专 业 视 角
POINT OF VIEW

香港联交所新规解读：风险管理体系构建实务

敏于知

2024 年 12 月，香港联合交易所（“联交所”）刊发有关优化《企业管治守则》及相关《上市规则》条文检讨的咨询总结。为加强企业的风险管理和内部控制，本次修订明确了对风险管理和内部控制系统的年度检讨要求，并将检讨过程和结果的披露提升至强制性披露要求。这些要求不仅仅是合规层面的约束，更是企业实现稳健运营、可持续发展的关键所在。

联交所新规下，风险管理为何至关重要?

新的《企业管治守则》已于 2025 年 7 月 1 日生效，即有关新规将适用于 2025 年 7 月 1 日或之后开始的财政年度的企业管治报告和年报。根据新的《企业管治守则》披露报告公司合规情况时间表如下：

财政年度的结束日期	适用新《企业管治守则》的首份企业管治报告
12 月 31 日 /3 月 31 日	2026 年企业管治报告及年度报告（即从 2026 年 1 月 1 日 /2026 年 4 月 1 日开始的财政年度）
6 月 30 日 /9 月 30 日	2025 年企业管治报告及年度报告（即从 2025 年 7 月 1 日 /2025 年 10 月 1 日开始的财政年度）

protiviti 甫瀚

合规要点大剖析

在新版《企业管治守则》中，将年度检讨从建议升级为强制要求，且必须披露检讨流程、重大监控缺陷及补救措施；同时需在报告中提供佐证材料，证明风险管理及内部监控系统的适当性和有效性。

	新版强制披露要求内容总结	旧版要求
H	发行人根据守则条文第 D.2.1 条就其及其附属公司的风险管理及内部监控系统的有效性所作的检讨（至少每年一次）的详情，包括：	若发行人根据守则条文第 D.2.1 条，在《企业管治报告》内说明董事会已经作出有关风险管理及内部监控系统有效性的检讨，则必须披露：
(a)	董事会声明： - 董事会责任 - 发行人检讨结果	董事会责任： 不遵守就解释的守则条文 发行人检讨结果：强制披露
(b)	识别、评估及管理重大风险的流程以及信息披露的程序	不遵守就解释的守则条文
(c)	风险评估（包括 ESG 风险）以及风险管理及内控系统的任何重大变更；	新规新增要求
(d)	是否设有内部审核功能；	强制披露
(e)	内外部检讨风险管理及内部监控系统有效性的责任，以及有关检讨的流程及频次；	检讨频次以及所涵盖期间： 强制披露 检讨程序： 不遵守就解释的守则条文
(f)	佐证董事会认为风险管理及内部监控系统适当及有效的数据，包括：管理层、相关委员会以及内外部的确认	管理层的确认： 建议最佳常规
(g)	检讨范围及检讨结果的详情，包括重大缺陷及补救措施	不遵守就解释的守则条文

根据新的《企业管治守则》

董事会：

» 须对发行人的风险管理及内部监控承担最终责任。

» 应持续监察发行人的风险管理及内部监控系统，至少每年一次检讨系统的有效性。

发行人：

» 每个汇报期的企业管治报告中均应加载董事会声明，确认其对发行人风险管理及内部监控系统负责，并确认发行人风险管理及内部监控系统适当及有效。

管理层：

» 负责风险管理及内部监控系统的具体设计及实施，将当中相关角色、责任及权限适当授予公司的不同部门及员工（以及参与的外部顾问），确保其日常运作畅顺，定期向董事会提供相关数据，确认系统实施概况及成效。

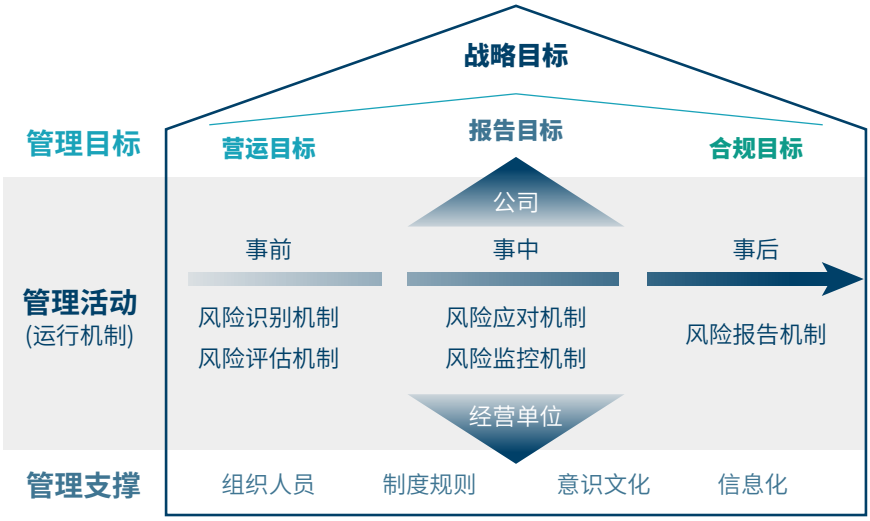
同时，2025 年 5 月联交所刊发了《董事会及董事企业管治指引》，就如何遵循《企业管治守则》提供了建议和示例，旨在支持董事会应用《企业管治守则》及透过提供建议、示例及进一步阐述引发董事会思考如何最有效地发挥其作用。

在《指引》中，联交所对上市公司风险管理体系的要求涵盖多个关键方面，从风险识别、评估到应对，形成了一套严谨的规范框架。公司须设定明确的目标，识别达标过程涉及的现有风险及新出现的风险，再厘定为了达标所愿意承担的风险水平。董事会可根据上述分析及公司的风险承受程度，与管理层一起建立并维持有效的风险管理系统。

构建实用风险管理体系

面对这一合规要求，一些企业的风险管理体系可能没有那么完善，或是刚上市的公司风险管理基础还比较薄弱，需要根据联交所的要求，设计并实施适用于本公司情况的风险管理体系。

风险管理体系图



一、设定目标

在风险管理工作的初始，并非立即开始PDCA[1]循环，也并非组织不同部门的员工、专家汇聚一堂，围绕市场、运营、财务、法律等领域头脑风暴，自由畅谈可能面临的风险。要了解所面对的风险，公司应先订立战略目标、营运目标、报告目标以及合规目标，再来探讨有哪些风险可能会影响和阻碍目标的达成。其中，战略目标是制定营运目标、报告目标以及合规目标的基础。

在订立目标后，未来的风险管理的主题，会紧紧围绕识别的目标开展，有的放矢，不做无用之功。

二、风险评估和管理

1 风险识别：火眼金睛识隐患

风险识别是风险管理的首要环节，如同医生诊断疾病，只有准确找出 “病因”，才能对症下药。在风险识别阶段，公司需根据订立的目标，全面、系统地梳理内外部风险因素，建立科学的风险识别机制，运用问卷调查、头脑风暴、管理层访谈、价值链分析、专家咨询等多种方法，确保不遗漏任何潜在风险，形成适用于公司的风险库。本次联交所特别提出了对 ESG 风险、网络安全风险和欺诈风险的识别。

1 Plan（计划）- Do（执行）- Check（检查）- Act（处理）

2 风险评估：精准度量风险值

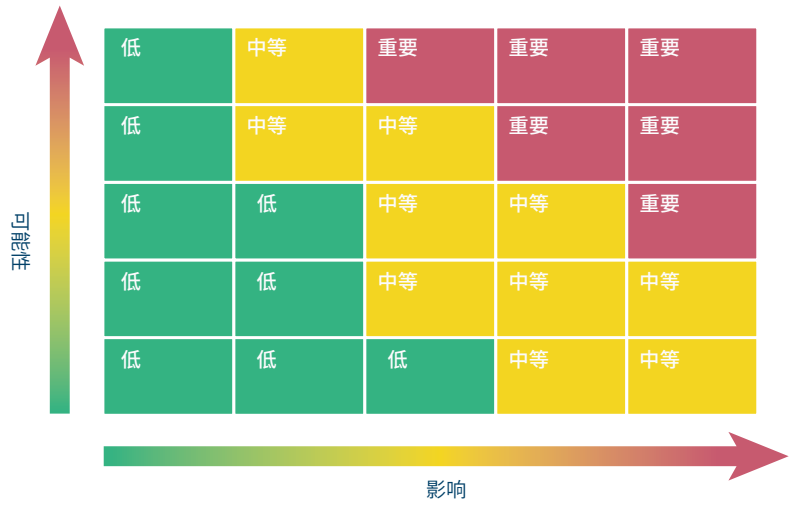
风险评估是对识别出的风险进行分析，确定其严重程度和优先级，为后续的风险应对提供科学依据，常用方法可分为定性评估和定量评估。

定性评估方法主要依靠专家经验和主观判断，比如管理层访谈、风险研讨会、问卷调差、标杆比较等，对风险发生的可能性和影响程度进行等级划分。

定量评估则借助数学模型和数据分析，使评估结果更具精确性。比如蒙特卡洛模拟则通过多次随机模拟，预测风险事件可能产生的各种结果及其概率分布。

联交所提出，公司可使用风险冷热图（如下图）评估已知风险对公司的影响，制成“冷热图”形式的矩阵，列出其面对的重大风险（可包括现有及潜在风险），并按发生的机率及对公司的影响程度来评级。

风险冷热图



来源：香港联交所《董事会及董事企业管治指引》

在风险评估环节，还应厘定公司为实现目标愿意承担的风险水平（风险容忍度）。风险容忍度的核心价值是将 “抽象的风险偏好” 转化为 “可操作的管理工具”。公司制定适合的风险容忍度，需要结合战略目标、风险偏好、业务特性、内外部环境等多重因素，是一个 “从宏观到微观、从定性到定量、从设计到落地” 的系统性过程。由于不同业务、不同风险类型的容忍度可能差异很大，公司不太能够“复制”别人的风险容忍度为己用，但可以从如下方面考量：

1) 回归目标。风险容忍度关注的是目标和绩效，而不是特定风险，需从企业的风险偏好和战略目标出发，明确 “为了实现什么目标，需要接受哪些具体风险”。

2) 识别关键风险领域。公司面临的风险类型包罗万象，无需对所有风险都设定容忍度，只需聚焦对战略目标有决定性影响的关键风险（如风险地图中影响程度大、发生可能性高的风险）

3) 设计具体指标。针对每个关键风险领域，结合风险偏好、财务模型、敏感性分析、压力测试、同行对标、监管要求等，设置“上下限”，将 “可接受的波动范围” 转化为具体指标。优先用定量指标，对难以量化的风险（如声誉风险）可用定性描述。如：

关键风险领域	定性描述 （示例）	定量指标 （示例）
现金流风险	确保日常运营不受影响	月度现金余额 ≥ 月度运营成本的 1.5 倍
供应链风险	不接受导致生产中断的供应问题	核心产品供应商交货延迟时长 ≤3 天
产品安全风险	零容忍重大安全事故	年度产品安全投诉次数 =0，抽检合格率 =100%

在该环节中，各相关部门应参与讨论和校正，确保提议的容忍度符合业务现实、可操作、且被理解，最终提交给高级管理层和董事会进行审议和批准，获得最高层的认可是执行的关键。同时还应考虑是否需要根据公司层级和业务性质，设置不同层次的容忍度。在执行前，应向相关人员（特别是承担风险责任的管理者和员工）进行充分的沟通和培训，确保他们理解其含义，以及超出容忍度可能带来的后果。

4) 嵌入决策流程与监控。将风险容忍度嵌入到战略规划、投资决策、预算制定、项目审批、合同评审、新产品开发等关键业务流程中。决策应评估是否在容忍度范围内。建立持续的风险监测和报告机制，定期将实际风险水平与设定的容忍度进行比较，生成风险报告。

5) 动态调整。风险容忍度不是一成不变的，需定期或在重大环境变化时（如行业政策调整、市场突变）重新评估。如若实际风险频繁突破容忍度，可能是指标过严，需结合能力提升调整。

3 风险应对：多管齐下巧化解

在风险应对方面，公司需根据风险评估结果，制定相应的应对策略，包括风险规避、降低、转移、接受和追求。对于高风险，企业应考虑采取风险规避措施，避免涉足可能带来巨大损失的业务领域；对于无法规避的风险，可以通过加强内部控制、优化业务流程等方式降低风险发生的可能性和影响程度；风险转移则是通过购买保险、签订合同等方式，将风险转移给第三方；对于一些风险较小、在企业承受范围内的风险，可以选择接受，企业可选择风险接受，但这并不意味着放任不管，仍需制定应急预案，确保在风险发生时能够迅速响应，将损失控制在最小范围内；对于通过主动承担更高风险以换取更优绩效的企业，应当明确边界，确保新增风险不超出企业为特定目标设定的容忍范围，且不违背整体风险偏好。

4 风险监控：动态追踪促长效

风险监控是一个持续的过程，公司应定期跟踪风险的变化情况。比如通过建立风险预警指标体系，设定关键风险指标的阈值，一旦指标超出阈值，立即发出预警信号。同时，定期对比风险指标与企业设定的风险容忍度，判断风险是否在可控范围内。公司还应定期对风险管理体系进行复盘，总结经验教训，针对发现的问题及时调整和完善风险管理策略与措施，确保风险管理体系的有效性和适应性。

5 风险报告：闭环呈现保合规

风险报告是风险管理全流程的收官环节，也是实现管理闭环的关键支撑。通过系统汇总风险识别、评估、应对及监控的全链条信息，风险报告需清晰呈现公司重大风险现状、应对措施落地成效、风险指标与容忍度的匹配情况，同时精准反映 ESG、网络安全、欺诈等重点领域的风险动态。报告需兼顾合规性与实用性，既满足联交所等监管机构的信息披露要求，又为管理层战略决策、流程优化提供数据支撑和行动建议。建立定期报告机制，确保报告内容的及时性、准确性和完整性，让风险管理成果可追溯、可复盘，推动风险管理体系持续迭代升级，为公司稳健运营筑牢防线。

落地实施与监督

风险管理体系的落地实施是一个系统工程，需要全体员工的共同参与和协作。公司应建立明确的风险管理机制和制定详细的实施计划，明确各部门在风险管理中的职责、分工和汇报机制，确保体系能够有效运行。可以设立风险管理委员会，负责统筹协调风险管理工作，定期召开会议，研究解决风险管理中遇到的重大问题。设立部门 / 职能牵头开展风险管理工作，以支持风险管理委员会统筹风险管理工作。各业务部门则应指定专人负责本部门的风险管理工作，及时收集、分析和报告风险信息，配合风险管理委员会制定和实施风险应对措施。

为了确保风险管理体系的有效运行，企业还需建立健全监督机制。内部审核职能部门应定期对风险管理体系的运行情况进行评估审阅，检查风险识别、评估和应对措施的执行情况，发现问题及时提出整改建议。通过建立监督机制，及时发现和纠正风险管理体系运行中的偏差，不断完善和优化风险管理体系，提高公司风险管理水平。

达于行

甫瀚咨询可提供的服务

甫瀚咨询可提供全面风险管理咨询服务，擅长根据企业规模和风险管理能力，打造既适用于企业当前情况又着眼于未来的风险管理体系。甫瀚根据企业的需要，协助众多企业从无到有建立风险管理体系，也就单独的领域提供专业服务，包括风险评估、专项风险治理、风险管理指标建设、风险信息化建设等。

关于甫瀚咨询

甫瀚咨询（上海）有限公司是一家具有全球视野的咨询机构。我们在中国开展业务至今已逾二十年，分别在上海、北京、深圳、成都和香港设有五个区域团队。依托甫瀚全球网络，我们能迅速汇聚甫瀚全球超过 25 个国家 90 个分支机构的资源与洞见，灵活调动更适合的专业团队为客户带来高质量的交付，并支持中国企业的海外拓展。

甫瀚咨询的业务遍及运营与财务管理绩效优化、风控与合规、内部审计、信息技术咨询、数字化转型，以及气候变化与可持续发展等领域。我们为中国各行业优秀企业、世界 500 强企业、全球各地资本市场的上市公司以及拟上市公司提供成熟及定制化的解决方案，亦为成长型企业提供陪伴式服务。

公司地址

北京
朝阳区建国门外大街 1 号
国贸写字楼 1 座 718 室
电话：(86.10) 8515 1233

上海
徐汇区虹桥路 1 号
港汇恒隆广场办公楼 1 座
2301+2310 室
电话：(86.21) 5153 6900

深圳
福田区中心四路 1 号
嘉里建设广场 1 座 1404 室
电话：(86.755) 2598 2086

成都
锦江区红星路三段 1 号
国际金融中心 1 号
办公楼 25 楼

香港
中环 干诺道中 41 号
盈置大厦 9 楼
电话：(852) 2238 0499

protiviti 甫瀚

关注甫瀚咨询
获取更多资讯