Atelier A6

Evolution des référentiels métiers et impacts pratiques sur le Risk Management

26èmes Rencontres du Risk Management | AMRAE 2018

Atelier A6

Intervenants

Françoise BERGÉ	**Associée**
Françoise GAUCHER	**Risk Manager expert Groupe La Poste** **Présidente CN Risques AFNOR**
Marie-Laure VACHEROT	**Directrice Audit Interne**

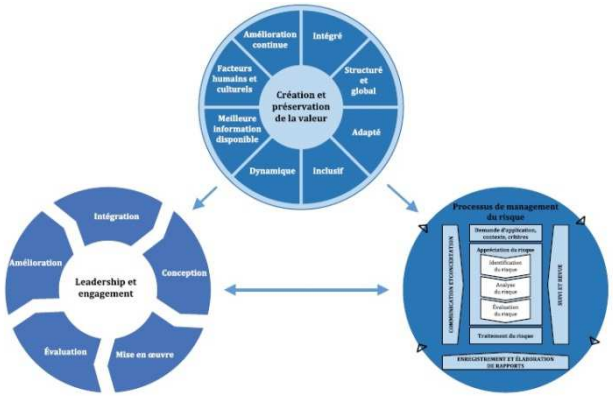
Modérateur

Mylène ZERBIB	**Risk Manager DSI Pôle emploi**

INTRODUCTION

Les référentiels ISO 31000, COSO ERM et AMF

ISO 31000 - Management du risque



⇨Norme qui fournit des principes, un cadre et des lignes directrices pour gérer toute forme de risque. Cette norme peut être utilisée par tout type d'organisme sans distinction de taille, d'activité ou de secteur. Elle n'a pas vocation à être certifiante.

COSO ERM

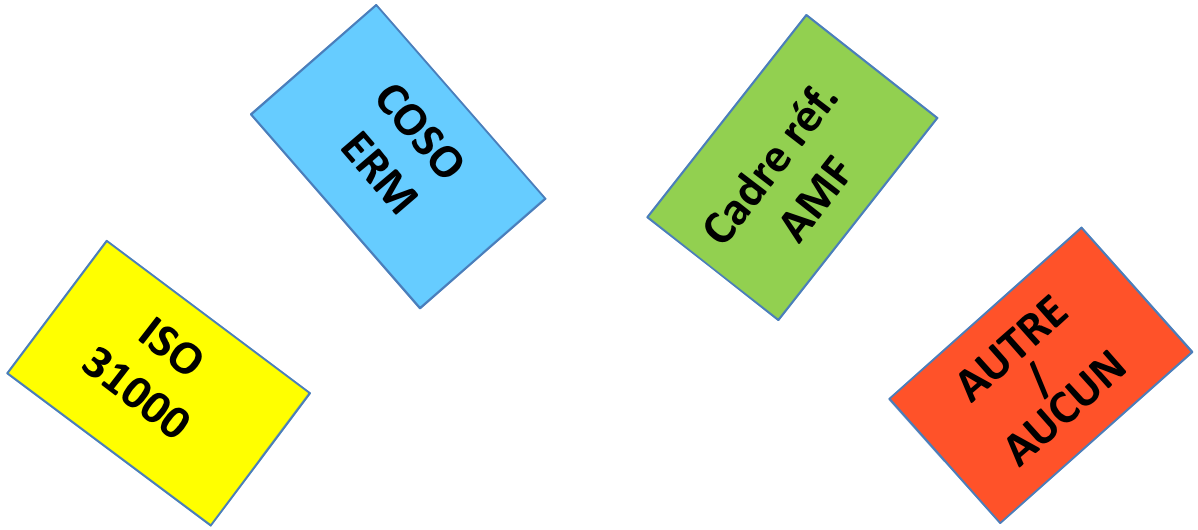
⇨ Référentiel qui permet aux entreprises de mieux comprendre l'impact concret de la culture sur la gouvernance des risques et l'appréciation des risques dans la sélection et l'exécution de la stratégie.

Cadre de référence AMF

AUTORITÉ DES MARCHÉS FINANCIERS

⇨Référentiel de contrôle interne et de gestion des risques visant à améliorer le pilotage des activités des entreprises et sécuriser l'atteinte de leurs objectifs.
Ce cadre a vocation à être adapté aux entreprises selon leurs spécificités de secteur, d'organisation et de taille.

Les référentiels ISO 31000, COSO ERM et AMF



Quel(s) référentiel(s) utilisez-vous?

Les référentiels de Gestion des risques

Extrait du baromètre du Risk Manager 2017

Référentiels de gestion des risques

Note : Les profils AP ne sont pas pris en compte dans la présente analyse. Il s'agit d'une question à choix multiple cette année.

81% des répondants utilisent un référentiel pour leur démarche, ce qui est en légère augmentation par rapport à 2015 où ils étaient 79% à faire usage d'un référentiel.

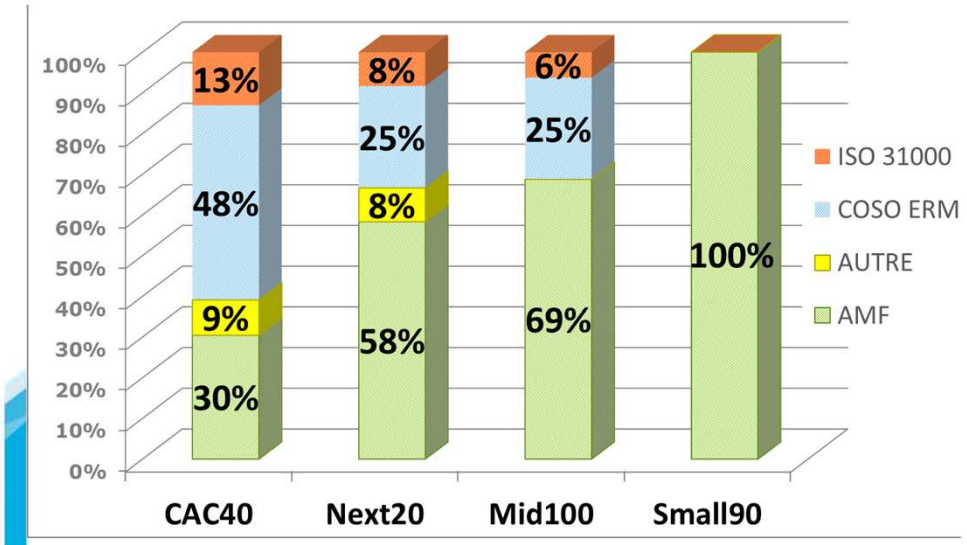
Pour 88% d'entre eux, les référentiels de gestion des risques sont utiles à leur fonction.

Près de la moitié des Risk managers (48%) déclare utiliser un référentiel interne de gestion des risques, ce qui est en forte augmentation par rapport à 2015 où seulement 28% des Risk managers déclaraient avoir un référentiel interne. Ils sont 32% à déclarer utiliser le COSO ERM (contre 25% en 2015).

Les référentiels de Gestion des risques

Source : Deloitte Décembre 2017

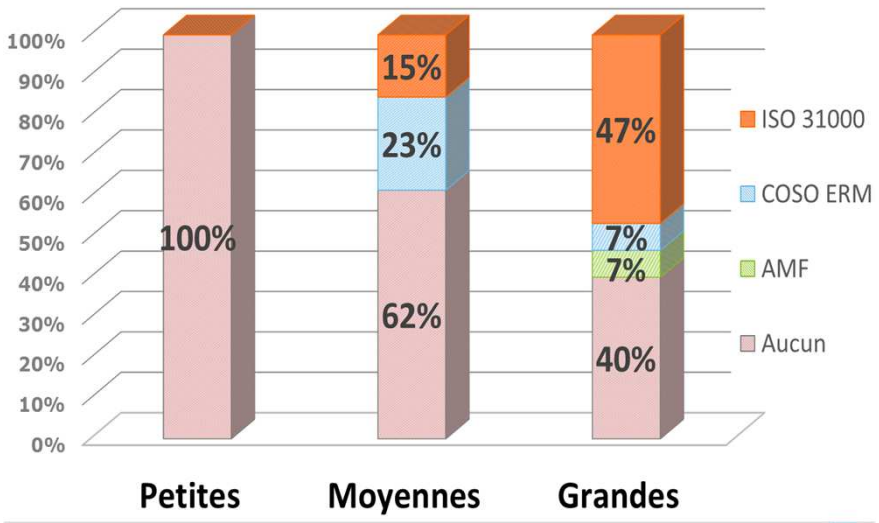
- **Comparaison des référentiels utilisés par les sociétés <u>cotées</u>***
  - Analyse par indice boursier**



**Résultats sur la base d'un échantillon représentatif de 43 entreprises du « CAC All Tradable » - Indice boursier regroupant 250 valeurs d'entreprises cotées en bourse à Paris – (23 entreprises du CAC 40, 12 entreprises du Next20, 16 entreprises du Mid100, 3 entreprises du Small90*

***CAC 40 : 40 premières capitalisations à la Bourse de Paris; Next 20 : 20 capitalisations suivant le CAC 40; Mid 100: 100 capitalisations suivant le Next 20 ; Small 90 : 90 capitalisations suivant le Mid 100*

- **Comparaison des référentiels utilisés par les sociétés <u>non cotées</u>***
  - Analyse par taille**



** Résultats sur la base de 20 organisations françaises non cotées en bourse : 2 Petites, 13 Moyennes et 5 Grandes.*

*** Les « Petites organisations » ont un effectif inférieur à 250 personnes. Les organisations de taille « Moyenne » ont un effectif inférieur à 5000 personnes. Les « Grandes organisations » ont un effectif supérieur à 5001 personnes.*

Norme ISO 31000 - 2018

La norme ISO 31000

- Présentation et objectifs
  - Norme internationale de référence pour l'approche risque
    - 1ère version parue en 2009
    - France représentée à l'ISO par afnor NORMALISATION (aujourd'hui 54 pays membres du comité technique ISO 31000)
  - Une norme qui propose
    - Des principes, un cadre et des lignes directrices pour gérer toute forme de risques…
    - … à destination de tout type d'entreprise ou d'organisation
    - Une définition du risque : effet de l'incertitude sur les objectifs

ISO 31000 – 2018
Les principaux changements

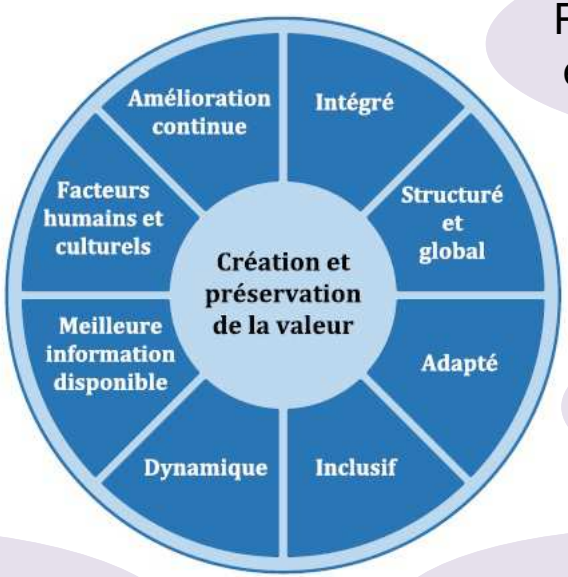
- Des principes révisés (clés du succès du risk management)
- Une réaffirmation du leadership de la Direction et une intégration du management des risques dans le pilotage en commençant par la gouvernance
- Une mise en exergue du caractère itératif du processus nécessaire du fait de nouvelles expériences, connaissances, analyses
- Une simplification et le maintien d'un système ouvert adaptable à tous les besoins ou les contextes

ISO 31000 – 2018
Les apports de la révision

- Des principes pour agir et s'améliorer

Le rôle clé de l'humain dans le RM

Partout dans l'organisation et pour tout type de risque



Attention au degré de confiance dans l'information

Adaptation à l'organisation et à son contexte

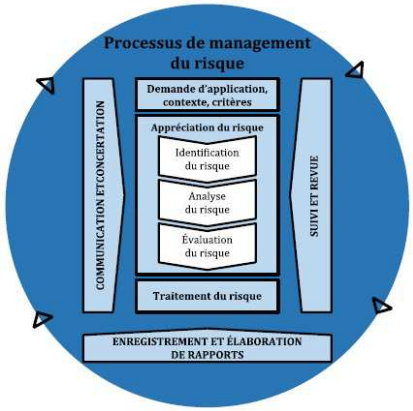
En permanence intégration des changements internes ou externes

Prise en compte des parties prenantes

ISO 31000 – 2018
Les apports de la révision

- Le cadre

- Le processus



Des engagements forts :

- *Alignement sur la stratégie, les objectifs et la culture de l'organisation*
- *Une politique de RM*
- *Des obligations et des engagements volontaires…*

Plus ouvert, plus dynamique :

- *Importance de la communication et de la consultation des parties prenantes*
- *Des critères de risques à faire évoluer si nécessaire*
- *Des analyses de risques intégrant le rythme des changements, les niveaux de sensibilité…*

ISO 31000 – 2018
Valeur ajoutée

Un standard souple et reconnu

- Norme « chapeau »
  - Compatible avec d'autres normes ISO (9001 qualité – 26000 RSE…)
  - Compatible avec les cadres réglementaires Banque ou Assurances
- Norme de plus en plus utilisée dans le monde
  - Amérique Latine, Chine…

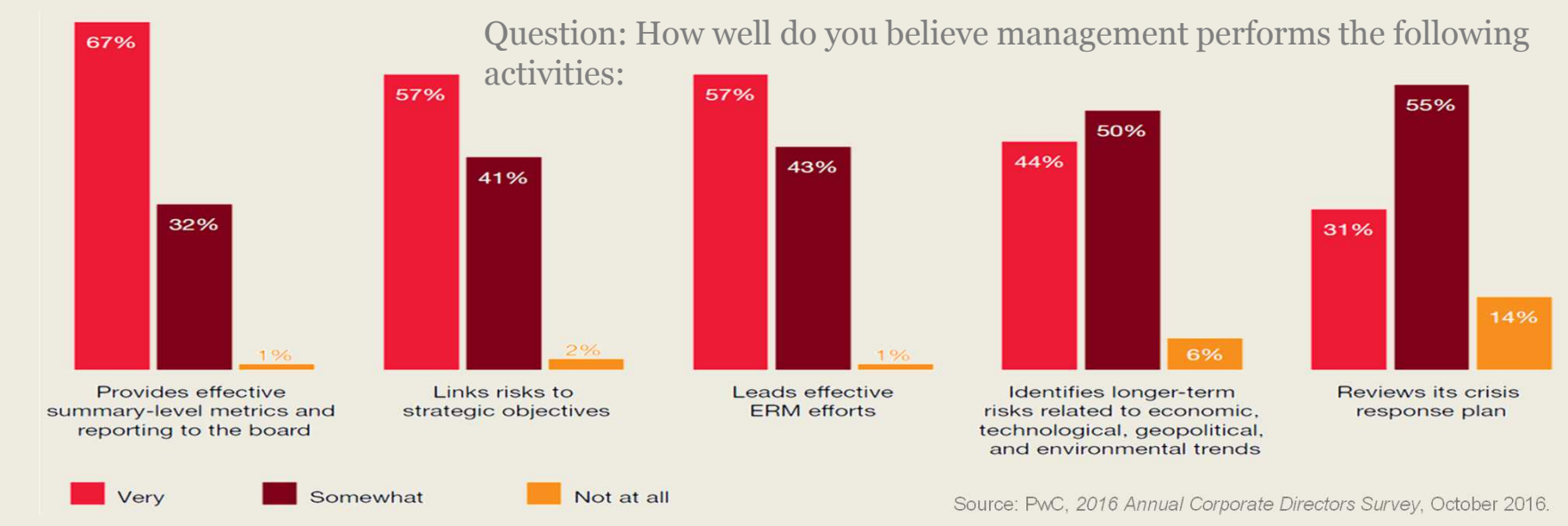
Un guide pratique

- Suivre la norme, c'est
  - Adopter des principes,
  - Suivre les indications pour mettre en place un dispositif intégré dans le fonctionnement de l'organisation
  - Dérouler le processus itératif proposé
- Et cela permet
  - Un management des risques lisible et efficace

COSO ERM

Pourquoi une nouvelle édition ?

- Les pratiques de l'ERM ont beaucoup évolué depuis 20 ans
- Les conseils d'administration attendent plus de valeur ajoutée des approches ERM
- Les entreprises se transforment par la technologie
- Les menaces évoluent



Le référentiel COSO ERM 2017

Une nouvelle représentation graphique qui souligne que la maîtrise des risques est un cycle intégré au cycle de management et de pilotage de l'organisation.

Définition
La culture, les capacités et les pratiques, liées à la définition et l'exécution de la stratégie, sur lesquelles une organisation s'appuie pour gérer ses risques dans l'objectif de créer et de préserver la valeur.

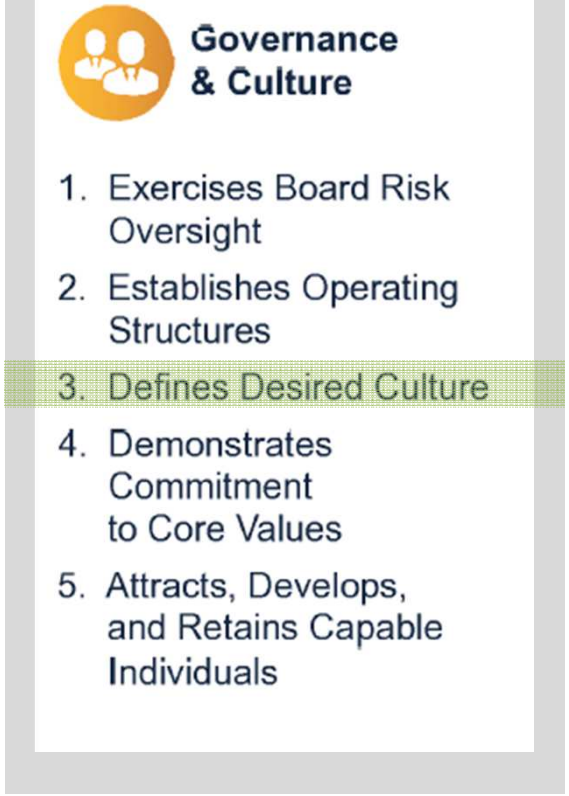
5
Composants alignés sur le cycle de vie de l'entreprise

20
Principes qui décrivent le référentiel ERM

Les principaux apports

- **Une nouvelle structure renforçant l'alignement du management des risques avec le cycle de vie de l'entreprise**
- **Un point de vue sur la prise en compte du rôle de la culture dans la gestion des risques**
- **Un focus sur l'intégration du management des risques dans la définition de la stratégie**
- **Une discussion sur les bénéfices de la mise en place d'une démarche ERM**
- **Abordé avec le point de vue du business pour faciliter l'adoption des principes du management des risques par le management**
- **Des pistes sur la mise en perspective du niveau de risques par rapport à la performance et le « risk appetite »**
- **Un zoom sur l'impact des risques identifiés sur les objectifs aux différents niveaux de l'organisation et l'approche portefeuille**
- **Une prise en compte des bouleversements induits par la technologie**

Focus 1 : Culture du risque



La culture est partie intégrante du dispositif de maîtrise des risques

- **Alignement des comportements** attendus **avec les valeurs de l'organisation**
- Alignement des valeurs avec le **"risk appetite"**

Focus 2 : Risques et stratégie

Strategy & Objective-Setting

6. Analyzes Business Context
7. Defines Risk Appetite
8. Evaluates Alternative Strategies
9. Formulates Business Objectives

Intégration des “risques” dans la définition de la stratégie au travers de 3 dimensions :

1. **Non alignement** de la stratégie avec la mission, la vision et les valeurs
2. **Profil de risques** de la stratégie arrêtée
3. **Marges de manœuvre** en cas d’évolution de l’environnement ou de non-exécution de la stratégie

Focus 3 : Digitalisation

Review & Revision

15. Assesses Substantial Change
16. Reviews Risk and Performance
17. Pursues improvement in Enterprise Risk Management

Information, Communication, & Reporting

18. Leverages Information and Technology
19. Communicates Risk Information
20. Reports on Risk, Culture, and Performance

- Agilité et capacité d'adaptation des pratiques mises en œuvre pour faire face à la rapidité des changements du contexte, comme par exemple ceux liés à la digitalisation
- Nouvelles capacités apportées par l'analyse des données sont prises en compte

Data Generation

Proportion of data that exists today was created in the past two years

Data Analysis

Only a small fraction of available data is currently analyzed

Impact on Industry

Percentage of CEOs that believe technology will completely reshape their industry

Source: PwC Mega Trends – Technological Breakthroughs

LE CADRE DE RÉFÉRENCE AMF

Le cadre de référence AMF : Chronologie réglementaire

2007

- **1ère publication d'un cadre de référence**
- Un outils pour :
  - Améliorer le pilotage des activités
  - Sécuriser l'atteinte des objectifs
- Complément d'un guide d'application relatif au CI de l'information comptable et financière publiée par les émetteurs

2008

- Directives européennes :
  - Des obligations en matière de gestion des risques
  - Les missions du comité d'audit
- Transposition en droit français : Loi 3 juill.2008, Ord. 8 déc.2008

2010

- Publication d'une **2nde version du cadre de référence** intégrant
  - l'évolution législative et règlementaire intervenue depuis 2007
  - les évolutions des référentiels COSO ERM et ISO 31000
- Actualisation du guide de mise en œuvre adapté aux valeurs moyennes & petites

2017

- Ordonnance du 12 juillet 2017, dite de « simplification »

Le cadre de référence AMF : sa finalité

Chaque société étant responsable de :
- son organisation
- son contrôle interne
- son dispositif de gestion des risques

➢ **Contribuer à :**
  - **Une plus grande homogénéité des concepts sous-tendant la rédaction des rapports des présidents sur le contrôle interne et la gestion des risques**
  - **Aux travaux des comités d'audit**

➢ **Basé sur des principes généraux**

➢ **Pouvant être utilisé par les sociétés pour :**
  - **superviser / développer les dispositifs de contrôle interne et de gestion des risques,**
  - **sans constituer des directives sur la <u>façon de concevoir leur organisation</u>**

➢ **Aucune vocation à :**
  - **être imposé aux sociétés**
  - **se substituer aux réglementations spécifiques de secteurs d'activité**

Le cadre de référence AMF : Son périmètre

1. **Le contexte**
2. **L'approche**

II - PRINCIPES GÉNÉRAUX DE GESTION DES RISQUES ET DE CONTRÔLE INTERNE

1. **Principes généraux de gestion des risques**
2. **Articulation entre la gestion des risques et le contrôle interne**
3. **Principes généraux de contrôle interne**
4. **Périmètre de la gestion des risques et du contrôle interne**
5. **Acteurs de la gestion des risques et du contrôle interne**
6. **Limites de la gestion des risques et du contrôle interne**

III- LES QUESTIONNAIRES RELATIFS AUX PRINCIPES GENERAUX

1. Questionnaire relatif à la gestion des risques
2. Questionnaire relatif au contrôle interne comptable et financier

IV - GUIDE D'APPLICATION RELATIF A LA GESTION DES RISQUES ET AU CONTROLE INTERNE DE L'INFORMATION COMPTABLE ET FINANCIERE PUBLIEE PAR LES EMETTEURS

1. Les risques liés à l'organisation et à l'information comptable et financière
2. Les objectifs de contrôle
3. Processus de pilotage de l'organisation comptable et financière
4. Processus concourant à l'élaboration de l'information comptable et financière publiée

Le cadre de référence AMF : Sa valeur ajoutée opérationnelle

➢ Une contribution à la stratégie et au Doc de Réf.

- Introduction - Principes généraux de gestion des risques & CI	- Communiquer & éduquer - Des principes pour énoncer une stratégie, établir des politique, structurer vs les objectifs	– S'aligner sur un schéma de restitution réglementaire
Questionnaires relatifs aux principes généraux	➢ Diagnostiquer l'existant ➢ Définir des plans d'actions ➢ Auto évaluer vs. un référentiel de contrôle interne générique & exhaustif	– Formaliser le degré de maturité – Etablir des objectifs vs les éditions suivantes
Guide relatif à la gestion des risques et CI de l'info. fin. & cpt.	➢ Auto évaluer vs. un référentiel de contrôle financier professionnel ➢ Etablir une synergie formalisée et structurée avec les CAC	– Structurer le CI financier – S'assurer de la couverture des risques de l'info. financière

CONCLUSION

MERCI DE VOTRE ATTENTION !

AVANT DE PARTIR , N'OUBLIEZ PAS DE REMPLIR L'EVALUATION !

Soit sur la feuille, à remettre à l'hôtesse à la sortie
Soit directement sur la **WEB APPLI**

Merci : vous participez à l'objectif ZERO PAPIER !

Les slides seront en ligne dès la semaine prochaine sur www.amrae.fr