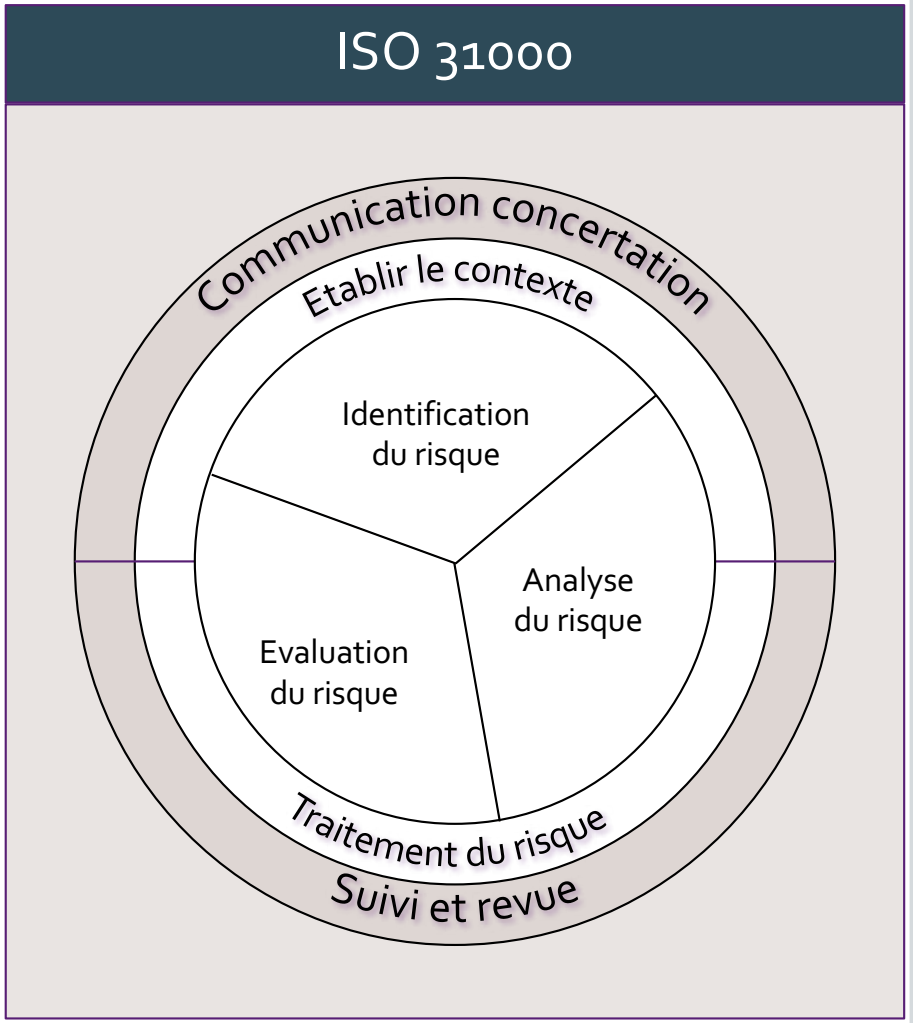
- La nouvelle définition met ainsi l'**accent sur les effets d'une connaissance incomplète** des événements ou des circonstances sur le processus de prise de décision.
- Elle fournie **une structure et des lignes directrices** sur les bonnes pratiques applicables à toutes les opérations concernées par le management du risque.
- L'objectif central de cette définition est de permettre à chaque organisation de **réaliser et de protéger la valeur de son travail**.
- Par son **caractère universel**, elle permet d'**améliorer la réalisation des objectifs** de tous projets ou entreprises.

SIGMA PARTNERS

LE DEVELOPPEMENT D'UN MANAGEMENT GLOBAL DES RISQUES (1/2)

L'ENTREPRISE RISK MANAGEMENT

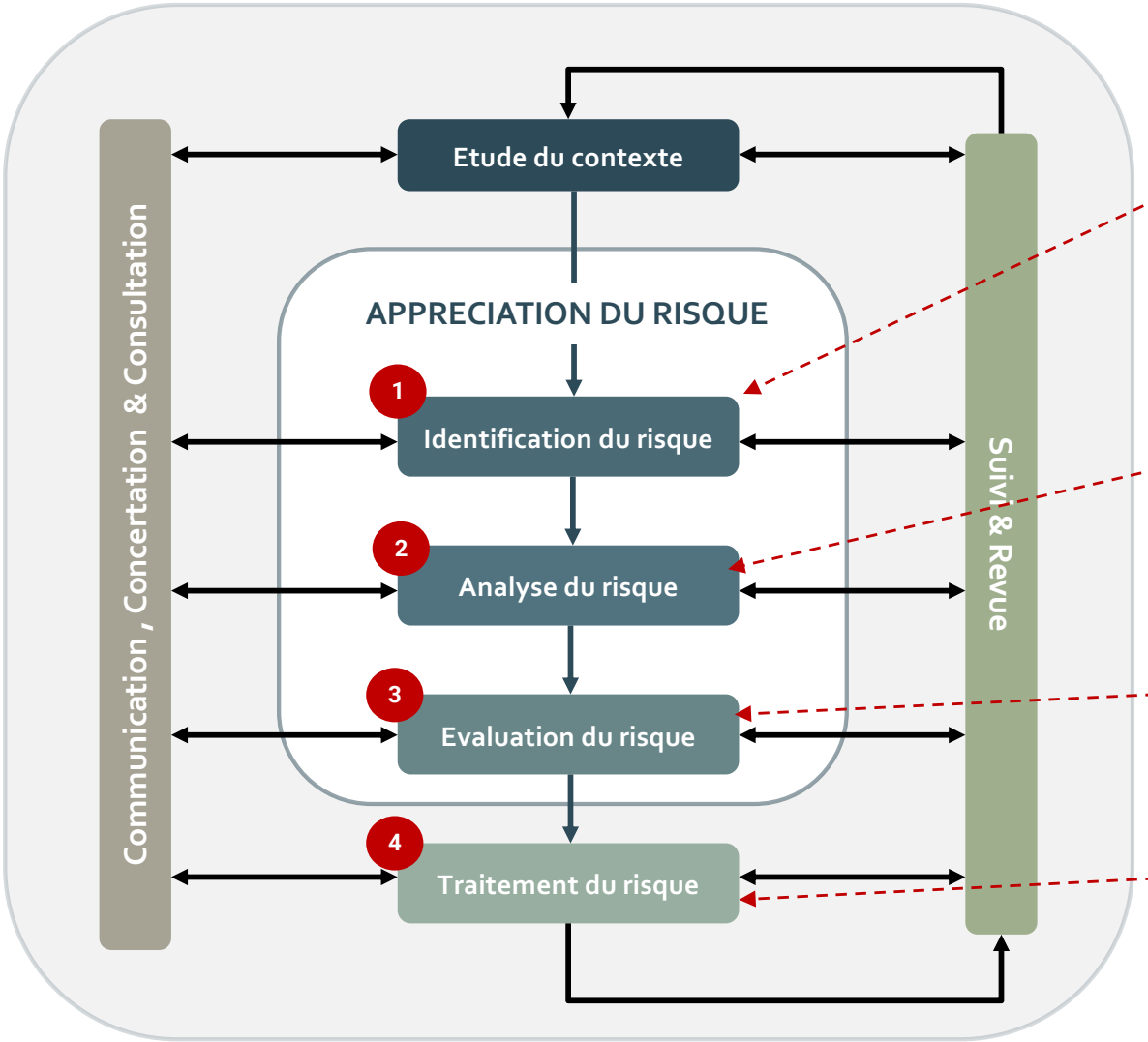
- Le Standard ISO 31000 propose une **approche pour développer un cadre** permettant aux entreprises d'**intégrer le management des risques**.
- Le point d'entrée est d'**aligner les objectifs de l'organisation, la politique de management des risques et les responsabilités** légales et contractuelles.
- Le **cadre** du management des risques doit être **intégré dans les processus de décisions et d'organisation** de toutes les activités de l'entreprise, en veillant aux contextes internes et externes, aux responsabilités de chacun et aux ressources disponibles aux niveaux stratégique et opérationnel.



SIGMA PARTNERS

LE DEVELOPPEMENT D'UN MANAGEMENT GLOBAL DES RISQUES (2/2)

LE DISPOSITIF DE MAITRISE DES RISQUES SELON LA NORME ISO 31000



Que pourrait-il arriver et pourquoi ?

Quelles en sont les conséquences ?

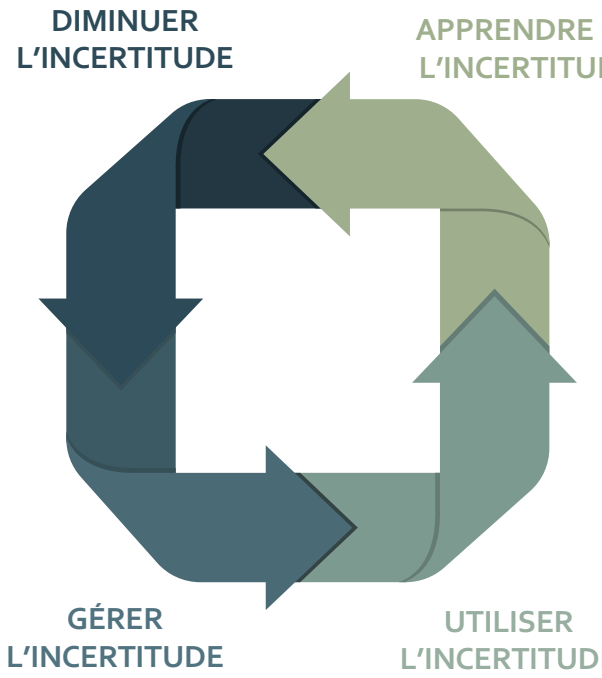
Quelle en est la probabilité de survenance ?

Comment transférer ou réduire la probabilité de ce risque ?

SIGMA PARTNERS

LE TRAITEMENT DE L'INCERTITUDE

TRAITER L'INCERTITUDE



DIMINUER L'INCERTITUDE

- En pratiquant la veille
- En utilisant des indicateurs et des tableaux de bord
- En faisant des diagnostics (FURSPE, PESTEL, SWOT…)

GÉRER L'INCERTITUDE

- En pilotant c'est-à-dire tenir un cap et pouvoir à tout moment réajuster les objectifs
- En favorisant la modularité, l'adaptabilité des organisations et l'autonomie du personnel
- En développant la polyvalence du personnel, le partage d'expertises et la formation

UTILISER L'INCERTITUDE

- En cherchant dans l'incertitude les opportunités de développer ce que vos compétiteurs ne voient pas
- En utilisant l'incertitude pour développer la résilience de votre organisation

APPRENDRE DE L'INCERTITUDE

- En faisant des retours d'expérience
- En analysant les incidents
- En pratiquant les groupes de résolutions de problèmes

SIGMA PARTNERS

UN OUTIL EFFICACE DE PARTAGE D'UNE CULTURE COMMUNE

UN PROCESSSUS ITERATIF

Le processus de management du risque est itératif , non seulement jusqu'à ce que le risque soit acceptable mais aussi pour, en permanence, identifier les nouveaux risques issus de l'évolution du contexte externe et interne de l'entreprise.

UNE DEMARCHE TRANSVERSALE

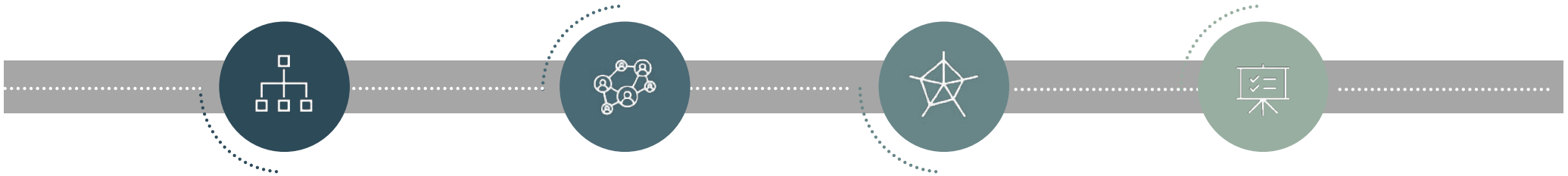
Le recours à des ateliers transversaux composés d'employés de l'entreprise de tous niveaux hiérarchiques permet d'améliorer la culture du risque des participants et offre des résultats plus fiables.

COMMUNICATION & CONSULTATION

Pour ISO 31000, si le processus de management des risques est important, il faut noter que le management des risques est avant tout une affaire de culture. La communication, la concertation et la consultation sont essentielles à chaque étape du processus.

SIGMA PARTNERS

IMPLÉMENTER LE MANAGEMENT DES RISQUES EN ENTREPRISE EN 4 ÉTAPES



Décomposer les objectifs

Pour démarrer la démarche de normalisation ISO 31000, il est primordial d'établir le contexte, c'est-à-dire définir les objectifs stratégiques de cette nouvelle orientation de management par le développement d'une analyse des processus de l'organisation.

Isoler les incertitudes

Chaque entité se caractérise par des hypothèses sources d'incertitudes qui génèrent des risques à analyser. L'ensemble des incertitudes devra ainsi être identifié et analysé afin de recenser l'ensemble des risques menaçant l'organisation.

Analyser les risques

Il s'agit de réaliser une cartographie des risques avec, par exemple, une matrice des risques bruts, une matrice de priorisation des risques et/ou un diagramme des causes et des conséquences, pour identifier les liens de cause à effets et souvent les corrélations entre les différentes hypothèses.

Traiter les risques

Vient ensuite l'objectif de diminution du risque de ne pas atteindre les objectifs de l'entreprise. Les choix de traitement du risque sont multiples – le refus du risque, la prise ou l'augmentation d'un risque afin de saisir une opportunité, l'élimination de la source de risque, le partage du risque, etc. – et sont propres à chaque risque identifié. Ces choix font l'objet d'une concertation interne pour une appropriation de tous.

SIGMA PARTNERS

CONCLUSION

- *Quelques points clés à retenir sur la norme ISO 31000*
- *Nous contacter*

SIGMA PARTNERS

QUELQUES POINTS CLÉS À RETENIR SUR L'ISO 31000

UN MANAGEMENT TRANSVERSAL ET INTÉGRÉ

- Au sens de l'ISO 31000 le management des risques est transversal et intégré. Le cloisonnement vertical du modèle organisationnel hiérarchique d'une entreprise peut être remplacé par un **modèle d'organisation horizontale par processus.**
- La norme ISO 31000 met en avant dans son cadre organisationnel l'**importance du leadership et de l'engagement de la direction générale** en donnant du sens et en reliant les objectifs de chaque processus à ceux de l'entreprise dans sa stratégie globale.

UNE PRIORISATION DES RISQUES

- C'est le symbole du passage d'un traitement technique du risque et de la recherche du risque zéro à une **gestion de portefeuille de risques**. Le gestionnaire du risque adopte alors un langage de management.
- Suivant leurs critères d'évaluation et suivant l'efficacité des moyens de mitigation mis en œuvre, il devient possible de **déterminer si le niveau de couverture du risque est acceptable**, et ceci **en fonction de l'appétence au risque** déterminée par la direction de l'entreprise sur la base de sa stratégie.

UN CENTRAGE SUR L'ATTEINTE DES OBJECTIFS

- L'objectif de l'ISO 31000 est d'aider l'entreprise à atteindre ses objectifs. Le décideur, quel que soit son niveau, doit avoir accès aux informations utiles et suffisantes pour **garantir l'atteinte des objectifs** et **identifier le cas échéant les opportunités** engendrées par certains scenarii de risques.
- Elle introduit en filigrane un concept absent jusqu'à présent du management des risques : le **risque à ne pas faire**. Il s'agit plus de dire comment atteindre un objectif en maîtrisant ses risques plutôt que de relever les obstacles que l'entreprise va rencontrer en tentant de réaliser ses objectifs.

LA STRATEGIE DE MITIGATION DES RISQUES

- La **stratégie de mitigation d'un risque sur un processus** donné de l'entreprise est alignée sur la stratégie globale de mitigation des risques de l'entreprise. C'est un point essentiel pour que le management des risques s'inscrive dans l'entreprise.
- De la même façon, il est essentiel que la stratégie globale de mitigation des risques soit **alignée avec la stratégie de l'entreprise**.
- L'entreprise peut alors piloter la gestion globale de ses risques en même temps qu'elle conduit ses différentes activités grâce à un dispositif de maitrise des risques embarqués dans les processus opérationnels.

SIGMA PARTNERS

NOUS CONTACTER

Sandrine STAUB
Executive Partner
s.staub@sigmap.fr

François FAURE
Directeur de mission
f.faure@sigmap.fr

Remy ZUCCHI
Consultant
r.zucchi@sigmap.fr