KPMG
毕马威

董事会工具箱之 -

公司治理之风险管理

公司治理之风险管理

风险管理的最终责任在于董事会。因此，风险管理是董事会和执行管理层关注的焦点。

本章节包括

- 关键概念
- 澳大利亚证券交易所《公司治理原则与建议》
- AS/NZS ISO 31000: 2018 风险管理原则与指南
- 风险与战略
- 风险治理
- 风险文化
- 风险管理政策
- 企业全面风险管理的裨益
- 风险偏好
- 危机管理
- 业务连续性
- 企业内部角色

公司董事自评问题清单

1. 与治理、风险和合规相关的角色和责任是否建立正式制度并形成文件?
2. 董事会是否对风险偏好有共同的看法，以便在决策中一以贯之地应用?
3. 鉴证活动是否基于适当、稳健的结构，并向企业的风险状况和偏好看齐?
4. 董事会成员是否清楚治理、风险和合规缺陷的潜在后果?
5. 在讨论中是否充分关注非财务风险和财务风险?
6. 是否有预警系统提醒董事会和高级管理层注意新兴风险?
7. 风险管理是否与战略方向和规划相结合且相协调?
8. 董事会是否了解管理层如何使用风险信息以及董事会确定的风险偏好来为决策提供信息?
9. 董事会如何识别和讨论错过的机遇或已发生的风险事件?
10. 董事会是否对危机管理和业务连续性计划进行监督?
11. 董事会是否奠定了“高层基调”，以促进风险意识文化?
12. 董事会是否对与公司相关的法律法规和《上市规则》有较好的了解?在此类法律法规发生修订后，董事会是否获悉?

警示信号

1. 董事会在讨论/文件中从未或很少提及公司章程。

2. 风险管理未与公司战略相关联。

3. 风险报告和风险管理计划在董事会层面未受到质疑。

4. 强大的风险文化未渗透至公司上下。

5. 未制定和传达风险偏好声明。

6. 董事会注意到风险问题，是通过媒体和利益相关方，而不是管理层。

7. 董事会无法清楚描述风险管理流程。

8. 审计和风险委员会未定期召开会议或向董事会报告。

9. 相较于非财务风险，过度关注财务风险。

10. 董事会层面讨论的风险（战略风险）、年度报告中报告的风险和管理层关注的运营风险之间存在脱节。

11. 风险管理被定位为幕后合规工作。

关键概念

风险是指“不确定性对目标的影响”。风险管理是指营造和制定适当的文化、流程和架构，在有效管理潜在机遇的同时管理潜在不利影响。

企业全面风险管理是指以经济高效的方式，在企业范围内识别、评估、沟通和管理风险，是一种综合的风险管理方法。风险治理应纳入必要的流程，将可靠的风险管理信息提请董事会关注。

高效的董事会考虑风险治理体系的稳健性，了解其工作原理及其在多大程度上能够为董事会提供保证。

ASX公司治理原则与建议

认识和管理风险是董事会和管理层的重要职能之一。如未能做好这一项工作，将对证券持有人和所有其他利益相关方产生不利影响。

《ASX原则》原则7建议企业建立健全风险管理框架，定期审查框架有效性[1]，并提出了以下建议：

- 建议7.1 — 上市公司董事会应设立一个或多个委员会来监测风险（既可以是独立的委员会，也可以与审计委员会合并）
- 建议7.2 — 董事会或董事会下属委员会应至少每年审查一次实体的风险管理框架，以确保框架的健全性；并在每个报告期披露是否进行了此类审查
- 建议7.3 — 上市公司应披露其是否设有内部审计职能、内部审计职能的组织结构及其扮演的角色；如未设立内部审计职能，应披露这一事实及其用于评估和持续改进风险管理和内部控制流程有效性的流程
- 建议7.4 — 上市公司应披露其是否存在任何重大环境或社会风险敞口；如存在，应披露目前或未来拟采用的应对方法。

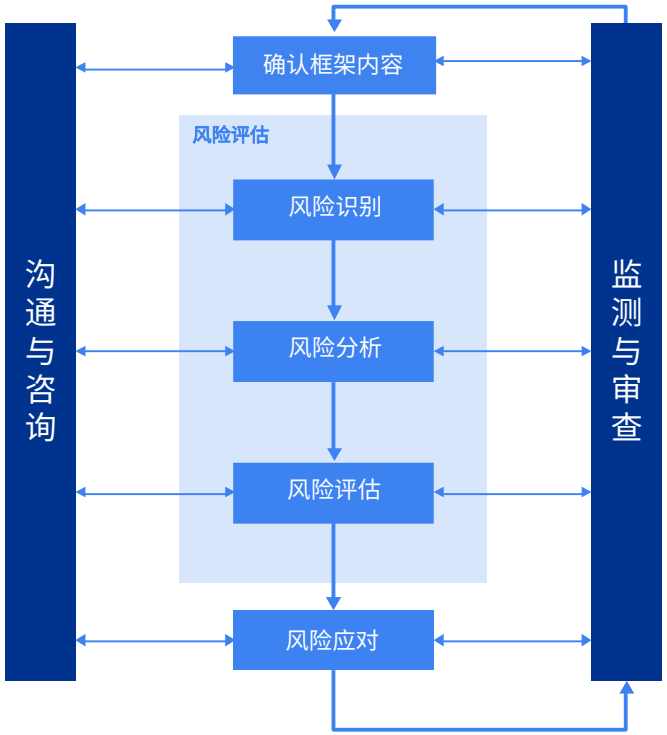
1.澳大利亚证券交易所公司治理委员会，《公司治理原则与建议》，2019年第4版，原则7。

AS/NZS ISO 31000:2018风险管理原则与指南

AS/NZS ISO 31000:2018（ISO 31000）规定了有效风险管理的原则，以及企业制定和实施全面风险管理框架应纳入的重要组成部分。ISO 31000标准是优秀的风险管理实践标准，广泛应用于澳大利亚私营和公共部门。ISO 31000: 2018的目标是协助各类组织制定企业全面风险管理战略，以有效识别和缓解风险，并实现组织的目标。为了实现这一目标，该标准确定了战略重点，并强调高级管理层的作用以及企业范围内的风险管理整合。有趣的是，ISO 31000将风险定义为“不确定性对目标的影响”，因此并不像传统风险管理那样纯粹关注风险的负面影响。这与该标准的战略重点一致：如果企业能够主动管理风险，风险实际上可能变成机遇（或有利因素）。

右图总结了ISO 31000中描述的风险管理方法。

ISO 31000中概述的原则与指南虽然不具有强制性，但被认为是高层次的最佳实践，有利于促进积极主动的风险管理。所有董事均应了解这些基本原则以及如何确保管理层有效落实。



风险与战略

风险和战略本质上是一枚硬币的正反面，战略的制定必须考虑影响战略实现的风险。尽管整合这两个关键流程大有裨益，但许多企业很难做到这一点，通常会在战略制定后识别战略面临的风险，而不是利用对风险环境的了解来为战略的制定提供信息，然后识别战略面临的风险。

经验表明，当企业将风险管理视为战略不可分割的一部分，在应对负面事件和不确定性方面将更具韧性。对重大业务风险的管理不善，被广泛认为是导致全球金融危机期间大量企业倒闭的关键因素之一。全球金融危机提供了有益的经验教训，上市公司应加以借鉴吸收，以改进风险管理以及面向利益相关方的风险披露。

风险治理

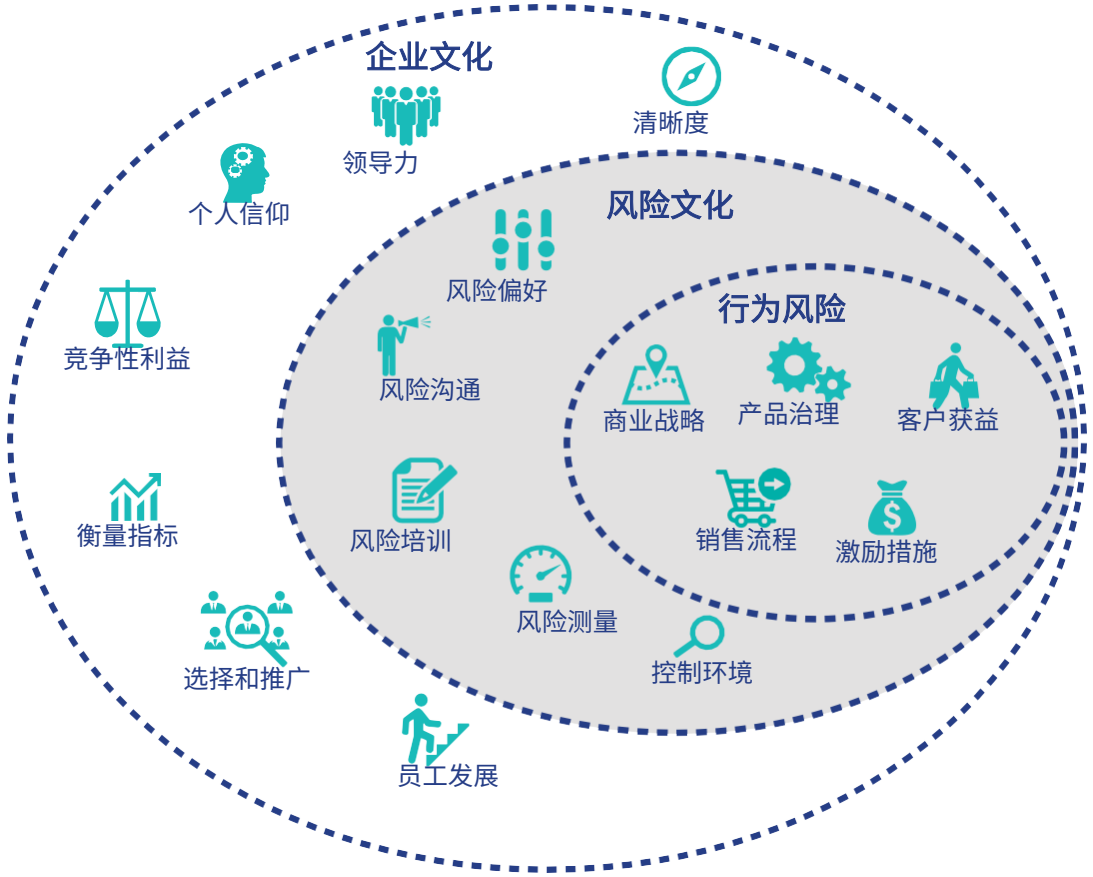
风险治理包括建立必要的流程和支持体系，将可靠的风险管理信息提请董事会关注。风险治理还包括总体风险管理结构，以促进企业范围内的风险管理，还包括针对关键风险领域、纪律方法和报告制定的正式政策程序。随着综合化的治理、风险和合规系统日益普及，且选择不断增加，澳大利亚开始以更快的速度采用风险管理技术。这为风险治理提供了有效的解决方案。

如今，许多审计委员会对企业风险管理流程及其面临的其他主要风险（包括财务、运营、网络安全、信息技术、法律和监管合规）负有监督责任，还有企业设立了单独的风险委员会，专门关注与风险识别和管理相关的监督事项。

风险文化

建立企业文化是董事会的责任，包括营造、传达和践行企业风险管理文化。

文化可能很难定义，但通常被理解成“企业的做事方式”。虽然企业可能有一套堪称最佳实践的政策和流程来管理关键风险领域，但如果员工不切实遵守的话，也无济于事。



澳大利亚证券和投资委员会（ASIC）等监管机构日益关注企业文化及其对商业行为对消费者信任和信心的影响[2]。 在风险管理方面，员工的行为可能快速影响财务绩效和企业声誉，因此至关重要。

风险管理的实施不仅需要付出巨大努力，还需要建立风险管理文化，确保企业致力于在董事会规定的范围内妥善管理风险。董事会负责奠定“高层基调”，而管理层则负责营造“中层情绪”。确保行为的一致性需要董事会采取积极主动的方法。为了建立企业范围内普遍认同的风险文化，关键行动包括：

- 向所有员工和利益相关方传达董事会的愿景、战略、政策、职责和工作汇报体系；
- 制定明确的风险偏好声明，就最终愿景和裨益进行沟通，并制定企业可以接受的决策阈值；
- 建立控制环境，分配风险管理责任，并辅以一致、有效的测量和问责框架；
- 实施风险管理培训计划（包括发现和培养“风险管理标兵”），建立知识分享体系；
- 宣传成功案例，并识别可以取得立竿见影效果的改进机遇。

风险管理政策

在澳大利亚成立的上市公司必须在董事会报告“业务经营和财务评估”部分纳入有关可能对实体未来财年前景产生不利影响的主要内外部风险源（包括环境和可持续发展风险）的讨论[3]。

如果发生重大风险事件，企业可能还必须根据《上市规则》规定的持续披露义务披露相关事件及其影响。

风险管理政策应反映公司的风险状况，并明确描述风险管理和内部审计职能的所有要素。 企业应借助政策内容，传达风险管理方法。相关政策应至少包括以下内容：

- 与企业相关的“风险”和“风险管理”定义；
- 风险管理目标和战略；
- 企业的风险偏好/承受能力；
- 风险管理目标测量方法；
- 风险管理责任。

企业全面风险管理的裨益

制定综合化的风险管理框架可以为企业带来以下裨益：

- 实现更明智的决策；
- 提升管理层共识；
- 加强管理层责任意识；
- 提高实现战略目标的能力；
- 减少收益波动；
- 更好地分配资源，继而提升盈利能力；
- 赋能企业将风险转化为竞争工具；
- 提升风险调整定价的准确度；
- 制定更优的应急计划；
- 改进危机响应能力。

企业风险管理框架的构成要素

风险战略与偏好	风险战略与偏好是指进行有意识的决策，利用风险管理助力业务计划、目标和战略目标的实现。包括一份风险偏好声明，并辅以风险承受能力、风险限额及相关违规行为章程，以控制企业范围内的风险水平。
风险治理	风险治理是指一种架构，企业借助这个架构来指导、管理和报告风险管理活动。包括明确界定的角色和责任、决策权、风险治理运营模式和工作汇报体系。
风险文化	风险文化是指企业范围内存在的影响风险决策的价值观和行为。风险文化影响着管理层和员工的决策，即使他们没有有意识地权衡风险和裨益。强大的风险文化有助于促进企业做出符合企业、股东和员工长期最佳利益的战略决策。
风险评估和测量	风险评估和测量是指企业为了识别、评估和量化已知和新兴风险而实施的活动。借助风险评估和测量流程，企业可以考虑潜在事件对目标实现的影响程度。包括企业为识别、评估和测量风险而开发实施的各类定性和定量方法、流程、工具和系统。
风险管理与监测	风险管理与监测是指管理层为管理、减轻风险而做出的响应。风险管理工作通过使用风险相关信息及风险管控信息来提高企业范围内的业务绩效，从而创造价值。结合既定指标对已识别的风险和管理活动进行系统监测，有助于企业在必要时及时主动响应。管理层负责设计相关活动，向利益相关方确保风险管控活动和措施在管理可能对目标实现产生影响的风险方面的有效性。
风险报告与洞察	报告风险和相关信息（如缓解活动）有助于企业真正了解风险管理活动的优劣势。向关键利益相关方披露风险管理信息，也有助于决策流程。有效的风险报告可及时提高可能影响目标实现的风险的透明度。
数据与技术	数据与技术是指管理风险数据，将其转化为对利益相关方有用的风险信息。包括开发和部署风险管理工具、软件、数据库、技术架构和系统，以支持风险管理活动。

风险偏好

风险偏好是指企业在追求价值的过程中，在广泛的层面上愿意接受的风险量，可以反映企业的风险管理理念和风险承担能力。风险偏好基于企业的战略目标和利益相关方的需求。在应对不确定和不断变化的风险环境时，风险偏好概念有助于企业采用重点突出的系统性方法。风险偏好声明可以为企业从战略和运营角度处理风险提供决策框架。由于企业不同部门可能有不同的风险偏好，且涉及到不同的风险类型，因此按领域和风险类型明确风险偏好至关重要。例如，企业对员工健康、安全和福祉相关风险的风险偏好普遍较低，但对创新相关风险的偏好较高（这有助于企业营造敢于冒险的创新文化）。这有助于企业针对每个领域制定控制框架并相应分配资源。

如果以适当的方式嵌入和使用，风险偏好有助于企业重新分配资源和降低成本。根据风险偏好设置关键风险指标，可以赋能企业监测和报告预警信号，实现积极主动的风险管理。

危机管理

企业应制定危机管理计划。此类计划应提及董事会在危机期间的作用，并应被视为董事会风险管理责任的一部分。董事会应坚持强调危机管理计划需要包含强有力的沟通元素。

如果没有有效的沟通，企业可能遭受额外的损害，包括：

- 失去对沟通流程的控制；
- 让谣言和猜测淹没真相；
- 声誉受损；
- 使员工士气和信任面临风险；
- 疏远股东、客户、供应商和其他利益相关方。

现代化风险管理框架（包括危机管理计划）应将缓解社交媒体风险作为一项关键元素。董事会和高级管理层需要做好随时应对社交媒体风险的准备。

业务连续性

由于所有企业均面临发生严重事件的风险，可能损害企业的持续运营能力，因此灾难规划不可或缺。

业务连续性管理的重点是对威胁企业持续运营能力的内外部危

机做出响应，目的是确保企业对可能严重影响企业的各类事件做好准备，并在事件发生后做出响应，恢复正常的业务运营。

业务连续性的最终目标是对事件做出响应，确保企业维持最关键的业务运营，并顺利度过运营中断风险。有效的业务连续性规划的关键要素是灵活简单。

准备充分的企业能够在正确的时间做出正确的决定，所依靠的不是手册中的僵硬指示，而是经过测试验证的替代工作方式。

业务连续性安排必须满足以下条件：

- 融入日常业务；
- 审视企业内外部风险；
- 为员工和利益相关方所理解；
- 定期进行测试，确保有效性。

企业内部角色

董事会

董事会对风险管理承担最终责任，并负责以下工作：

- 批准审计和风险委员会建议的风险偏好；
- 定期审查和批准企业风险管理政策，并对政策进行持续监督；
- 批准企业风险管理框架；
- 定期接收审计和风险委员会关于关键风险、风险变化和新兴风险的最新汇报；
- 设立董事会下属委员会（审计和风险委员会），并评估相关委员会的绩效。

首席风险官

对于企业而言，任命首席风险官或风险经理目前是常规操作。任命首席风险官有助于风险管理集中化，还可以带来其他几个好处，例如跨越部门了解以前可能不明显的不同风险之间的关系。这一点的重要性与日俱增，因为随着全球企业日益多元复杂，单个业务部门经理可以接受的风险从整个企业的角度来看可能是不合适的。通过使用全面的风险矩阵，首席风险官可以在企业范围内识别此类联系，并进行更有效的管理。

首席风险官使企业受益的另一个重要方式是，赋能企业在更好地了解风险与回报之间的关系，并在此基础上做出决策。

首席风险官可以通过以下方式发挥最大作用：帮助董事会对企业风险领域获得清晰的认识，协助制定风险分摊和抵消政策，并努力传达这一认识，以便管理者了解并提供支持。

首席风险官提供风险管理框架，而业务一线的管理者和员工负责就可接受的风险进行决策。

风险管理委员会

《ASX原则》建议，上市公司董事会应设立风险委员会来监测风险，风险管理委员会应至少每年一次审查公司风险管理框架（并披露是否进行了此类审查）[2]。 许多公司设立了风险管理委员会，或审计与风险联合委员会，作为有效的机制，确保公司建立适当的风险监督、风险管理和内部控制，提供监督公司风险管理框架所需的透明度、专注力和判断力。对于未设立风险管理委员会的公司（例如，董事会规模小，建立正式的委员会结构不一定能产生同样的效率），应通过董事会的工作程序提出正常情况下可能由风险管理委员会考虑的问题。

一般而言，风险管理委员会可以在风险和合规治理中发挥关键作用，包括：

- 监督风险管理框架及其执行情况；
- 审议风险报告并提出质疑；
- 监督合规框架；
- 审议管理层对关键风险问题采取的响应措施，并提供指导。

2. 澳大利亚证券交易所公司治理委员会，《公司治理原则与建议》，2019年 第4版，建议7.1和7.2。

参考文献

- 澳大利亚证券和投资委员会（ASIC），2016年，《良好的企业文化、价值观和职业道德》，http://asic.gov.au/about-asic/media-centre/speeches/good-corporate-culturevalues-and-ethics/
- ISO 31000: 2018 风险管理 — 指南
- 毕马威，2019年，《风险重塑》，https://assets.kpmg/content/dam/kpmg/au/pdf/2019/risk-recimaginge-seize-opportunity-in-risk.pdf

毕马威

Frank Mei
梅放
风险管理咨询
主管合伙人
毕马威中国
frank.mei@kpmg.com

Johnson Li
李斌
治理、风险与合规服务
内地主管合伙人
毕马威中国
johnson.li@kpmg.com

Lee Alva
李懿玲
治理、风险与合规服务
香港主管合伙人
毕马威中国
alva.lee@kpmg.com

Vera Li
李迪
治理、风险与合规服务
合伙人
毕马威中国
vd.li@kpmg.com

Kelvin Leung
梁安超
治理、风险与合规服务
合伙人
毕马威中国
kelvin.oc.leung@kpmg.com

May Gao
高原
治理、风险与合规服务
合伙人
毕马威中国
may.gao@kpmg.com

kpmg.com/cn/socialmedia