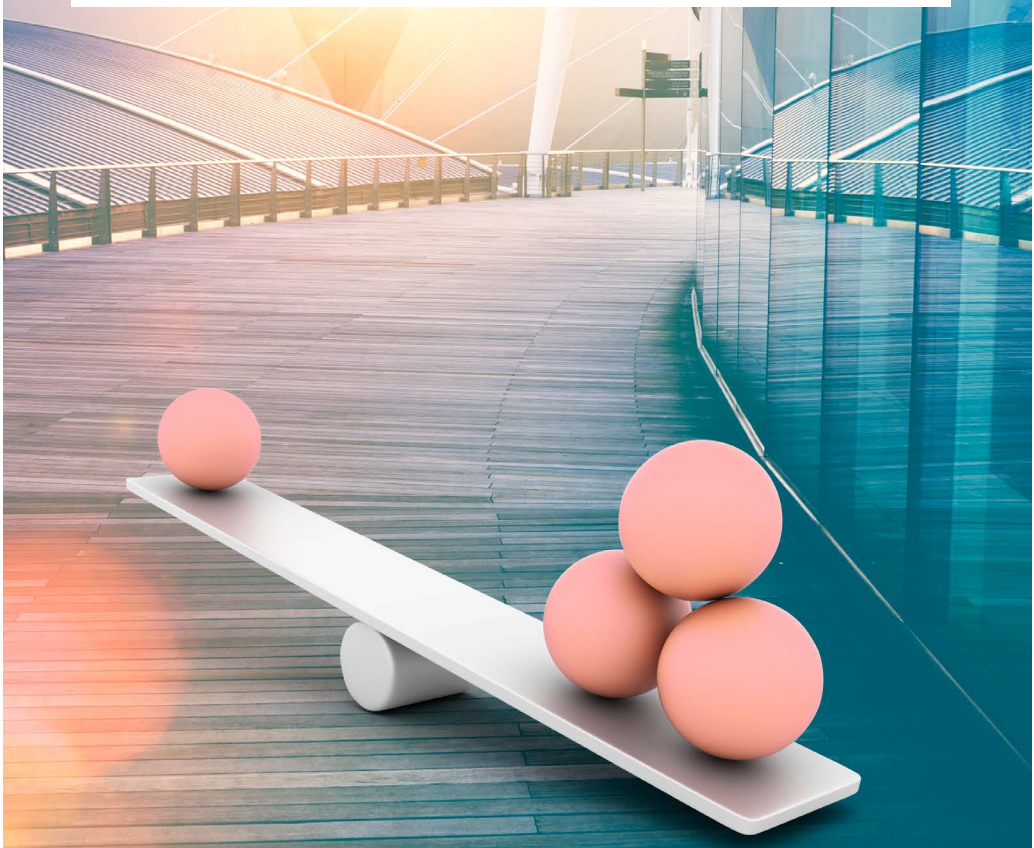
Guide pratique pour les Risk Managers

ACCOMPAGNER VOTRE ENTREPRISE DANS LA DÉFINITION DE SON APPÉTENCE AUX RISQUES



Ce document est destiné aux entreprises de l'industrie et des services et ne couvre pas les secteurs réglementés de la banque et de l'assurance.

AMRAE

pwc

L'AMRAE remercie particulièrement Françoise Bergé (PwC France et Maghreb), les membres de la Commission ERM 360° de l'AMRAE (Stéphanie Canino, Winifrey Caudron, Sylvie Mallet, Philippe Noirot), ainsi que Laurent Magne pour la préparation et la rédaction de ce document, sans oublier Gérard Payen et Anne Piot d'Abzac pour leur relecture, et Hélène Dubillot pour la coordination de la publication.

A propos de l'AMRAE

L**'AMRAE** (**A**ssociation pour le **M**anagement des **R**isques et des **A**ssurances de l'**E**ntreprise) est l'association professionnelle de référence des métiers du risque et des assurances en entreprise. Elle rassemble plus de 1 500 membres appartenant à plus de 750 organisations privées ou publiques.

L'AMRAE soutient ces organisations dans l'atteinte de leurs objectifs stratégiques et opérationnels pour leur permettre d'améliorer leurs performances et de maîtriser leurs risques.

La gestion des risques est une démarche vertueuse protégeant l'entreprise, ses employés et partenaires, y compris assureurs et, partant, l'économie dans sa globalité.

AMRAE l'Association rassemble les acteurs majeurs des lignes de maîtrise du risque (Risk Management, contrôle et audit internes, assurance, juridique, éthique...).

A travers ses comités scientifiques, ses publications et ses nombreuses manifestations, l'AMRAE produit pour ces experts les contenus qui nourrissent leurs compétences, leur évolution dans leur métier et leur contribution à la réussite de la stratégie de l'entreprise.

Avec AMRAE Formation, elle répond à leurs besoins de développement professionnel adapté aux évolutions des organisations, en dispensant des formations certifiantes de haut niveau.

AMRAE Les Rencontres organise le congrès annuel de référence des métiers du risque et des assurances (plus de 3 000 congressistes en 2020). Ces trois jours constituent le rendez-vous métier incontournable des acteurs de la maitrise des risques et de son financement.

A propos de PwC France et Maghreb

En France et au Maghreb, PwC développe des missions de conseil, d'audit et d'expertise juridique, avec pour ambition stratégique de contribuer à réconcilier entreprise, économie et société. Les entités de PwC en France et Maghreb rassemblent plus de 6000 personnes qui partagent leurs expertises au sein d'unréseau international comptant plus de 284 000 personnes dans 155 pays. Parmi ses initiatives, le cabinet s'engage dans la montée en compétences collective de tous ses collaborateurs, ses clients et ses parties prenantes afin d'anticiper les usages du futur. Rendez-vous sur www.pwc.fr.

SOMMAIRE

La prise de risque est inhérente à l'entreprise dans sa recherche de création de valeur. Toutefois, sous l'effet, par exemple, des transformations radicales de certains modèles d'affaires « classiques », de la digitalisation croissante de l'économie, du développement de nouvelles technologies, de la multiplication des réglementations, des incertitudes géopolitiques, des mutations de la société, ou des défis du changement climatique, les risques de l'entreprise évoluent rapidement. Il apparait dès lors indispensable de mieux cadrer la prise de risque. L'entreprise doit être en capacité d'examiner l'ensemble de ses risques au regard de l'opportunité de création de valeur (qu'elle soit financière ou non).

Il est essentiel pour l'entreprise d'être alignée avec ses parties prenantes internes (collaborateurs et organes de gouvernance) sur la stratégie de prise de risque et de communiquer sur ce sujet vis-à-vis de ses parties prenantes externes (clients, investisseurs et autorités).[1, 2]

Chaque entreprise[3] envisage sa prise de risque en fonction de sa vision, sa mission ou sa raison d'être, sa stratégie, sa culture, ses ressources, et le contexte dans lequel elle évolue, règlementaire en particulier. Elle définit aussi les risques qu'elle assume de prendre, c'est-à-dire, en un mot, son **appétence aux risques**[4] en fonction de ce qu'ambitionnent ou peuvent supporter ses actionnaires et ses autres parties prenantes.

L'appétence aux risques est différente d'une entreprise à une autre, elle est aussi appelée à évoluer dans le temps en fonction des transformations de l'entreprise ou sous l'influence de facteurs externes comme l'évolution de la concurrence et des technologies ou encore une période de récession économique.

Dans les secteurs de la banque et de l'assurance, le régulateur s'est saisi du sujet et impose le déploiement d'un dispositif *(Risk Appetite Framework)* visant à définir, diffuser et suivre la mise en œuvre du *Risk Appetite* qu'il définit comme *« le niveau et le type de risque qu'un établissement peut et souhaite assumer dans ses expositions et ses activités, compte tenu de ses objectifs opérationnels et de ses obligations ».*[5, 6]

Lorsqu'elles définissent leur appétence pour les risques opérationnels, les banques font face aux mêmes défis que les entreprises des autres secteurs et notamment :

- **Comment exprimer l'appétence pour le risque opérationnel au sommet de l'organisation,** compte-tenu des multiples facettes de ce risque, de l'absence de méthodes de mesure robustes et d'une gestion de ces risques souvent décentralisée dans l'ensemble de l'organisation ?
- **Comment tenir compte de l'appétence pour le risque opérationnel dans la prise de décision,** compte-tenu de la difficulté à lier une déclaration globale d'appétence au risque à des indicateurs de performance ou aux risques plus granulaires ?

Ce cadre réglementaire n'existe pas dans les autres secteurs d'activités ; toutefois des réglementations définissent pour certains risques des limites qui s'imposent aux entreprises concernées[7].

Qu'est-ce que l'appétence aux risques pour ces entreprises ? Comment est-elle définie et diffusée ? Comment le Risk manager peut-il accompagner son entreprise dans la définition et la diffusion de son appétence aux risques ?

L'AMRAE a constitué un groupe de réflexion afin de répondre à ces questions. Ce document, issu des travaux du groupe, vise à fournir aux Risk managers des éléments utiles à la formulation de l'appétence aux risques, sa diffusion au sein de l'entreprise et sa communication. Il comprend deux parties. La première rappelle les définitions et les principes, la seconde décrit des pratiques illustrées par des exemples issus de démarches mises en œuvre par certaines entreprises, notamment pour initier la discussion au sein du Conseil. Il s'adresse aux Risk managers des entreprises de toutes tailles et tous secteurs[8] et à leurs parties prenantes internes, notamment les responsables des trois lignes de maîtrise[9], les dirigeants et les administrateurs. Il s'inscrit dans la lignée des travaux de l'Institut Français des Administrateurs, IFA, qui a publié en janvier 2016 *« Le rôle du Conseil dans la détermination du Risk Appetite »*[10]. Il les complète en mettant en perspective la contribution du Risk manager sur ce thème.

1. Fiches pratiques de l'AMF relatives aux questions susceptibles de se poser concernant l'entrée en application du règlement (UE) 2017/1129 (règlement Prospectus) et notamment sur l'application de l'article 16 sur les facteurs de risques ; ESMA Guidelines on risk factors under the Prospectus Regulation, ESMA31-62-1217, mars 2019.
2. Les parties prenantes internes de l'entreprise sont notamment les dirigeants, les salariés, les syndicats, les actionnaires. Ses parties prenantes externes sont par exemple ses clients, ses fournisseurs, les autorités de contrôle, les agences de notation, et plus largement la société civile.
3. Le terme Entreprise dans ce document recouvre toutes les organisations privées, publiques et parapubliques quelle que soit leur taille.
4. La terminologie *Appétence aux Risques* a été retenue par l'AMRAE, toutefois certaines publications en français utilisent la terminologie *appétit aux risques*, d'autres encore utilisent la terminologie anglaise *Risk Appetite* sans la traduire.
5. Arrêté de contrôle interne du 3 novembre 2014 (transposition de la directive CRD IV) qui encadre la définition des risques et des limites qui sont intégrées dans le cadre d'appétence.
6. Le *Risk Appetite* est formulé au travers du *Risk Appetite Statement*, en faisant le lien avec la stratégie (à court et long terme), et en mettant en avant les limites internes pour chaque type de risque.
7. Limites d'exposition aux matières dangereuses par exemple.
8. Il ne traite pas du cas évoqué plus avant dans le texte des entreprises des secteurs tels que la banque et l'assurance pour lesquelles la réglementation encadre les pratiques relatives à l'appétence aux risques.
9. *«Trois ligne de maîtrise pour une meilleure performance»*, AMRAE et IFACI, 2013.
10. Dans la suite du document, les termes Conseil ou Conseil d'administration sont utilisés indifféremment et désignent les instances de gouvernance dans différents schémas d'organisation, comme par exemple une organisation avec directoire et conseil de surveillance.

1 Qu'est-ce que l'appétence aux risques ?

L'appétence aux risques détermine la stratégie de management des risques de l'entreprise et facilite ainsi la prise de risque dans le cadre des processus décisionnels en lien par exemple avec la définition du plan stratégique, la validation des investissements, la négociation et la signature des contrats commerciaux. Elle aide notamment à limiter les biais cognitifs dans les processus décisionnels car elle permet de mieux rationaliser les critères de prise de décision en les rendant plus homogènes.

1.1 Les définitions

Outre la définition du régulateur bancaire, les définitions de l'appétence aux risques apportées par la littérature sont nombreuses. Celles retenues par les principaux référentiels et l'IFA sont rappelées dans les paragraphes suivants.

Définition retenue par le COSO[11] dans son référentiel paru en 2017 « Le management des risques de l'entreprise : une démarche intégrée à la stratégie et à la performance »

Le *Risk Appetite* est défini comme **« le type et la quantité de risque, au sens large, qu'une entreprise est disposée à accepter afin de créer de la valeur. L'expression première du *Risk Appetite* se fait au travers de la mission et la vision de l'entreprise »[12]**.

11. COSO (Committee of Sponsoring Organizations of the Treadway Commission) est un comité regroupant plusieurs associations professionnelles américaines comme l'institut des auditeurs internes qui vise à établir des référentiels relatifs au management des risques, au contrôle interne et à la prévention de la fraude.
12. Traduction libre de la version originale en anglais : "*Risk Appetite* is the types and amount of risk, on a broad level, an organization is willing to accept in its pursuit of value. The first expression of *risk appetite* is an entity's mission and vision."

ENTREPRISE RISK MANAGEMENT

Governance & Culture

1. Exercises Board Risk Oversight
2. Establishes Operating Structures
3. Defines Desired Culture
4. Demonstrates Commitment to Core Values
5. Attracts, Develops, and Retains Capable Individuals

Strategy & Objective-Setting

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

Performance

10. Identifies Risk
11. Assesses Severity of Risk
12. Prioritizes Risks
13. Implements Risk Responses
14. Develops Portfolio View

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

L'un des vingt-trois principes développés par le COSO (principe 8) traite du *Risk Appetite* et décrit les bonnes pratiques préconisées :

- L'entreprise définit son *Risk Appetite* en lien avec sa culture et sa stratégie.
- Pour ce faire, elle s'appuie sur une panoplie de techniques comme des ateliers, l'analyse de l'historique des objectifs de performance vs celui des résultats, ou encore la modélisation de scénarios de risques.
- Le *Risk Appetite* est formulé en termes généraux par nature de risque (risques inacceptables) ou quantitativement (montant de risque).
- Les dirigeants favorisent une culture d'entreprise qui responsabilise le management sur la prise en considération des risques et du *Risk Appetite* dans la prise de décision.

1

En 2020, COSO a publié une prise de position sur l'apport de l'appétence aux risques pour les entreprises qui doivent gérer leurs activités dans un contexte géopolitique et socio-économique mondial mouvementé[13].

> Définition retenue par l'AFNOR dans le cadre de la norme ISO 31000 « Management du risque - Lignes directrices »

La politique d'appétence aux risques consiste **en la formalisation par les instances dirigeantes des attentes et des limites en matière de prise de risques.** Cette formalisation doit être l'aboutissement d'échanges dans lesquels les points de vue des instances dirigeantes et, plus globalement, des parties prenantes ont été pris en compte, à tout le moins ont été entendus. La politique d'appétence est le document final qui explicite la vision retenue pour l'organisation en matière de prise de risques. Elle fait foi et s'applique à tous.

> Définition retenue par l'IFA dans le cadre de ses travaux de 2016

Le *Risk Appetite* est **« la définition du type et du niveau des risques qu'une entreprise est prête à accepter au regard de sa stratégie. Ce niveau de risque « voulu » est la balance entre les bénéfices potentiels de la prise de risque (une innovation, un investissement, etc.) et les menaces inhérentes à tout changement ».**

1.2 Position de l'AMRAE

L'appétence aux risques est une notion clé qui accompagne – ou devrait accompagner - toute prise de décision pour l'éclairer, quels que soient son niveau (stratégique ou opérationnel) et son domaine (opérations, ressources humaines, finance, technologie de l'information, marketing, juridique, communication, etc.).
L'entreprise doit travailler à l'équilibre entre la valeur attendue d'une décision et le niveau de risque que celle-ci engendre ou qu'elle est prête à prendre pour la mettre en œuvre.

Formuler l'appétence aux risques de l'entreprise est un exercice complexe. Cela nécessite tout d'abord de prendre en compte les valeurs, les ressources, la culture, la stratégie de l'entreprise, et le contexte réglementaire. Il faut également gérer l'équilibre entre les différents points de vue s'exprimant dans une équipe dirigeante. Enfin, sans

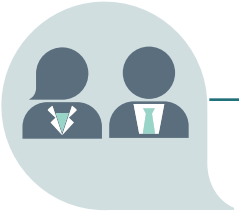
13. *Risk Appetite – Critical to Success, Using Risk Appetite to Thrive in a Changing World*, COSO, 2020.

remettre en cause la souveraineté de l'équipe dirigeante, il est parfois utile de prendre en considération les attentes de certaines parties prenantes, lesquelles peuvent avoir un regard et des analyses différents sur la stratégie et les objectifs de l'entreprise. Cette formulation est complétée pour certains domaines de risques auxquels l'entreprise est exposée par la fixation de limites qui sont parfois (et pas uniquement) des limites édictées par la réglementation.

L'entreprise doit par ailleurs constamment s'adapter aux nouvelles menaces de son environnement dont certaines sont liées à des opportunités. Cela est par exemple le cas pour les risques liés à la cybersécurité et les opportunités liés à la digitalisation. Dès lors, en lien avec ses parties prenantes, l'entreprise doit être capable de préciser son appétence au regard de ces risques.

L'appétence aux risques s'exprime également dans les choix de l'entreprise en matière de couverture assurantielle et notamment l'arbitrage qu'elle opère entre faible prime et forte franchise ou forte prime et faible franchise. De même, les crises que l'entreprise a pu traverser dans son histoire et la manière dont celles-ci ont été vécues et gérées laissent une trace sur son niveau d'appétence.

La direction générale a la responsabilité de formuler l'appétence au risque de l'entreprise, de fixer les limites pour les domaines de risques pour lesquels cela est pertinent et d'en obtenir la validation auprès du Conseil d'administration[14]. Ce dernier doit pour sa part, au travers d'un dialogue avec la direction générale, s'assurer que l'appétence aux risques proposée est en adéquation avec les valeurs, la stratégie et les ressources de l'entreprise.



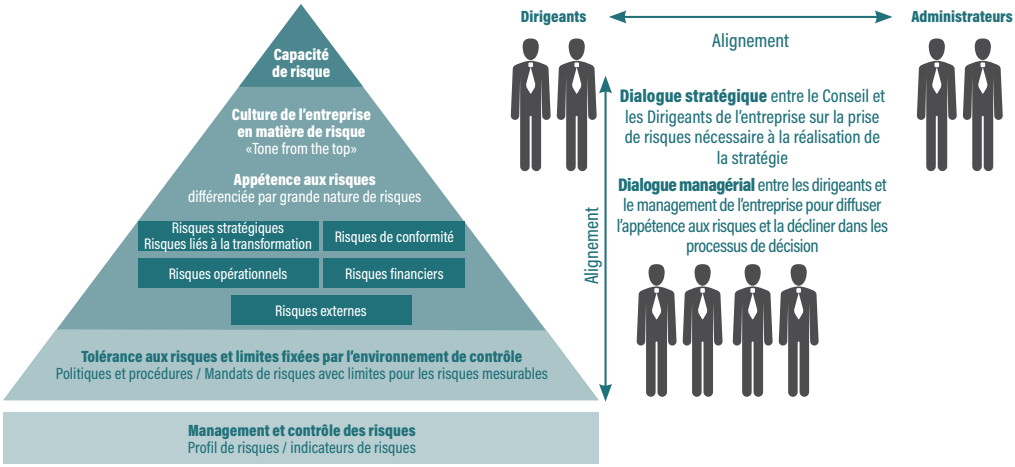
Le Risk manager est associé à cette démarche. Il apporte un appui technique et méthodologique en fournissant des informations sur les pratiques sectorielles, en animant les réflexions autour de la prise de risques dans l'entreprise, en étant en appui de la formulation de l'appétence aux risques, de la définition des limites et des échanges avec le Conseil d'administration. Il accompagne la diffusion de l'appétence aux risques dans le cadre de ses analyses de risques et dans les instances décisionnelles auxquelles il participe.

14. Ou un comité habilité par le conseil à cet effet.

1

1.3 Les composantes de la maîtrise des risques associées à l'appétence aux risques

L'appétence aux risques doit être abordée en lien avec plusieurs autres composantes de la maîtrise des risques qui sont représentées dans le schéma ci-dessous.

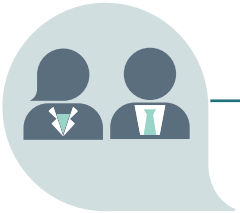


La capacité de risque de l'entreprise

Le niveau de risque que l'entreprise peut supporter est déterminé par ses ressources financières, incorporelles et humaines, les contraintes réglementaires et opérationnelles (ex : infrastructures techniques, expertise, etc.) qui s'appliquent à elle et aux engagements qu'elle a pris vis-à-vis de ses parties prenantes.

La capacité de risque est le niveau de risque maximum que l'entreprise peut supporter sur une période donnée sans remettre en cause sa pérennité. L'appétence aux risques est fixée en tenant compte de cette capacité.

Les échanges entre le Conseil d'administration et la direction générale sur la capacité de risque de l'entreprise sont importants, le sujet étant stratégique. Le Conseil peut considérer que les dirigeants ne prennent pas assez de risques au regard de la capacité de l'entreprise et de la création de valeur attendue, ou inversement qu'ils en prennent trop.



Le Risk manager aide l'entreprise à s'assurer que les risques auxquels elle est exposée ne dépassent pas sa capacité de risque en élaborant des scénarios de risques (scénarios « du pire » restant réalistes) et des scénarios de cumuls de risques. Il peut, pour cela, s'appuyer sur des études actuarielles.

La culture de l'entreprise en matière de risque

La culture de l'entreprise influence la prise de risque. Elle détermine la façon dont l'ensemble des collaborateurs (dirigeants, managers et personnels) perçoivent les risques auxquels l'entreprise est confrontée, les comprennent, échangent et agissent face à ceux-ci.

Elle influence aussi la perception du risque. Le risque est la plupart du temps perçu comme une menace dont l'entreprise redoute la survenance. Cependant, la prise de risque est indissociable de l'acte d'entreprendre et nécessaire à la réalisation de la stratégie de l'entreprise. A ce titre, les différences de perception du risque sont souvent mises en avant entre les entreprises dites « matures » qui développent plutôt une perception du risque orientée vers la menace et les « start-up » qui inversement se focalisent en général plus sur les opportunités.

1

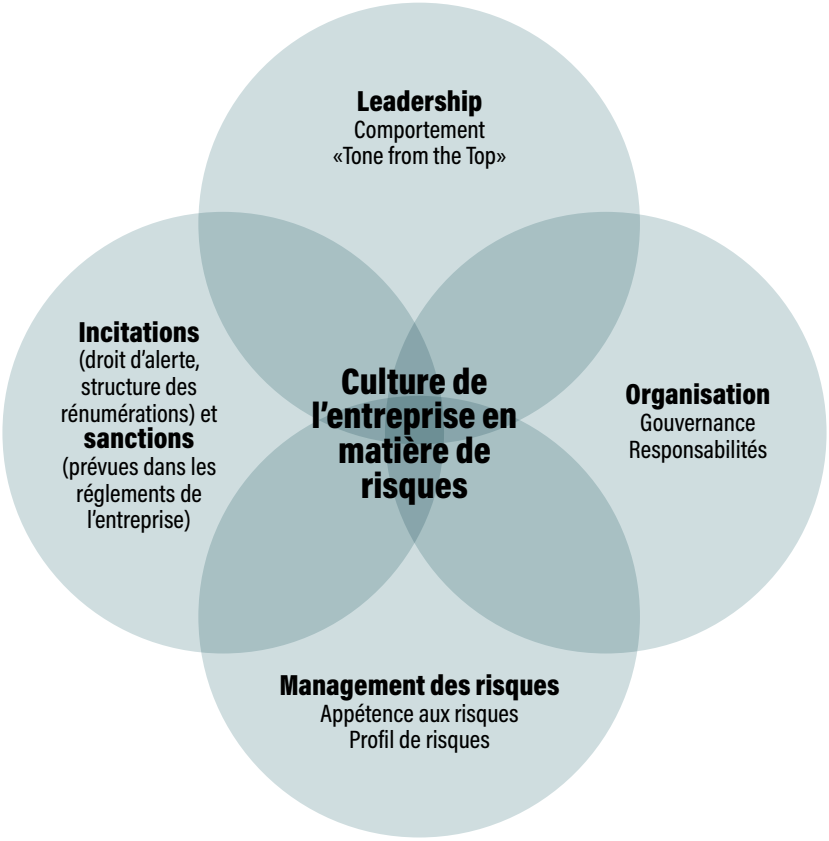
L'appétence aux risques vise précisément à traiter cette contradiction apparente : il s'agit d'encadrer la prise de risque grâce à une réflexion partagée sur les risques que l'entreprise est prête à prendre selon les situations[15]. L'entreprise peut décider de prendre un risque si celui-ci est porteur d'opportunités (par exemple une innovation ou une acquisition) ou si elle est en capacité de réagir à sa survenance ou d'en absorber les impacts. Le risque est parfois inhérent à son modèle économique ou opérationnel (ceci est par exemple le cas pour les industries qui traitent des produits dangereux), ou bien nécessaire à sa pérennité (redéploiement de ses activités en cas de disruption sur son métier cœur par exemple). Inversement, certains risques sont qualifiés de « non acceptables ». Il s'agit notamment des risques portant atteinte aux personnes et à l'environnement ou relevant de la transgression des règles éthiques et des lois.

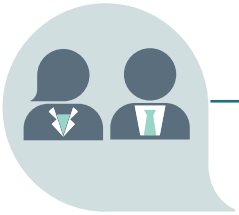
Des révisions récentes de plusieurs codes de gouvernement d'entreprise[16] mettent en avant le rôle du Conseil dans la définition, l'évaluation et la supervision de la culture de l'entreprise.

On peut citer, parmi les principaux éléments constitutifs d'une culture du risque :

- L'exemplarité des comportements au plus haut niveau de l'organisation,
- Un environnement ouvert à la prise de parole et à la discussion,
- L'analyse systématique des crises ou quasi crises que subit l'entreprise[17] afin d'en tirer les leçons,
- Une prise de conscience partagée des risques auxquels l'entreprise est exposée.

15. Certains articles ou prises de positions introduisent les notions de risques redoutés vs risques pris ou encore de risques voulus vs subis.
16. Par exemple : le *UK Corporate Governance Code* qui, à l'instar des autres codes, prescrit l'évaluation de la culture de l'entreprise par le conseil, le *Japan's Corporate Governance Code* ou le *Dutch Corporate Governance Code*.
17. L'examen des crises subies par les autres entreprises est aussi source d'enseignements précieux pour l'entreprise.





Le Risk manager contribue avec les autres fonctions de la deuxième ligne de maîtrise à la définition et à la diffusion de comportements adaptés à la culture et à l'appétence aux risques de l'entreprise. Il collabore avec l'audit interne pour évaluer l'alignement entre les comportements réels et ceux attendus, et pour s'assurer que les mesures nécessaires sont prises afin de réduire les éventuels écarts.

1

La tolérance aux risques et les limites fixées par l'environnement de contrôle

La tolérance aux risques traduit, pour les risques quantifiables, un certain degré de flexibilité autour d'une valeur cible qui découle du cadre fixé par l'appétence aux risques. Opérer dans les limites de la tolérance au risque permet de s'assurer que l'entreprise agit en cohérence avec son appétence aux risques. Ainsi, une entreprise qui a défini le taux d'indisponibilité maximum de ses systèmes d'information critiques à 0,01% peut tolérer un écart de 20% par rapport à ce taux pour les filiales qu'elle intègre.

La différence entre appétence et tolérance s'illustre notamment pour les risques jugés inacceptables par l'entreprise comme par exemple les risques liés à la santé, sécurité et à la corruption. Le risque « zéro » n'existant pas, sauf à supprimer l'activité à son origine, la tolérance aux risques permet de reconnaitre le fait que des évènements peuvent survenir malgré les dispositifs de prévention en place. La survenance d'un risque doit alors systématiquement s'accompagner d'une analyse des causes, de mesures de traitement et le cas échéant de sanctions.

Ces éléments sont documentés dans les politiques, les procédures ou encore les mandats de risques qui constituent l'environnement de contrôle de l'entreprise. Lorsque cela est possible, comme, par exemple, pour les risques financiers, des indicateurs sont mis en place pour suivre le respect des limites.

Le profil de risque de l'entreprise

Le profil de risque de l'entreprise est généralement établi à l'aide de la cartographie des risques, un exercice le plus souvent coordonné par le Risk manager. Il reflète les risques auxquels l'entreprise est exposée, identifiés au moment où la cartographie est réalisée.

La cartographie des risques repose sur une échelle d'impacts propre à l'entreprise qui, lorsque l'entreprise n'a pas encore défini son appétence aux risques, constitue un indicateur de cette appétence. En effet, cette échelle d'impacts, souvent proposée par le Risk manager, puis validée par la direction générale et les organes de gouvernance, détermine les seuils au-delà desquels les conséquences d'un risque seront considérées comme critiques et/ou devant faire l'objet d'une mesure de traitement.

Lorsque l'entreprise a défini son appétence aux risques, le Risk manager propose une échelle d'impacts en cohérence avec l'appétence.

Des actions de renforcement de la maîtrise des risques sont décidées lorsque la criticité[18] d'un risque est jugée trop élevée et doit être ramenée à un niveau cible (niveau maximal auquel l'entreprise souhaite voir évoluer le risque, à une échéance donnée). Cette cible, validée par les dirigeants, traduit directement l'appétence aux risques de l'entreprise pour les risques de cette nature.

Certains risques critiques nécessaires à la réalisation de la stratégie de l'entreprise seront acceptés bien que restant élevés malgré les mesures prises, même si celles-ci sont – et doivent être – renforcées. On peut par exemple citer le risque lié à la cybercriminalité, risque externe pour lequel l'entreprise ne dispose pas de tous les leviers de maîtrise, corolaire des stratégies actuelles de digitalisation des processus ou des offres.

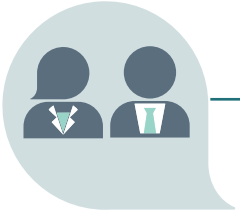
Enfin, l'entreprise met en place un suivi de son exposition aux risques et de la mise en œuvre des renforcements de la maîtrise des risques qu'elle a décidés.

1.4 Les principales caractéristiques de l'appétence aux risques

L'appétence aux risques est, par définition, alignée avec les valeurs et la stratégie de l'entreprise

Les valeurs et les engagements portés par l'entreprise par exemple en matière de santé, sécurité et bien-être au travail, d'éthique ou d'inclusion préfigurent l'appétence aux risques de l'entreprise dans certains domaines.

Par ailleurs, lorsque la direction générale décrit les orientations choisies et les moyens mis en place par l'entreprise pour atteindre ses objectifs stratégiques, elle doit aussi définir et communiquer sur le niveau de risque que l'entreprise est prête à accepter dans le cadre de cette stratégie. Ainsi, pour poursuivre avec l'exemple du risque lié à la cybercriminalité, une stratégie de digitalisation des produits ou des activités de l'entreprise implique d'augmenter l'exposition à la menace « cyber ». Lorsqu'elle définit sa stratégie, l'entreprise fixe des objectifs de part de marché et de marge pour les nouveaux produits ou des objectifs d'efficacité pour ses activités. Elle doit, en regard, déterminer l'appétence aux risques pour que des moyens appropriés de prévention, de détection et de gestion des évènements soient déployés.



Le Risk manager contribue à formuler l'appétence aux risques dans le cadre des travaux de la gouvernance et des comités stratégiques. Il s'assure par la suite dans les instances de décisions auxquelles il participe, que les discussions autour de l'équilibre entre les risques pris et les opportunités attendues sur chaque décision sont en ligne avec l'appétence aux risques formulée dans le cadre de la stratégie.

18. La criticité d'un risque correspond au croisement de sa probabilité de survenance et de ses impacts.

1

L'appétence aux risques prend en compte les attentes des parties prenantes

Les parties prenantes internes et externes de l'entreprise expriment par différents moyens leur perception des risques et leurs attentes en matière de maîtrise.

Ainsi s'agissant des parties prenantes internes :

- Les discussions en Conseil d'administration (autour de la cartographie des risques ou d'opérations que l'entreprise soumet à l'approbation du Conseil notamment) et les échanges lors des séminaires stratégiques permettent aux administrateurs de s'exprimer sur leur appétence aux risques. Cela se fait au travers de leurs attentes en matière de création de valeur, de leur perception des menaces qui pèsent sur l'activité de l'entreprise (comme par exemple les disruptions technologiques ou les risques sur les hommes clés) et de leurs attentes en matière de prévention de certains risques comme les risques de fraude ou de corruption.
- Les enquêtes auprès des salariés et les échanges en réunions du comité social et économique avec les représentants du personnel permettent d'appréhender leur perception de certains risques et leurs attentes en matière de prévention de ces risques.

Par ailleurs, pour les parties prenantes externes, les entreprises mettent souvent en place des systèmes d'écoute basés sur des moyens comme des enquêtes clients, des études de matérialité ou des comités des parties prenantes dans le cadre de leur démarche RSE (Responsabilité Sociétale des Entreprises) afin de comprendre leur perception et leur acceptabilité des risques.

De plus les entreprises partagent des règles, des engagements ou des pratiques avec leurs prestataires et leurs fournisseurs, notamment pour prendre toutes les mesures nécessaires en matière de maîtrise des risques liés au respect des droits humains, à la santé et la sécurité au travail, au respect du droit du travail, au respect des exigences climatiques et environnementales, ou encore à la prévention de la corruption.

Lorsqu'elle formule son appétence aux risques, l'entreprise tient compte de ces éléments. Elle assure ainsi une cohérence globale entre la stratégie, les valeurs, la culture, les engagements et les réalisations de l'entreprise. Or, cette capacité à assurer la cohérence est aujourd'hui une attente des parties prenantes tant internes qu'externes de l'entreprise. Ainsi, à terme, les entreprises qui communiqueront sur leur appétence aux risques renforceront la confiance de leurs parties prenantes.

L'appétence aux risques s'exprime généralement en des termes qualitatifs. Pour certains domaines de risques, l'expression de l'appétence aux risques s'accompagne d'une cible quantifiée.

Par exemple concernant le développement de nouvelles activités ou de nouveaux produits dans le cadre du plan stratégique de l'entreprise, l'appétence aux risques s'exprime quantitativement en termes de pertes financières acceptables au regard des gains attendus et de la capacité de risque de l'entreprise.

Pour les risques financiers tels que les risques liés aux taux de change, les risques sur les marchés financiers ou sur les marchés de matières premières, l'appétence aux risques s'exprime aussi quantitativement en termes de pertes financières acceptables au regard des gains attendus, du coût de la couverture et de la capacité de risque de l'entreprise.

Dans d'autres domaines, les impacts des risques ne se mesurent pas directement en termes de pertes financières mais sont quantifiables. C'est par exemple le cas du risque de non-qualité des produits qui peut s'exprimer par un taux de rebut. L'appétence aux risques est alors déterminée au regard de la stratégie de l'entreprise, des exigences qualité des clients, du niveau recherché de satisfaction clients, du coût de la non-qualité et du coût des mesures d'amélioration. Elle se traduit en objectifs sur le niveau de qualité.

Pour les risques difficilement quantifiables, comme les risques liés à l'indisponibilité de ressources ou de fonctions essentielles à la survie de l'entreprise, l'entreprise peut formuler son appétence aux risques en inscrivant dans ses politiques une exigence en matière de continuité d'activité, incluant la priorisation de l'accès aux ressources (et par exemple un plan de succession ou un plan d'assurance prévoyance dite « homme-clé »).

Enfin, comme évoqué précédemment pour des risques ayant des impacts sur la santé, la sécurité et le bien-être des salariés ou des populations, ou encore sur l'environnement ou la corruption, les entreprises s'expriment généralement sur leur inacceptabilité et s'engagent dès lors sur la mise en œuvre de moyens de protection au niveau des meilleures pratiques.

2 Formuler, diffuser et communiquer l'appétence aux risques

L'appétence aux risques encadre le niveau de risque pris par l'entreprise dans chacune de ses décisions structurantes au regard des bénéfices attendus, par exemple :

- Le lancement d'un nouveau produit,
- Le développement d'un nouveau marché (nouveau segment ou nouvelle zone),
- Une offre commerciale (et sa contractualisation),
- Le lancement d'un projet de transformation de l'entreprise,
- Un projet d'acquisition externe.

L'appétence aux risques se forge, se diffuse et s'exprime dans l'entreprise au travers notamment :

- Des échanges et décisions au sein des instances de gouvernance,
- Des échanges et décisions dans les comités (comité d'investissement, comité nouveaux produits, comité des offres, comités de pilotage des projets de transformation, comité éthique ou de déontologie...),
- Des échanges et décisions dans le cadre de la réalisation et de l'examen des cartographies globales des risques (à la maille de l'entreprise, à la maille d'une entité ou à la maille d'un processus par exemple) et des analyses de risques ciblées (risques industriels, risques liés aux marchés financiers, risque de corruption, risques de fraude, risques psycho-sociaux...),
- De l'environnement de contrôle (délégations de pouvoirs, délégations d'autorité ou de signature, politiques et procédures),
- Des échanges et décisions dans le cadre des revues d'activités,
- De l'attitude du management de proximité et des dirigeants, qui peut encourager ou dans certains cas freiner ou empêcher l'expression des risques et la discussion des stratégies de traitement.

Elle est aussi influencée par les biais cognitifs individuels et collectifs. En effet, comme le souligne le rapport de l'IFA, les études comportementales menées sur les biais cognitifs dans la prise de décision, notamment lorsqu'elle comporte des risques (par exemple lors des comités d'investissements ou de lancement de nouveaux produits) montrent que l'individu a une forme de réticence à prendre des risques identifiés, tout en étant structurellement « optimiste » ou confiant dans l'avenir. Les entreprises ont tendance à amplifier ces comportements, notamment du fait d'une asymétrie entre la prise de risque et le gain espéré, et parfois d'une déresponsabilisation individuelle au profit du consensus.

On voit que l'appétence aux risques qui existe de facto dans l'entreprise peut in fine ne pas correspondre à celle qui aurait été voulue par le Conseil d'administration, et ne pas être adaptée à la capacité de risque de l'entreprise. La formulation de l'appétence aux risques permet d'éviter les écarts potentiels et de mieux les détecter, et favorise l'alignement structurel des décisions de l'entreprise.

2

2.1 Rôles et responsabilités en matière de formulation et de diffusion de l'appétence aux risques

Dans le cadre des missions qui lui sont confiées par le Code de commerce[19], le Conseil d'administration établit la raison d'être et définit la stratégie de l'entreprise sur la base des propositions de la direction générale de l'entreprise. A ce titre, il lui revient de formuler l'appétence aux risques et le cadre dans lequel la direction générale exécute la stratégie. Par ailleurs, au titre de la mission de suivi de l'efficacité des systèmes de gestion des risques et de contrôle interne confiée au comité d'audit, et notamment au travers de l'examen de la cartographie des risques, le Conseil s'assure que le profil de risque de l'entreprise est en adéquation avec l'appétence aux risques.

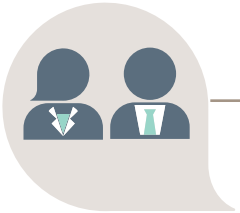
La direction générale définit le cadre (délégations de pouvoir, politiques, autorisations d'engagement, comités décisionnels) dans lequel les décisions sont prises au sein de l'entreprise. A ce titre, elle s'assure de la cohérence de ce cadre avec l'appétence aux risques. Elle contribue aussi à la diffusion et au respect de l'appétence aux risques par sa volonté de mettre en avant la recherche d'un équilibre entre opportunités et risques dans les décisions.

Les directions fonctionnelles de la deuxième ligne de maîtrise définissent les règles qui prévalent en matière d'environnement de contrôle (politiques et procédures) et suivent leur bonne application dans l'entreprise.

Les directions opérationnelles de l'entreprise, première ligne de maîtrise, sont responsables de gérer les risques intrinsèques à leurs activités et les risques induits par les décisions qu'elles prennent dans le cadre de l'appétence aux risques. Elles mettent en œuvre pour cela des opérations de contrôle dans le respect des règles fixées (contrôle de premier niveau). Elles intègrent le suivi des risques au même titre que le suivi de la performance dans le pilotage des activités.

L'audit interne, troisième ligne, s'assure dans le cadre de ses travaux de vérification que l'environnement de contrôle est en cohérence avec le niveau d'appétence formulé et se traduit par des règles et des indicateurs appropriés.

19. Articles L 225-35 et suivants.



Le Risk manager est en appui de la direction générale et des premières et deuxième ligne de maîtrise. Il fournit le cadre méthodologique et accompagne la formulation et la diffusion dans l'entreprise de l'appétence aux risques. En lien avec les autres fonctions de la deuxième ligne, il assure un contrôle de second niveau du respect du cadre.

Le Risk manager se coordonne avec la direction de l'audit interne (troisième ligne de maîtrise) dont les travaux apportent une évaluation objective et indépendante du niveau de contrôle des risques couverts par son plan d'audit. La non mise en œuvre validée par le management d'une recommandation importante de l'audit interne peut traduire un manque d'alignement sur l'appétence aux risques au sein de l'organisation.

2.2 Formulation de l'appétence aux risques

Partant de l'idée dégagée plus haut qu'entreprendre induit de prendre des risques dans le respect des valeurs de l'entreprise, et dans un environnement où les ressources humaines et matérielles sont par définition limitées, une formulation générale de l'appétence aux risques se dessine.

Ainsi, bien que la formulation de l'appétence aux risques ne soit pas aujourd'hui une pratique répandue en dehors des secteurs de la banque et de l'assurance, toutes les décisions stratégiques ou significatives de l'entreprise sont le reflet de son appétence aux risques.

La formulation de l'appétence aux risques instaure un dialogue entre le Conseil et les dirigeants sur les limites dans lesquelles la direction générale exécute la stratégie et de ce fait contribue à l'efficacité de la gouvernance.

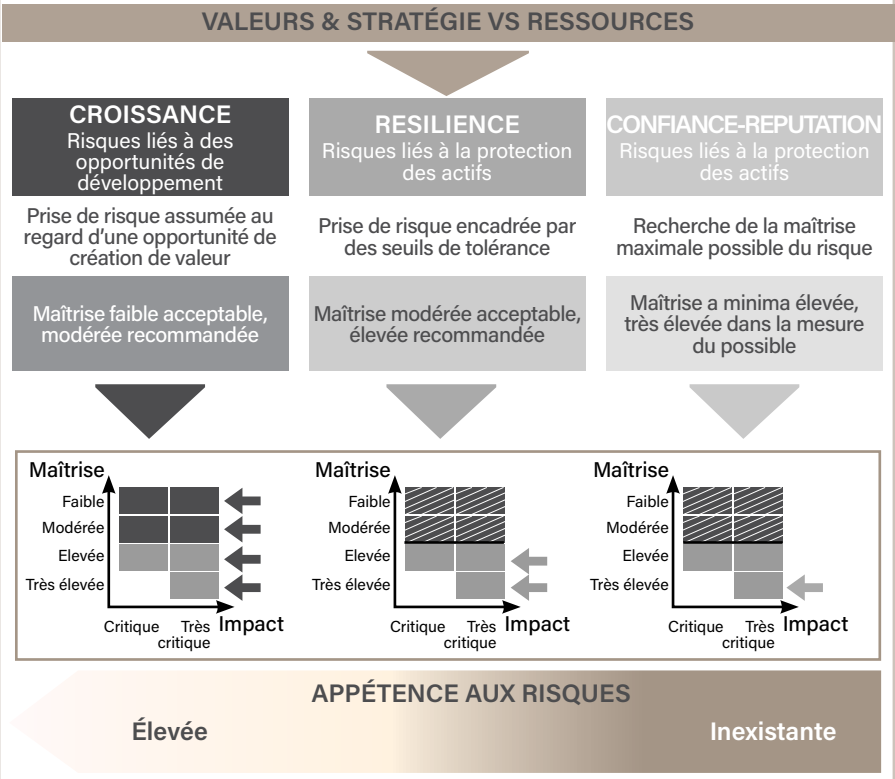
Elle s'appuie aussi sur des discussions en Conseil autour de la capacité de l'entreprise à faire face à des scénarios de risques « raisonnablement pessimistes »[20], « noirs »[21] ou « disruptifs »[22] pour aligner la direction générale et les administrateurs sur la capacité et la volonté de l'entreprise à prendre certains risques.

20. Scénario prenant en compte des situations et des évènements au-delà des variations de paramètres prises en compte dans les études de sensibilité du scénario médian de référence.
21. Scénario dont l'impact pourrait être catastrophique mais dont la probabilité d'occurrence est très peu probable. L'augmentation des crises et les risques environnementaux qui pèsent sur l'activité des entreprises amènent les entreprises à évaluer leur capacité de résilience à de tels scénarios.
22. Scénario prenant en compte un changement dans l'environnement compétitif ou une innovation technologique qui change fondamentalement les hypothèses prises en compte dans le scénario médian de référence.

Illustration 1

Dans l'exemple ci-dessous, le Risk manager propose de formuler l'appétence aux risques en lien avec le niveau de maîtrise cible en distinguant trois natures de risques :

- Les risques liés à des opportunités de développement (lancement d'un nouveau produit ou d'un nouveau marché, croissance externe...) ;
- Les risques liés à la protection des actifs majeurs (arrêt partiel ou total de production) ou impactant l'efficacité des activités (défaillance d'un fournisseur) ;
- Les risques liés à l'éthique, la conformité ou la sécurité (des personnels et des clients).



Lors d'une prise de décision, les trois natures de risques coexistent souvent : la formulation de l'appétence aux risques permet de structurer le débat et les choix à effectuer.

La pratique montre que si la formulation de l'appétence aux risques de réputation et de résilience fait en général consensus, celle concernant les risques de croissance est souvent un sujet de débats.

Illustration 2

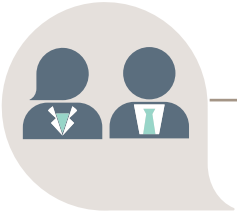
Le tableau ci-dessous illustre les types de formulation de l'appétence aux risques possibles, appétence globale ou par nature de risques.

Types de formulation		Exemples
Qualitative	Une formulation qualitative de l'appétence aux risques décrit la culture de risque de l'entreprise, quels risques sont acceptables et pourquoi. Elle fait aussi le lien entre la gestion des activités et de la performance et la gestion des risques.	▪ L'entreprise reconnait que certains risques, bien qu'ayant des impacts potentiels indésirables, ne peuvent pas être évités. ▪ L'entreprise accepte les risques pour lesquels le coût du traitement excède les pertes estimées, ou pour lesquels les pertes estimées restent dans le cadre des limites de tolérance. ▪ L'entreprise définit les comportements qui ne sont pas tolérés, par exemple le non-respect des règles ou l'atteinte à l'environnement.
Quantitative	Une formulation quantitative repose sur des seuils qui indiquent le niveau de risques toléré.	▪ Niveau de performance, par exemple taux de défaillance des systèmes critiques. ▪ Seuils pour les autorisations d'engagement.
Absolue	La formulation de l'appétence aux risques fixe le montant de risque acceptable exprimé en €, volumes, délai.	▪ Tolérance zéro sur les risques de non-conformité.
Relative	Le montant de risque acceptable est variable par rapport à un *benchmark.*	▪ Ne pas subir des pertes plus importantes que les concurrents. ▪ Les pertes tolérables sont exprimées en proportion du résultat opérationnel.

Illustration 3

L'illustration ci-dessous fournit un exemple d'échelle pour exprimer qualitativement l'appétence au risque, globalement ou par nature de risques.

Aucune expression	Appétence modérée	Faible appétence	Pas d'appétence	Appétence nulle
	Expression d'une appétence se traduisant par une gestion active pour contenir, maîtriser et limiter le risque.		Expression de l'appétence typiquement utilisée pour les risques de non-conformité. En pratique la différence entre ces deux expressions correspond au niveau de tolérence quant à la survenance d'évènements et aux mesures prises en cas de survenance.	



Le Risk manager en lien avec les fonctions de la deuxième ligne, et notamment la fonction en charge d'animer l'élaboration de la stratégie, facilite les échanges au sein des comités[23] et du Conseil pour faire émerger une formulation de l'appétence aux risques qui est revisitée si nécessaire dans le cadre des cycles stratégiques.

Il coordonne l'analyse des scénarios de risques « noirs » et disruptifs » et anime les discussions en Conseil.

23. Comité des risques lorsqu'il existe, comité de direction, comité exécutif ou directoire.

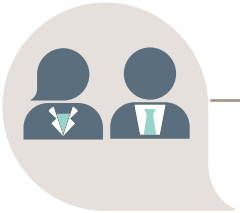
2.3 Diffusion de l'appétence aux risques au sein de l'entreprise

Au travers de ses valeurs et de sa stratégie, l'entreprise diffuse largement des éléments de son appétence aux risques.

Par ailleurs, depuis le début des années 2000 sous l'impulsion croisée de la loi[24] et des codes et guides professionnels[25], les entreprises ont structuré leur gouvernance et développé un environnement de contrôle qui fournit un cadre pour la prise de décision à tous les niveaux de l'organisation. Il s'agit par exemple :

- Des directives pour la sélection des fournisseurs,
- Des directives interdisant toute activité commerciale avec d'autres tiers faisant l'objet de sanctions économiques,
- Des directives en matière de sécurité et de santé au travail accompagnées d'objectifs et d'indicateurs suivis du taux d'accidents,
- Des directives en matière de disponibilité des systèmes d'information accompagnées d'objectifs et d'indicateurs suivis du taux de défaillance,
- Des mandats de risques pour les risques liés aux investissements sur les marchés financiers (placements de trésorerie par exemple) ou les risques liés aux marchés de l'énergie et des matières premières,
- Des directives en matière d'anti-corruption et anti-blanchiment (cf. loi dite Sapin2).

Les directives et les pratiques forment un cadre qui transcrit l'appétence aux risques de l'entreprise et en est un vecteur de diffusion.



Le Risk manager en lien avec le contrôle interne et les autres fonctions de la deuxième ligne de maîtrise analyse la cohérence du cadre procédural et des limites fixées et rend compte à la direction générale et à la gouvernance des éventuelles incohérences, des besoins d'ajustement au fil du temps sous l'influence de facteurs internes ou externes et le cas échéant des manques.

L'audit interne dans le cadre de ses travaux évalue périodiquement cette cohérence.

24. Loi sur les nouvelles régulations économiques (NRE, 2001), loi de sécurité financière (LSF, 2003), loi du 3 juillet 2008 portant diverses dispositions d'adaptation du droit des sociétés au droit communautaire (dite « loi DDAC »), recommandations de l'autorité des marchés financiers (AMF).
25. Code Afep-Medef de gouvernement d'entreprise des sociétés cotées (actualisé en janvier 2020) ainsi que les nombreux guides publiés par l'IFA, l'IFACI et l'AMRAE.

2

L'appétence aux risques est aussi diffusée dans l'entreprise via l'expression de ses valeurs et de ses engagements qui influencent les comportements.

Enfin, les discussions dans le cadre du dialogue managérial (discussions avec le management de proximité, discussions dans les revues d'activités) et les discussions dans les instances de décision (comme le comité des offres ou le comité d'investissement) sont le troisième pilier de la diffusion de l'appétence aux risques.

Il résulte de la diffusion de l'appétence aux risques une culture d'entreprise où les décisions sont prises en tenant compte de la capacité et de la volonté de l'entreprise à prendre certains risques.

Des analyses de risques sont-elles réalisées et prises en compte dans l'élaboration de la stratégie ou des plans à moyen terme ?

Si oui, ces analyses sont-elles déclinées selon plusieurs scénarios ? Par exemple : un scénario « raisonnablement pessimiste », un scénario « noir » (ou scénario « du pire »), et un scénario « disruptif ».

Les dirigeants statuent-ils sur l'acceptabilité des risques majeurs au regard de la capacité de risque de l'entreprise ?

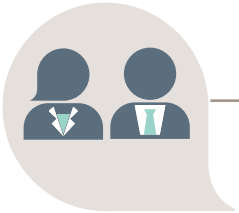
Des analyses de risques indépendantes sont-elles fournies aux instances décisionnelles ?

L'équilibre risques / opportunités / capacité de financement est-il abordé lors des instances décisionnelles ?

Les risques sont-ils traités avec l'attention nécessaire lors des revues de performance ?

Les dérives des indicateurs par rapport aux limites acceptables sont-elles explicitées lors des revues de performance ?

Les risques sont-ils un sujet habituel dans le dialogue managérial en général ?



Le Risk manager contribue activement à la diffusion de l'appétence aux risques au sein de l'entreprise au travers des échanges qu'il mène avec les trois lignes de maîtrise dans le cadre de ses travaux (animation de la démarche de cartographie des risques, veille sur les risques émergents, analyse des risques de disruption, etc.) et dans les instances décisionnelles auxquelles il participe (comité projet, investissement, stratégique, etc.).

Le Risk manager anime des sessions de sensibilisation et de formation à la gestion des risques qui sont des vecteurs privilégiés de la diffusion de l'appétence aux risques. A cette occasion, le Risk manager apporte sa connaissance des situations à risque en se basant sur l'histoire de l'entreprise en matière de choix stratégiques, de prise de décisions et de gestion de crise ainsi que sur l'analyse des risques émergents.

Le Risk manager apporte les méthodes d'analyse des risques, est en appui de certaines d'entre elles et peut conduire des analyses indépendantes du management.

2.4 Suivi du respect du cadre fixé

Le respect des règles et limites fixées par l'environnement de contrôle est suivi dans le cadre du contrôle interne. Un premier niveau de contrôle est assuré par les fonctions opérationnelles de la première ligne et un deuxième niveau par les fonctions de la deuxième ligne. Dans certaines entreprises, les première et deuxième lignes partagent des tableaux de bord constitués des indicateurs de pilotage pertinents au regard des risques et suivent leur évolution par rapport aux limites fixées.

Différentes stratégies peuvent être envisagées en cas de dépassement significatif et durable des limites, et notamment :

- L'entreprise décide d'accepter le risque malgré le dépassement des limites car c'est un risque voulu et assumé. Les limites doivent alors être revues.
- Le seuil d'alerte est atteint, mais la capacité de risque n'est pas encore dépassée. Un arbitrage doit être pris afin de déterminer s'il faut accepter ce niveau de risque au regard de la stratégie de l'entreprise ou au contraire le traiter ou le transférer afin de revenir dans les limites fixées.
- La capacité de risque a été dépassée : l'entreprise ne peut pas supporter un tel niveau de risque. Une nouvelle stratégie compatible avec la capacité de risque de l'entreprise doit alors être définie.

2

Dans le cas de dépassement critique et durable, le Conseil d'administration est informé des dérives observées ou envisagées et des stratégies pour revenir au niveau de l'appétence aux risques définie.

L'audit interne assure une évaluation périodique de l'efficacité du contrôle interne.

2.5 Communiquer autour de l'appétence aux risques de l'entreprise

L'appétence aux risques est un engagement de l'entreprise. C'est notamment le cas lorsqu'une entreprise mentionne un objectif en matière d'accident du travail, de conformité ou d'environnement.

Les entreprises sont appelées par le régulateur ou leurs parties prenantes externes à communiquer de plus en plus d'informations sur les risques auxquels elles sont exposées et les moyens qu'elles mettent en œuvre pour les gérer. Ainsi, même si les entreprises en dehors des secteurs de la banque et de l'assurance n'ont pas à ce jour obligation de communiquer sur leur appétence aux risques, à terme, cela sera un moyen de renforcer la confiance que ses parties prenantes ont dans l'entreprise.

Chaque entreprise détermine le meilleur moyen de communiquer sur son appétence aux risques auprès de ses parties prenantes externes en tenant compte des contraintes de confidentialité dans un environnement concurrentiel.

Le Risk manager participe à l'élaboration de la stratégie de communication externe en matière de gestion des risques et il s'assure de la cohérence de cette communication avec la vigilance nécessaire à la communication sur certains sujets lié par exemple au secret des affaires.

Il suit la réalisation des engagements pris par l'entreprise dans ce cadre.

Quelques conseils pour débuter la réflexion sur l'appétence aux risques au sein de votre entreprise

Les exemples partagés ci-dessous illustrent des pratiques initiées par quelques entreprises pour débuter la réflexion sur l'appétence aux risques. Certaines seront plus ou moins pertinentes selon le contexte de votre entreprise. Elles peuvent aussi être combinées le cas échéant.

Exemple #1 : Analyse de l'historique des décisions

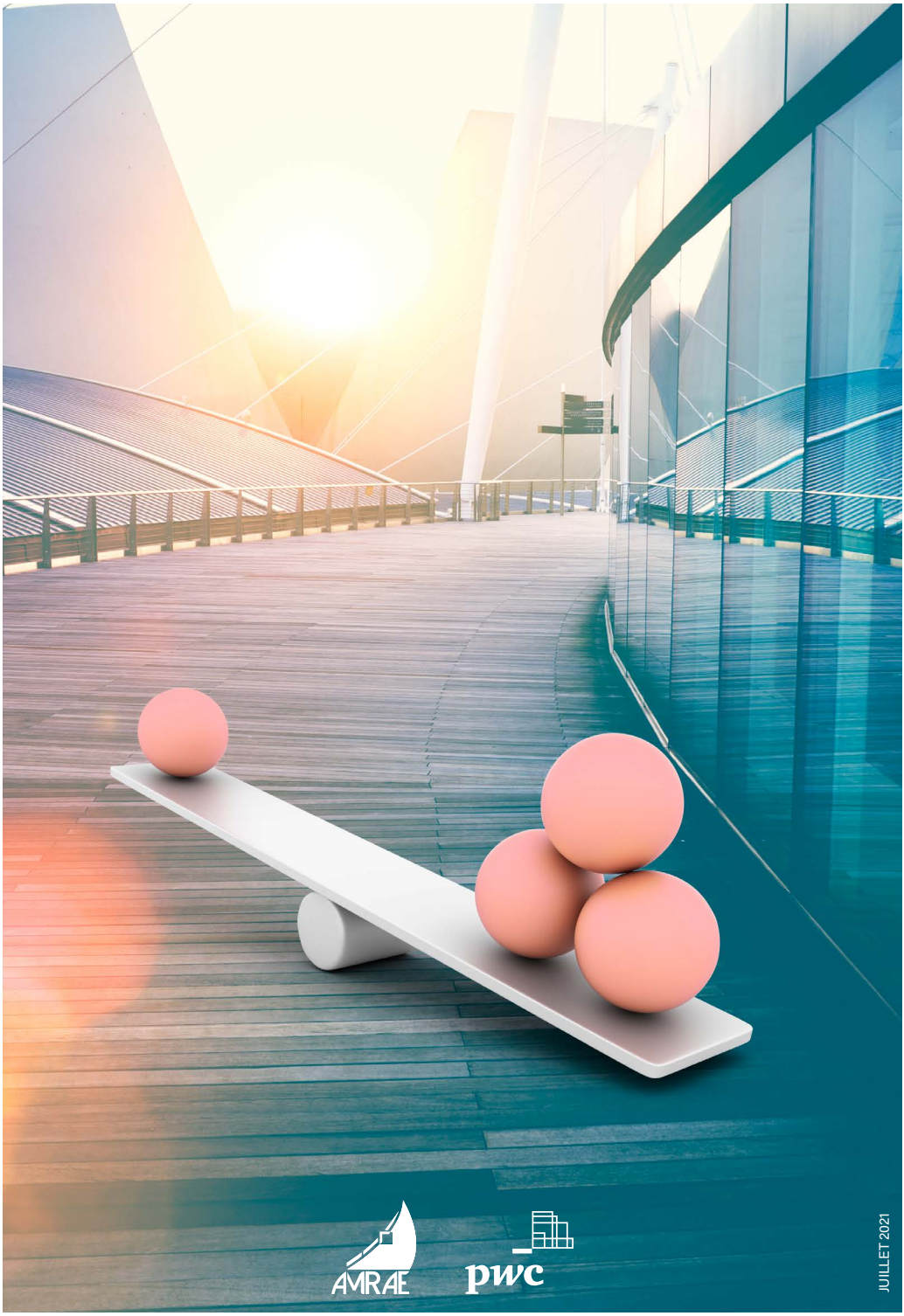
- Dresser une liste des prises de décisions importantes de l'entreprise sur les dernières années (exemples de documents source utilisés : comptes rendus de Comex / Conseil d'administration, communiqués de presse) ;
- Analyser l'évolution des cartographies dans les mises à jour postérieures à chacune de ces décisions ;
- Synthétiser les enseignements de l'analyse en matière d'appétence aux risques (idéalement en dégageant des spécificités par nature de risques) ;
- Sur ces bases, animer une ou plusieurs discussions avec le Conseil pour une réflexion commune sur la formulation de l'appétence aux risques (éventuellement par nature de risques).

Exemple #2 : Analyse de l'environnement de contrôle

- Répertorier les règles en vigueur en matière de délégations de pouvoir ainsi que les processus de décision (comités décisionnels) ;
- Faire une mise en regard avec les limites de risques (par exemple, les seuils retenus en matière d'exposition du personnel à des situations dangereuses par rapport aux seuils réglementaires), les seuils d'évaluation des risques et les seuils de déclenchement des cellules de crise ;
- En tirer les enseignements en matière d'appétence aux risques (idéalement en dégageant des spécificités par nature de risques) ;
- Sur ces bases, animer une ou plusieurs discussions avec le Conseil pour une réflexion commune sur la formulation de l'appétence aux risques (éventuellement par nature de risques).

Exemple #3 : Définition des risques non négociables ou inacceptables

- Analyser les prises de position internes et publiques de l'entreprise et de ses dirigeants sur les risques (ex : zéro tolérance à la corruption) ;
- Analyser l'expression et l'évaluation des risques dans les mises à jour de la cartographie et, le cas échéant, prendre en compte le niveau cible des risques ;
- Sur ces bases, proposer à la direction générale et au Conseil une liste de risques inacceptables, accompagnée de modalités spécifiques de suivi et d'action en cas de survenance.



AMRAE

pwc

JUILLET 2021