



COMMISSION ERM 360°

4 mai 2018





Ordre du jour

- Tour de table
- Questions et remarques sur réunion précédente et CR ?
- ISO 31000 (Françoise Gaucher)
- Points d'actualité
 - Avancement des GT
 - Autres sujets
 - Dates et sujets des réunions
- Annexe : Rappel de la feuille de route 2017 /2018
 - GT 1
 - GT 2
 - GT 3
 - GT 4 risques de l'entreprise étendue



ISO 31000

Françoise Gaucher



Gouvernance et gestion des risques des tiers

Objectif de l'échange d'aujourd'hui pour la commission :

- Comprendre les apports de l'évolution de la norme ISO 31000
- Échanger avec les acteurs impliqués dans le groupe de travail



Norme ISO 31000 - 2018

Management du risque – Lignes directrices
*Présentation de la norme actualisée version
2018*

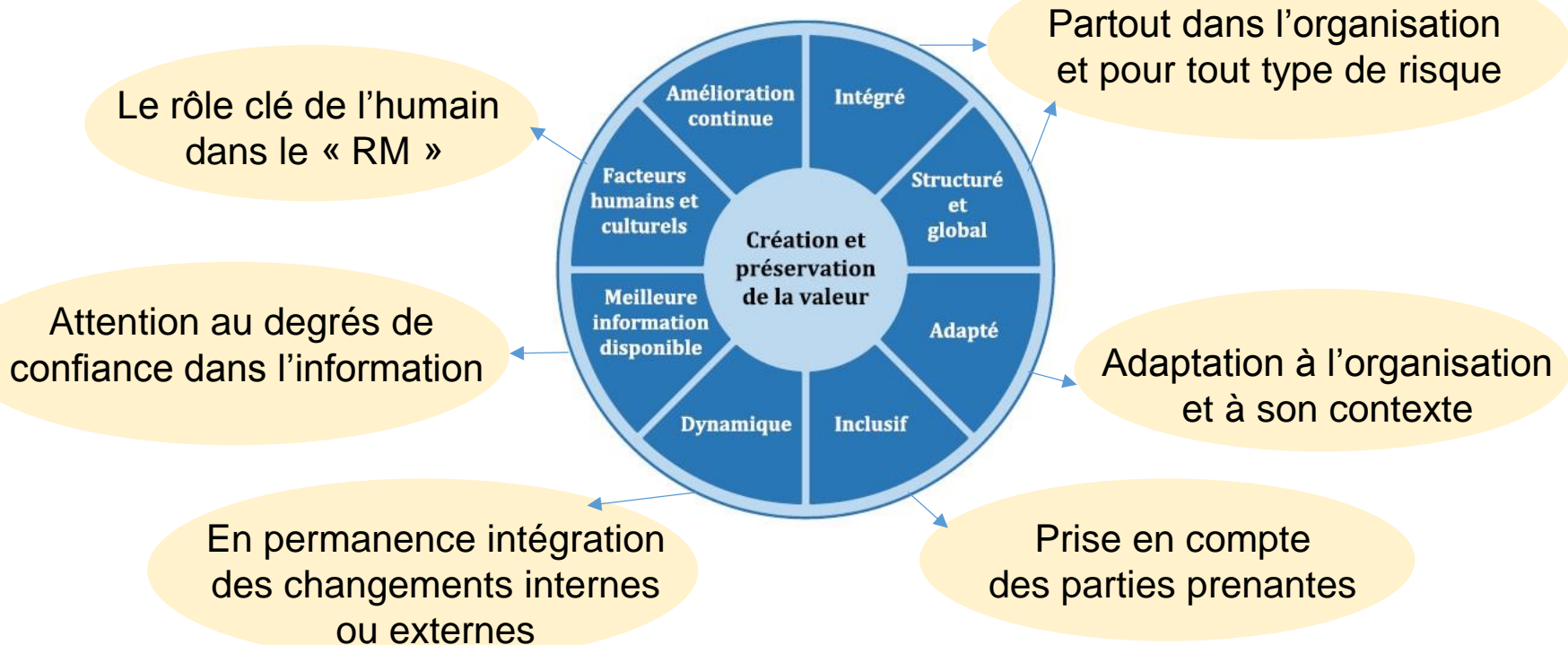
Mai 2018

Introduction

- Norme internationale portée en France par l'AFNOR
- S'adresse à tout type d'organisme
- Version 2018 : plus claire et mieux adaptée au contexte actuel (interne et externe)
- Norme présentant les lignes directrices du management du risque (tout type de risque)
- **S'adresse à toutes les personnes, dans l'entreprise, qui créent de la valeur et la préservent :**
 - La filière « risk mangement »
 - Les décideurs
 - Ceux qui définissent et proposent les objectifs
 - Ceux qui ont en charge l'atteinte des objectifs
 - Ceux qui contribuent à l'amélioration de la performance

Finalité et principes

- Finalité
 - *Création et préservation de la valeur*; le management du risque *améliore la performance, favorise l'innovation et contribue à l'atteinte des objectifs*
- Principes pour un management du risque efficace et efficient



Cadre organisationnel : généralités



- Pourquoi un cadre organisationnel ?
 - Aide l'organisme à intégrer le management du risque dans les activités et les fonctions significatives
 - Nécessite un soutien de la direction

Le cadre organisationnel
du management du risques



Cadre organisationnel : leadership et engagement

- Leadership et engagement de la direction :
 - Le management du risque est intégré dans toutes les activités de l'organisation
 - Le cadre organisationnel est adapté
 - Une déclaration générale (politique, plan ou ligne de conduite... pour le management du risque) est diffusée
 - Les délégations de responsabilité sont établies aux niveaux appropriés de l'organisme.



Cadre organisationnel : intégration dans l'organisme



- L'intégration du management du risque s'appuie sur la compréhension des structures et du contexte de l'organisme
- Schématiquement :
 - La gouvernance guide l'évolution de l'organisme
 - Les structures de management traduisent l'orientation de la gouvernance en **stratégie et objectifs pour atteindre les niveaux souhaités de performance durable et de viabilité à long terme**
- La détermination de la responsabilité du management du risque et des **rôles de suivi** au sein de l'organisme fait partie intégrante de la gouvernance de l'organisme.
- L'intégration du management du risque :
 - Un processus dynamique et itératif
 - Adapté aux besoins et à la culture de l'organisme

*Lien avec
le contrôle
interne, la
sécurité...*



Cadre organisationnel : conception



- La **conception** nécessite :
 - Compréhension de l'organisme et de son contexte
 - Contexte externe : facteurs sociaux et culturels; cadre politique, légal, réglementaire; parties prenantes externes; ...
 - Contexte interne : vision, missions, valeurs; gouvernance, organisation, responsabilités; ...
 - Définition claire de l'engagement en matière de management du risque :
 - But de l'organisme en matière de management du risque et les liens avec ses objectifs et ses autres politiques
 - **Pilotage de l'intégration du management du risque** dans les principales activités et **dans la prise de décision**
 - Pouvoirs et responsabilité
 - Ressources nécessaires au management du risque...
 - Des méthodes de communication et de consultation pour soutenir le cadre organisationnel du management des risques



Cadre organisationnel :

mise en œuvre, évaluation, amélioration

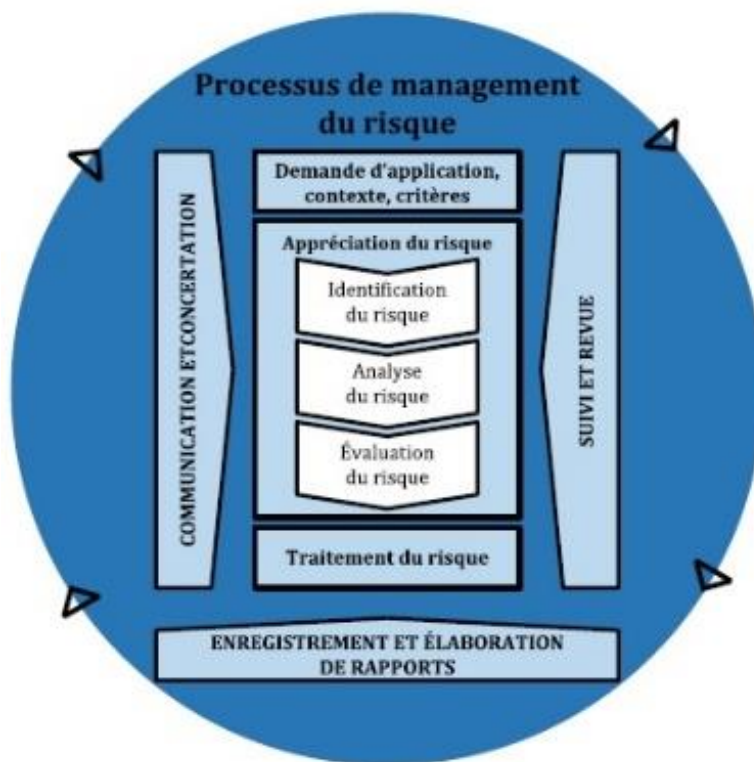


- Une mise en œuvre appropriée garantit :
 - Que le processus de management du risque fait partie intégrante de toutes les activités, à tous les niveaux, y compris la prise de décision.
 - Et que les changements de contexte interne et externe seront suivis
- L'évaluation et l'amélioration :
 - Vérification de la pertinence du cadre pour aider à atteindre les objectifs
 - Adaptation aux changements et amélioration continue



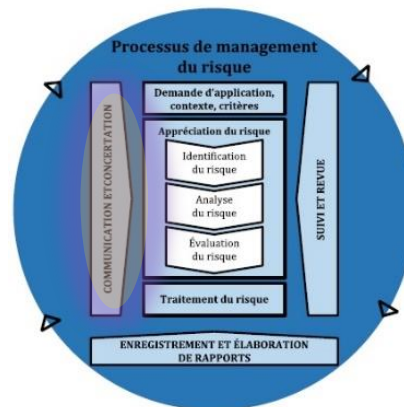
Le processus du management du risque

- Fait partie intégrante du management et de la prise de décision
- Peut être appliqué aux niveaux stratégique, opérationnel, programme ou projet



Le processus : communication et consultation

- But : aider les parties prenantes pertinentes à **comprendre les risques, les principes de prise de décision et les raisons pour lesquelles certaines actions sont nécessaires**
- Coordination entre communication et consultation :
 - Pour faciliter des échanges d'information factuels, opportuns, pertinents, précis et compréhensibles
 - Tout en prenant en compte **la confidentialité et l'intégrité des informations ainsi que le droit privé des personnes**

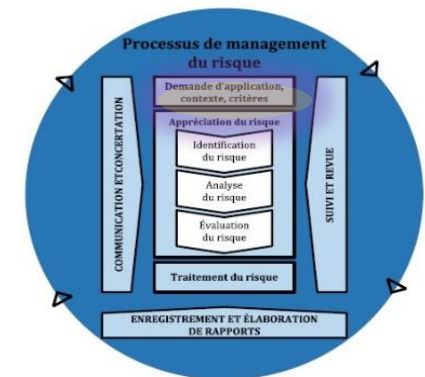


Le processus :

périmètre d'application, contexte et critères



- Périmètre et domaine d'application : exemple = niveau d'organisation ou programme ou processus...
- Contexte du management du risque : environnement spécifique de l'activité à laquelle le processus de management du risque doit être appliqué
- Critères de risque :
 - Niveaux et types de risques pouvant être pris ou non par l'entreprise en fonction des objectifs
 - Reflètent les valeurs, les objectifs et les ressources de l'organisme
 - Tiennent compte des obligations de l'organisme et de l'opinion des parties prenantes



Appréciation du risque



■ Processus global d'identification, d'analyse et d'évaluation

— Identification :

- Rechercher, reconnaître et décrire les risques
- *À ce stade, les risques sont des incertitudes pouvant aider ou empêcher un organisme d'atteindre ses objectifs*

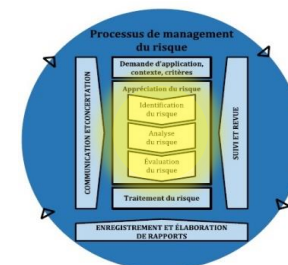
— Analyse :

- Comprendre la nature du risque et ses caractéristiques
- Prise en compte détaillée des incertitudes, des sources de risque, des conséquences...
et des **moyens de maîtrise et de leur efficacité**
- Analyse qualitative ou quantitative ou combinaison de techniques (pour scénarios complexes, risques systémiques, risques extrêmes...)

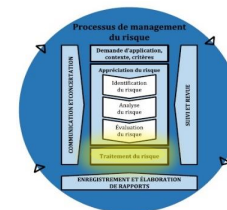
Lien avec le contrôle interne, la sécurité...

— Évaluation :

- À partir des données fournies par l'analyse
- But : permettre des décisions judicieuses par comparaison des résultats de l'analyse aux critères de risques
- Décisions possibles : ne rien faire de plus, examiner des options de traitement, maintenir les moyens de maîtrise existant...



Traitement du risque

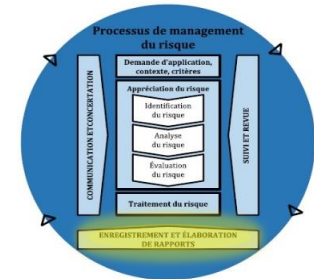


- But : choisir et mettre en œuvre des options pour aborder les risques
 - Sélection des options de traitement du risque :
 - Comparaison des avantages potentiels en termes d'atteinte des objectifs par rapport aux coûts, aux efforts et aux inconvénients de leur mise en œuvre
 - La **justification d'un traitement du risque dépasse le cadre des seules considérations économiques** => obligations de l'organismes, engagements, opinion des parties prenantes
 - Communication et consultation autour des options de traitement
 - Anticipation du suivi : résultats escomptés et conséquences inattendues
 - Risque résiduel
 - Élaboration et mise en œuvre des plans de traitement du risque :
 - Les plans de traitement : précisent la manière dont les options choisies seront mises en œuvre
 - Le plan de traitement doit prévoir l'ordre de mise en œuvre
 - Les **plans de traitement sont intégrés aux plans et aux processus de management de l'organisme** (en concertation avec les parties prenantes concernées)

Suivi et revue, enregistrement et élaboration de rapports



- Suivi et revue
 - S'assurer et améliorer la qualité et l'efficacité de la conception, de la mise en œuvre et des résultats du processus
- Enregistrements et rapports :
 - Un processus documenté
 - Des rapports élaborés selon des procédures appropriées
 - **Prise en compte du caractère sensible des informations et du contexte externe et interne pour la création, la consultation et le traitement des informations**
 - Des rapports pour :
 - Améliorer la qualité du dialogue avec les parties prenantes
 - **Aider la direction et les organes de surveillance à faire face à leurs responsabilités**





QUESTIONS/RÉPONSES



Points d'actualité

Avancement des GT
Autres sujets
Dates des réunions

GT1 : Gouvernance

- Participants : Pia Olders, Thierry Pertus et Valérie Bonnel
- Réunion le 11 janvier : préparation de l'atelier aux Rencontres de Marseille
 - ✓ Évolution de la réglementation et pratiques de place
 - ✓ Cohérence des chapitres risques et assurances du document de référence
 - ✓ Retour d'expérience sur le process d'élaboration du document de référence
- Travaux du GT à venir sur la culture du risque
 - ✓ Intervention en préparation dans la commission du 29/6
- Rappel : Réunion précédente du GT le 9/11 sur la communication sur les risques
 - ✓ Communication subie (répondre aux différentes attentes du législateur, spécificités de certains secteurs, sanctions)
 - ✓ Communication choisie (reporting intégré, communication incident cyber...)
 - ✓ Communication interne (articulation des fonctions, matérialité, cohérence d'ensemble)
 - ✓ Communication externe (comply or explain, parties prenantes)
 - ✓ Transformer la contrainte de la réglementation en opportunité de différenciation



GT 2 : Pratiques

Rappel des objectifs de production

Dans un contexte fortement impacté par les évolutions réglementaires, les entreprises doivent :

- se mettre rapidement en conformité,
- détecter les nouveaux risques
- s'assurer que les moyens de maîtrise mis en place sont efficaces.

Le Risk Manager doit quant à lui être suffisamment agile pour déceler rapidement les nouveaux besoins. Pour répondre à l'évolution du contexte, il peut dès lors adapter les outils et pratiques ou en créer de nouveaux, afin de mieux :

- anticiper
- évaluer les mesures à prendre,
- organiser et de suivre leur mise en œuvre,
- mettre sous surveillance le dispositif de maîtrise des activités.



Les pratiques et outils c'est quoi ...?

Quelques exemples :

- Description et optimisation du processus global de gestion des risques
 - Sources d'identification
 - Cartographie
 - Reporting
 - Etc.
- Recherche, étude et détermination de principes (charte, politique, procédures) et méthodes (guide méthodologique, modèles, etc.)
- Mise en place d'outils :
 - fichiers excel ou autres,
 - recours à des logiciels,
 - etc.



Comment s'organise t'on pour détecter de nouveaux besoins dans les pratiques de gestion des risques?

Nous devons identifier et recenser les nouveaux besoins dans les pratiques, auprès des deux autres groupes de travail permanents (Gouvernance et Évolutions), et des groupes de travail temporaires (ex : entreprise étendue).

Pour ainsi répondre au « comment ? », et avec « quelles pratiques ? ».

Ces nouveaux besoins pourront être hiérarchisés par priorité et travaillés en groupe ou sous-groupe de travail avec pour objectif la production d'un livrable.

Nous fixerons très prochainement quelques dates en fonctions du planning des autres groupes de travail.

Élaboration de la feuille de route 1/2

| Sujets | Problématique / enjeu | Livrables | Principaux intéressés |
|---|---|---|---|
| <u>Sujet(s) de conformité :</u> | | | |
| Compliance éthique anti-corruption/RSE (Sapin 2, Loi devoir de vigilance, ...) | Comment évaluer et piloter la conformité ? | Méthodologie d'évaluation | Winifrey Jonathan (Samuel) |
| Compliance éthique digitale (LIL / LRN / GDPR, e-Privacy, Privacy Shield, ...) | Comment évaluer et piloter la conformité ? | Méthodologie d'évaluation | (Thierry) |
| Compliance spécifiques (juste à mentionner ?) (LSF / SoX > Marchés financiers, BCBS > Etablissement bancaires, ORSA > Sociétés d'assurance/RE, SEVESO 3 / CLP / REACH > ICPE, LPM / NIS > OIV/OSE, HAS > ES, DUER > Risques professionnels...) | Comment évaluer et piloter la conformité ? | Méthodologie d'évaluation | (Thierry) |
| <u>Sujet(s) hors conformité :</u> | | | |
| Cartographie des risques | Comment réaliser une cartographie des risques et la restituer selon l'auditoire ? | Guide pratique sur les métriques, catégories de risques, modèles de présentation, etc. | Thierry Jonathan Ghislain Samuel |
| Pilotage des risques et reporting | Comment et avec quels outils le RM assure le pilotage des risques et la communication associées (interne/externe) ? | Outils de veille, de pilotage, Business Intelligence... Communication de type newsletter | (Thierry) Jonathan Ghislain Samuel |
| Identification des risques émergents | <u>Détection de nouveaux risques (risques émergents)</u> : | Outils de veille, d'analyse tendancielle interne (analytics) | (Thierry) |

Élaboration de la feuille de route 2/2

| Sujets | Problématique / enjeu | Livrables | Principaux intéressés |
|--|---|---|-----------------------|
| <u>Enjeu de performance / stratégie :</u> | | | |
| Autoévaluation : | Comment s'assurer de leur efficacité ? | Guide | Winifrey (Samuel) |
| Risk Appetite (GT3) | Comment déterminer et évaluer l'appétence au risque ? | <ul style="list-style-type: none"> - Questionnaire - Tableau de formalisation du Risk Appetite | Winifrey Ghislain |
| Capital et fonds propres | Comment le RM peut participer ou contribuer au pilotage du capital et à l'amélioration des fonds propres? | <ul style="list-style-type: none"> - Note méthodologique – Etude de cas | Winifrey Ghislain |
| Stress Test / Tests de résistance | Comment se préparer aux situations de crises grâce à des simulations à travers des scénarii de stress diverses (historiques, hypothétiques, concurrentiels, politiques, environnementaux, etc.), instantanés ou durables. | <ul style="list-style-type: none"> - Note méthodologique / guide pratique / cas d'étude (définition des scénarios, métriques, élaboration de plan d'actions) | Ghislain |

GT3 : Tendances et évolutions

Thème 2017 – Risques et stratégie

- Participants : Stéphanie, Winifrey, Thibault
- Rappel du sujet et avancement



Pourquoi cette évolution ?
Définition des risques
stratégiques vs risques
majeurs
Risques émergents
Risk appetite
Gouvernance associée
Rôle du RM



Participation à 2 échanges
dédiés au sujet :
-Cercle des risk managers
(Pwc)
-Club risk connect
(Deloitte)

-interview Directeur de la
stratégie/GDR
-exploitation du résultat du
baromètre du RM (avec
pwc)



Point de vigilance
Interaction IFA – attente du retour de
B.Bouquot

GT3 : Tendances et évolutions

Thème 2017 – Risques et stratégie

Outils



Objectifs initiaux

Recueil de bonnes pratiques
Tool kits : guide d'entretien, méthodologie de mise en application du risk appetite

Réalisation et actions à suivre

Finaliser la synthèse de nos travaux d'ici juin

Tool kits -> à passer en GT2?
KPI de suivi de la performance de l'ERM -> identifier au titre du GT2

GT3 : Tendances et évolutions

Thème 2017 – Risques et stratégie

Communication
et publication
des travaux



Objectifs initiaux

- Atelier Rencontres
- Publication dans Atout Risk (T1 2018)
- Communication newsletter
- Journée des commissions
- Réseaux sociaux

Réalisation et actions à suivre

- Atelier Rencontres
- Journée des commissions
- Publication dans Atout Risk (T3 2018)
- Communication newsletter ?
- Réseaux sociaux : sujet plus large que le GT / posture globale de l'association
- Intervention dans le cadre de l'AG du CCA

GT4 (provisoire) : Risques de l'entreprise étendue

Objectif : publication pour les rencontres 2019

8 réunions en juillet, septembre, octobre , novembre, janvier, février, avril

- Collecte des documents d'entrée
 - Liste des idées maitresses
 - 1^{er} macro structure d'argumentation
 - Répartition des travaux
 - Mise en place du plan
 - Prise en compte des documents ateliers rencontres AMRAE 2016 et 2018
 - Début de rédaction : introduction et développements
 - Collecte de cas publics pour illustrer le propos
-
- Partenariat avec Deloitte pour coordination de la rédaction (à finaliser)
 - Membres du GT 4 : Fanny Dreyfous-Ducas / Isabelle Henocq / Pia Olders / Patrick Lheureux / Denis Zandvliet / Philippe Noirot
 - Léopold Larios apportera son expertise pour la partie sous-traitance IT
 - Le sujet a fait l'objet d'un atelier aux Rencontres de Marseille

Risques et opportunités 2030

Partenariat de l'AMRAE avec ARENGI ET TILT sur cette démarche

- Juin 2017 : présentation de l'étude en journée des commissions
- Q4 2017 : Extension à une plus large communauté de répondants
- 15/12/17 : échange commission ERM avec Arengi
- Q1 2018 : Communication des résultats aux rencontres AMRAE Marseille

En attente publication des résultats par Arengi

À décider : 2^{nde} session de travail en commission. Juin ? Septembre ?



Risk appetite : point d'avancement

- Suite au document IFA, des restitutions de départ lors de la réunion de la commission de juin 2016 ont conduit à une synthèse par un groupe de travail de la commission
- Échange Brigitte Bouquot / Agnès Touraine planifié le 30 mai 2018.
- Une réunion AMRAE (B Bouquot / S.Mallet / Ph Noirot) avec l'IFA sera organisée
- PwC a identifié un contact membre de l'IFA, et accompagnera cette démarche
- Une restitution plus complète prévue en commission après la réunion IFA
- Coordination avec le GT risques et stratégie à prévoir
- Réflexion collective
 - situer le niveau hiérarchique, la ligne de reporting, etc.
 - à quelle référence formalisant la stratégie, les risques majeurs sont-ils à mettre au regard ? (ex : plan d'affaire)



Points divers

- **Groupe de Travail Compliance**
 - Axé principalement sur Sapin 2 et Devoir de Vigilance
 - Plusieurs membres de la commission ERM 360 y participent
 - Synthèse en commission ERM prévue en octobre

- **FERMA séminaire des risk managers**
 - Anvers les 8/9 octobre 2018
 - Préparation d'un atelier sur la loi sur le devoir de vigilance
 - Volontaires ?

- **Enquête mondiale 2018 Deloitte Extended Enterprise**
<https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/risk/deloitte-uk-third-party-gov-risk-management-2018-interactive.pdf>

- **Groupe de Travail Risques et Projets AMRAE**
 - Piloté par Loic Roussin
 - Finalisation en cours avec Deloitte
 - Rapprochement avec commission ERM ?



Points divers

- Invitation transmise à l'AIRMIC pour la JDC
 - Pas de membre francophone disponible
- Moyens de réunion « visio » pour associer les membres non parisiens aux réunions : décision prise par le C.Adm, en cours...
- APREF association des professionnels de la réassurance en France : cartographie des risques et de leur coût pour la collectivité
<https://www.apref.org/fr/cartographie-risques-risk-management-france>
- Rendez-vous du club adhérent Afnor 2018 du 25 mai « Manager les risques avec la nouvelle norme ISO 31000 » avec Mylène et Thierry

Développer la culture du management du risque avec la norme ISO 31000:2018

Vendredi 25 mai 2018 9h30 – 13h00
AFNOR – La Plaine Saint Denis

Non, cela n'arrive pas qu'aux autres !

Suspension de permis de conduire de votre meilleur commercial.
Inondation. Absence prolongée d'une personne clé dans votre PME...

L'identification et l'atténuation des risques constituent un véritable défi pour chaque entreprise, chaque organisation, quelle qu'en soit sa taille, son activité, son emplacement.

Le risque est toujours une préoccupation du dirigeant.

La norme ISO 31000 « Management du risque » guide les entreprises sur la manière d'intégrer la prise de décision fondée sur le risque aux processus de gouvernance, de planification, de management en décrivant les principes, les ressources dédiées et le processus dans une logique de management global, Vous souhaitez instiller une culture du management du risque en restaurant notamment une prise de conscience de vos salariés et vos de vos parties prenantes de l'importance du suivi et de la maîtrise des risques ; saisir les opportunités positives et éviter les conséquences négatives associées au risque ; prendre des décisions plus éclairées donc plus efficaces notamment en matière d'affectation des ressources.

La nouvelle version de la norme volontaire ISO 31000 sert ces intérêts donc la performance des organisations.

Les experts qui ont travaillé à la révision de la version de 2009 viennent vous présenter cette nouvelle version, plus stratégique, au contenu rationalisé, à la portée visant toutes les strates de l'organisation.

Structurante, donc et tellement utile...

Les acteurs concernés :

- directeurs généraux,
- responsables risques,
- responsables qualité,
- responsables contrôle interne,
- responsables QSE,
- responsables sécurité,
- responsables développement durable,
- responsables prévention,
- coordinateurs/coordonnateurs normalisation,
- gérants

Développer la culture du management du risque avec la norme ISO 31000:2018

Vendredi 25 mai 2018 9h30 – 13h – AFNOR – La Plaine Saint Denis

PROGRAMME

| | |
|-------|--|
| 9h00 | Accueil |
| 9h30 | Le contexte du management des risques des organisations <ul style="list-style-type: none"> - contexte actuel des incertitudes multiples - définition du management des risques pour une organisation, - la norme ISO 31000 en quelques mots ... Françoise Gaucher, Présidente de la commission de normalisation AFNOR « Management des risques » |
| 9h45 | La nouvelle ISO 31000 dans ses grands principes Steve O'BRIEN, Chef de la délégation AFNOR au comité technique international ISO sur le management du risque et enseignant chercheur - ESAIP |
| 10h00 | Table Ronde animée par Françoise Gaucher, Présidente de la commission de normalisation AFNOR « Management des risques » et Risk Manager expert Groupe La Poste <ul style="list-style-type: none"> - Exemple de déploiement dans le secteur public et d'intégration dans d'autres systèmes de management : Sylvie LOISEL, Responsable qualité et développement durable - ANSES - Liens avec le contrôle interne : Jean-François CHARBONNIER, Secrétaire Général pour l'Administration – Ministère des Armées - Le management des risques au regard d'autres approches -sécurité, continuité d'activité... : Yves MÉRAN - IMaR |
| 10h45 | Pause |
| 11h00 | Témoignages <ul style="list-style-type: none"> - Témoignage sur l'intérêt et les apports d'une participation à la normalisation sur le management des risques Myliène Zerbib, Direction des Systèmes d'Information - Pôle Emploi - Témoignage sur la déclinaison opérationnelle de la norme ISO 31000 : retour d'expérience sur le management du risque cyber appliqué au secteur du transport ferroviaire et transport public urbain Thierry PERTUS, Risk Management & Cyber Security – CONIX - Témoignage de l'approche globale de l'ISO 31000 lors d'un projet majeur Damien BARRE, Ingénieur HSE, Coordinateur pipeline des dépôts pétroliers de distribution et Jean-Yves BICHEMIN, Responsable HSE des dépôts pétroliers – CIM - CCMP |
| 11h45 | Les travaux proposés Rodolphe CIVET, Responsable du pôle normalisation - AFNOR |
| 12h15 | Echanges avec la salle |
| 12h30 | Clôture |

Contact : Laëtitia CRONIER – adherent@afnor.org – 01 41 62 85 00



Calendrier

- **prochaines commissions ERM 360**
 - 29/06/2018 : Culture du risque (Sabine Drujon)
 - 21/09/2018 : réunion de rentrée feuille de route (+éventuellement rencontre IFA)
 - 26/10/2018 : synthèse travaux du GT compliance (Anne France Arnoux Sagnac)
 - 14/12/2018 : travaux de la commission SI y compris GDPR (François Beaume)

- **Autres dates AMRAE**
 - Assemblée générale 17 mai 2018
 - Journée des commissions 14 juin 2018



Annexe :

**Organisation de la commission ERM 360
Feuilles de route 2017 / 2018 des GT**

Cohérence avec les axes prioritaires du Comité Scientifique Permanent

- la Commission abordera directement les sujets suivants :
 - Gouvernance des risques
 - Fonction risk manager ERM
 - Communication des risques
 - Gestion des risques dans les grands projets
 - Nouveaux risques, nouveaux business models
- En fonction des besoins, d'autres thématiques pourront être abordées indirectement :
 - supply-chain,
 - PCA et gestion de crise,
 - cyber risques,
 - transition énergétique,
 - éthique et responsabilités,...

Objectifs de la commission

- Contribuer à la professionnalisation du Risk Manager,
- Accompagner l'évolution de la fonction ERM face aux changements environnementaux (nouveaux business model, digitalisation, big data,...).
- Faire **le lien avec la thématique GRC** (Gouvernance, Risques et Compliance) : **périmètre d'action du Risk Manager , valeur ajoutée et place de l' ERM dans et pour l'entreprise**, évolutions structurantes à suivre : rapprochement avec la **fonction stratégie**, évolutions des **référentiels (ISO31000, ISO9001, COSO ERM, etc.)**, **approches intégrées audit, contrôle et risque**, ou encore arrivée **du reporting intégré**.
- L'animation de sessions **d'échanges entre les adhérents** complétées par des interventions d'experts lorsque cela est nécessaire et possible, contribueront à l'atteinte des objectifs fixés et au succès de la commission.
- Par ailleurs, la commission souhaite développer le partage de ces travaux et réflexions avec l'ensemble des adhérents, au travers de **publications, ou de prises de positions, ou de contenus scientifiques** lors des séminaires. À titre d'exemple, l'ouvrage sur la communication des risques publié en 2017, inclut des travaux de la commission en particulier sur le top 10 des documents utiles aux organisations.

Organisation de la commission

- La commission ERM 360 est structurée en 3 groupes de travail permanents pour structurer (quoi ?) , mettre en œuvre (comment ?) et explorer (vers où ?).

1. **Gouvernance** : référentiels, culture et communication

Sous le pilotage de Valérie Bonnel

1. **Pratiques** : processus, méthodes, outils

Sous le pilotage de Winifrey Caudron

1. **Évolutions** : risque et stratégie, risk appetite, approches intégrées

Sous le pilotage de Sylvie Mallet

- Des groupes de travail ponctuels peuvent s'y ajouter. Ainsi en ce moment:

1. **Risques de l'entreprise étendue** (y compris les effets des lois Sapin II, devoir de vigilance, GDPR)

Sous le pilotage de Philippe Noirot

Feuille de route détaillée des Groupes de Travail

- Focus du GT1 :
 - nouveau COSO ERM,
 - update ISO31000,
 - culture du risque
- Focus du GT2 : pratiques exemplaires du métier de l'ERM
- Focus du GT3 : échanges avec l'IFA sur la notion de risk appetite
- Focus du GT4 : structuration d'une publication sur les risques de l'entreprise étendue

[Se rendre sur la page de la commission ERM 360 du site AMRAE](#)



Groupe de travail 1 :

Gouvernance

(référentiels, culture et communication)





Objectifs du groupe de travail Gouvernance

Partager sur :

- **Gouvernance des risques** : acteurs, comitologie, règles, bonnes pratiques
- **Référentiels** : évolution ISO 31000, COSO ERM,...
- **Culture** : culture du risque et culture d'entreprise
- **Communication** : reporting intégré, document de référence, attentes du législateur, communication subie et communication choisie



Groupe de travail Gouvernance : référentiels, Culture et Communication

- Inviter un membre du chantier sur l'évolution de l'ISO 31000
- Inviter un associé de PwC pour le COSO ERM
- Atelier des Rencontres « La communication sur les risques : reporting intégré, évolution de la communication et attentes du législateur »
- Intervention sur la culture du risque



Organisation du Groupe de Travail

Qui ?

Pia Olders, Thierry Pertus et Valérie Bonnel

Quand ?

Avant les réunions de la commission, avant le 15/12 sur la communication (reporting intégré, document de référence)

Comment ?

Réunion à l'AMRAE, conf call, mail



Groupe de travail 2 :

Pratiques du métier ERM

(processus, méthodes et outils)





Pratiques ERM : Objectifs du groupe de travail

Dans un contexte fortement impacté par les évolutions réglementaires, les entreprises doivent :

- se mettre rapidement en conformité,
- détecter les nouveaux risques
- s'assurer que les moyens de maîtrise mis en place sont efficaces.

Le Risk Manager doit quant à lui être suffisamment agile pour déceler rapidement les nouveaux besoins. Pour répondre à l'évolution du contexte, il peut dès lors adapter les outils et pratiques ou en créer de nouveaux, afin de mieux :

- anticiper
- évaluer les mesures à prendre,
- organiser et de suivre leur mise en œuvre,
- mettre sous surveillance le dispositif de maîtrise des activités.



Les pratiques et outils c'est quoi ...?

Quelques exemples :

- Description et optimisation du processus global de gestion des risques
 - Sources d'identification
 - Cartographie
 - Reporting
 - Etc.
- Recherche, étude et détermination de principes (charte, politique, procédures) et méthodes (guide méthodologique, modèles, etc.)
- Mise en place d'outils :
 - fichiers excel ou autres,
 - recours à des logiciels,
 - etc.



Comment s'organise t'on pour détecter de nouveaux besoins dans les pratiques de gestion des risques ?

Nous devons identifier et recenser les nouveaux besoins dans les pratiques, auprès des deux autres groupes de travail permanents (Gouvernance et Évolutions), et des groupes de travail temporaires (ex : entreprise étendue).

Pour ainsi répondre au « comment ? », et avec « quelles pratiques ? ».

Ces nouveaux besoins pourront être hiérarchisés par priorité et travaillés en groupe ou sous-groupe de travail avec pour objectif la production d'un livrable.

Nous fixerons très prochainement quelques dates en fonctions du planning des autres groupes de travail.



Organisation du Groupe de Travail?

Quand ?

Dates à déterminer. Probablement une première date au Q4 avec l'input des autres GT ?

Où ? À l'AMRAE si on décide de réunions physiques

Sinon par téléconférence ? Avantages : pouvoir impliquer des non parisiens, et possibilité de réunions plus fréquentes et plus courtes

À discuter avec les membres intéressés !!!!



Groupe de travail 3 : Évolutions et nouvelles tendances

**(risques et stratégie, risk appetite, approches
intégrées)**



Objectifs du groupe de travail

- Partager sur les évolutions / tendances d'aujourd'hui et de demain de notre activité et sur le rôle du RM
 - Capitaliser sur nos différentes expériences et identifier des bonnes pratiques
 - Alimenter les 2 précédents groupes de travail

 - Communications envisagées :
 - article dans Atout Risk, échéance fin d'année ou T1 2018,
 - représentation aux ateliers des Rencontres
- « RM : du chef d' orchestre au business partner »
- Autres ateliers?



Risques et stratégie

Synthèse de la réunion du 21 juillet

Pourquoi cette évolution, ce rapprochement entre risques/stratégie ?

Qu'entend-on par stratégie ?

Quand parle-t-on risques et stratégie ? Quels interlocuteurs ?

Gouvernance

Stratégie de pilotage des risques

Rôle du RM dans cette évolution

Bonnes pratiques à mettre en œuvre

Thématiques 2017 / 2018



A word cloud of various themes arranged in a roughly circular shape. The words are in different colors and sizes, indicating their relative frequency or importance. The themes include:

- Enjeux
- Expertise
- Synergie
- IA
- Valeur
- Sponsor
- Ethique
- Digitalisation
- GDPR
- Risk Appetite
- Business Partner
- Devoir De Vigilance
- Entreprise Etendue
- Audit
- Univers Des Risques
- Stratégie
- Responsabilités
- Agilité
- Priorités
- Transformation
- IFA
- Communication
- Big Data
- Pragmatisme
- Sapin 2
- Innovation
- Cyber Risk

D'autres idées ?



Organisation et prochains rdv

- Participants :
T.Bulabois, W.Caudron, G.Sutra, S.Canino, C. Cantournet
- Agenda
dates à caler d'ici fin décembre
- Les travaux du groupe de travail précédent Risques et stratégie sont intégrés dans le GT3



Groupe de travail 4 : Risques de l'entreprise étendue

(production d'un ouvrage)

Objectif et feuille de route

Groupe de travail :

- Isabelle Hénocq
 - Patick Lheureux
 - Philippe Noirod (pilote)
 - Géraldine Sutra
 - Denis Zandvliet
-
- Objectif : publication en 2018 d'un ouvrage AMRAE sur les risques de l'entreprise étendue
 - Périmètre tous les risques de l'entreprise étendue, y compris les effets des lois récentes Sapin II, devoir de vigilance, GDPR
 - Travaux sources : atelier des rencontres 2016, atelier à venir des rencontres 2018, étude Deloitte en cours