

Les 20 principes du COSO ERM

Les vingt principes proposés par le COSO en matière d'ERM¹ (*Enterprise Risk Management / Management du risque d'entreprise*) sont regroupés selon les cinq composantes suivantes :

- Gouvernance et culture ;
- Stratégie et définition des objectifs ;
- Performance ;
- Revue et amendement ;
- Information, communication et reporting.

Gouvernance et culture	
1. Exercer une surveillance des risques par le conseil	Le conseil assure la surveillance de la stratégie et assume les responsabilités en matière de gouvernance pour soutenir la direction générale dans la réalisation de la stratégie et des objectifs opérationnels.
2. Définir les structures organisationnelles	L'organisation définit des structures organisationnelles dans la perspective de la réalisation de la stratégie et des objectifs opérationnels.
3. Définir la culture souhaitée	L'organisation définit les comportements attendus qui caractérisent la culture souhaitée par l'entité.
4. Démontrer l'engagement en faveur de valeurs fondamentales	L'organisation démontre son engagement pour les valeurs fondamentales de l'entité.
5. Attirer, former et fidéliser des personnes compétentes	L'organisation s'engage à développer le capital humain en adéquation avec la stratégie et les objectifs opérationnels.
Stratégie et définition des objectifs	
6. Analyser le contexte de l'organisation	L'organisation prend en considération l'impact potentiel de son contexte sur le profil de risque.
7. Définir l'appétence pour le risque	L'organisation définit l'appétence pour le risque dans le contexte de la création, de la préservation et de la concrétisation de la valeur.
8. Évaluer les stratégies alternatives	L'organisation évalue les stratégies alternatives et leurs impacts potentiels sur le profil de risque.
9. Définir les objectifs opérationnels	L'organisation prend en considération les risques lors de la définition, à différents niveaux, d'objectifs opérationnels qui soient en phase avec la stratégie et la soutiennent.
Performance	
10. Identifier les risques	L'organisation identifie les risques qui affectent la réalisation de la stratégie et des objectifs opérationnels
11. Évaluer la criticité des risques	L'organisation évalue la criticité des risques.
12. Prioriser les risques	L'organisation priorise les risques pour sélectionner les modalités de traitement de ces risques.
13. Mettre en œuvre les modalités de traitement des risques	L'organisation identifie et sélectionne les modalités de traitement des risques.
14. Développer une vision globale du portefeuille de risques	L'organisation développe une vision globale et une évaluation du portefeuille de risques.

¹ Source : COSO – Le management des risques de l'entreprise - Une démarche intégrée à la stratégie et à la performance (2017)

Revue et amendement	
15. Évaluer les changements substantiels	L'organisation identifie et évalue les changements qui pourraient affecter substantiellement la stratégie et les objectifs opérationnels.
16. Réexaminer les risques et la performance	L'organisation revoit la performance de l'entité et prend en considération les risques.
17. Poursuivre l'amélioration du management des risques de l'entreprise	L'organisation poursuit l'amélioration du management des risques de l'entreprise.
Information, communication et reporting	
18. Tirer parti des données et des technologies	L'organisation exploite les systèmes d'information et technologiques de l'entité pour soutenir le management des risques de l'entreprise
19. Communiquer les informations relatives aux risques	L'organisation utilise les moyens de communication pour soutenir le management des risques de l'entreprise.
20. Rendre compte des risques, de la culture et de la performance	L'organisation rend compte des risques, de la culture et de la performance à différents niveaux et dans toute l'entité.

Si certains de ces principes sont plus ou moins proches de ceux du COSO relatif au référentiel intégré de contrôle interne, l'organisation devrait cependant conduire une démarche globale et intégrée pour identifier les faiblesses et les points forts de ses pratiques en regard de l'ensemble des principes afin de s'assurer de sa robustesse quant à la mise en œuvre de sa stratégie et à la réalisation de ses missions.