

企业风险管理调查问卷

ENTERPRISE RISK MANAGEMENT QUESTIONNAIRE

Universal Edition · All Industries · Management Tool

本问卷依据 ISO 31000:2018、COSO ERM 2017、ISO 22301（业务连续性）及国际一流企业风险管理实践设计，用于诊断治理成熟度、识别关键风险、校准风险偏好，并形成可执行改进清单。可直接作为董事会/风险委员会/内控的日常管理工具。

组织名称 Organization	_____	行业 Industry	_____
填表人 Prepared by	_____	职务 Title	_____
部门 Department	_____	日期 Date	___ / ___ / _____
审核人 Reviewed by	_____	版本 Version	Universal v1.0
覆盖范围 Scope	☐ 全集团 ☐ 事业部 ☐ 单实体 ☐ 项目		保密 Confidentiality ☐ 内部 ☐ 受限

填写指引 How to complete: 请据实选择最接近现状的选项；评分 1-5（1=几乎不/很弱，5=卓越/完全做到）。不确定请选「一般」并在备注说明。完成后请提交风险管理部门汇总，形成行动登记册。
评分图例 Scale: 1 Almost never / Weak · 2 Limited · 3 Adequate · 4 Strong · 5 Leading / Fully embedded

A 治理与风险文化 | Governance & Risk Culture

A1 董事会/最高管理层是否定期审议企业风险管理（ERM）政策与重大风险清单？

☐ 1 几乎不 ☐ 2 较少 ☐ 3 一般 ☐ 4 较好 ☐ 5 卓越

A2 是否明确风险偏好（Risk Appetite）与风险容忍度，并书面下发业务单元？

☐ 1 几乎不 ☐ 2 较少 ☐ 3 一般 ☐ 4 较好 ☐ 5 卓越

A3 三道防线（业务/风控合规/内审）职责是否清晰且有效协同？

☐ 1 几乎不 ☐ 2 较少 ☐ 3 一般 ☐ 4 较好 ☐ 5 卓越

A4 员工是否理解「风险人人有责」，并具备上报渠道且无打击报复？

☐ 1 几乎不 ☐ 2 较少 ☐ 3 一般 ☐ 4 较好 ☐ 5 卓越

A5 当前风险管理总体成熟度自评（COSO 视角）：

☐ 初始 ☐ 可重复 ☐ 已定义 ☐ 可管理 ☐ 优化

B 战略、目标与风险整合 | Strategy, Objectives & Risk Integration

B1 重大战略决策（并购、新市场、重大投资）是否强制开展风险评估？

☐ 1 几乎不 ☐ 2 较少 ☐ 3 一般 ☐ 4 较好 ☐ 5 卓越

B2 关键绩效指标（KPI）是否与风险指标（KRI）联动监控？

☐ 1 几乎不 ☐ 2 较少 ☐ 3 一般 ☐ 4 较好 ☐ 5 卓越

B3 是否识别战略假设失效情景（如需求骤降、监管突变、技术颠覆）？

☐ 1 几乎不 ☐ 2 较少 ☐ 3 一般 ☐ 4 较好 ☐ 5 卓越

B4 请列出本年度 Top 5 战略风险（名称即可）：

C 风险识别 | Risk Identification

C1 贵组织系统识别的风险类别覆盖情况（可多选）：

- ☐ 战略
- ☐ 运营
- ☐ 财务
- ☐ 合规法律
- ☐ 网络信息
- ☐ 供应链
- ☐ 人员/HSE
- ☐ 声誉/ESG

C2 是否建立并维护统一风险登记册（Risk Register），且责任人、控制措施齐全？

- ☐ 1 几乎不
- ☐ 2 较少
- ☐ 3 一般
- ☐ 4 较好
- ☐ 5 卓越

C3 是否结合内外部信息（审计发现、事故、监管通报、舆情）动态更新风险清单？

- ☐ 1 几乎不
- ☐ 2 较少
- ☐ 3 一般
- ☐ 4 较好
- ☐ 5 卓越

C4 新兴风险（Emerging Risks，如 AI、气候、地缘）是否有识别机制？

- ☐ 1 几乎不
- ☐ 2 较少
- ☐ 3 一般
- ☐ 4 较好
- ☐ 5 卓越

D 风险分析与评价 | Risk Analysis & Evaluation

请对贵组织当前最关键的一项风险，在矩阵中勾选对应单元格（可能性 × 影响）。也可复印本页用于多项风险。

关键风险名称：_____

影响 Impact →\可能性 Likelihood ↓	1 轻微	2 较小	3 中等	4 重大	5 极端
5 几乎确定	☐	☐	☐	☐	☐
4 很可能	☐	☐	☐	☐	☐
3 可能	☐	☐	☐	☐	☐
2 不太可能	☐	☐	☐	☐	☐
1 罕见	☐	☐	☐	☐	☐

D1 风险评估是否同时考虑固有风险与剩余风险（控制有效性后）？

☐ 1 几乎不 ☐ 2 较少 ☐ 3 一般 ☐ 4 较好 ☐ 5 卓越

D2 是否对重大风险开展情景分析/压力测试（乐观-基准-悲观）？

☐ 1 几乎不 ☐ 2 较少 ☐ 3 一般 ☐ 4 较好 ☐ 5 卓越

D3 定量与定性方法是否结合使用（财务损失、概率、专家判断）？

☐ 1 几乎不 ☐ 2 较少 ☐ 3 一般 ☐ 4 较好 ☐ 5 卓越

D4 评价后的风险处置优先级规则是否清晰（进入风险偏好红线必须上报）？

☐ 1 几乎不 ☐ 2 较少 ☐ 3 一般 ☐ 4 较好 ☐ 5 卓越

E 风险应对与控制 | Risk Treatment & Controls

E1 重大风险是否明确应对策略（可多选实际采用的）：

☐ 规避 ☐ 降低 ☐ 转移/保险 ☐ 接受 ☐ 共享

E2 关键控制是否有负责人、执行频率、证据留存要求？

☐ 1 几乎不 ☐ 2 较少 ☐ 3 一般 ☐ 4 较好 ☐ 5 卓越

E3 是否定期测试控制有效性（穿行测试/抽样），并对失效控制升级？

☐ 1 几乎不 ☐ 2 较少 ☐ 3 一般 ☐ 4 较好 ☐ 5 卓越

E4 保险与风险转移安排是否与风险画像匹配并定期复盘？

☐ 1 几乎不 ☐ 2 较少 ☐ 3 一般 ☐ 4 较好 ☐ 5 卓越

F 监测、报告与持续改进 | Monitoring, Reporting & Improvement

F1 是否有定期风险报告报送董事会/风险委员会（至少季度）？

☐ 1 几乎不 ☐ 2 较少 ☐ 3 一般 ☐ 4 较好 ☐ 5 卓越

F2 关键风险指标（KRI）是否设预警阈值并触发行动？

☐ 1 几乎不 ☐ 2 较少 ☐ 3 一般 ☐ 4 较好 ☐ 5 卓越

F3 事件/近失事件 (Near miss) 是否记录、根因分析并闭环?

☐ 1 几乎不 ☐ 2 较少 ☐ 3 一般 ☐ 4 较好 ☐ 5 卓越

F4 内外部审计发现是否纳入风险登记册并跟踪整改?

☐ 1 几乎不 ☐ 2 较少 ☐ 3 一般 ☐ 4 较好 ☐ 5 卓越

G 关键风险域快评（通用） | Key Risk Domains — Quick Scan

请对下列领域成熟度打分（1-5）。不适用请勾选 N/A。

G1	合规与监管 Compliance & Regulatory				
☐ 1	☐ 2	☐ 3	☐ 4	☐ 5	☐ N/A
G2	财务与流动性 Financial & Liquidity				
☐ 1	☐ 2	☐ 3	☐ 4	☐ 5	☐ N/A
G3	运营与流程 Operational Processes				
☐ 1	☐ 2	☐ 3	☐ 4	☐ 5	☐ N/A
G4	网络安全与数据 Cybersecurity & Data				
☐ 1	☐ 2	☐ 3	☐ 4	☐ 5	☐ N/A
G5	供应链与第三方 Supply Chain / Third Party				
☐ 1	☐ 2	☐ 3	☐ 4	☐ 5	☐ N/A
G6	人员、健康安全 HSE & People				
☐ 1	☐ 2	☐ 3	☐ 4	☐ 5	☐ N/A
G7	业务连续性与危机 BCM / Crisis				
☐ 1	☐ 2	☐ 3	☐ 4	☐ 5	☐ N/A
G8	ESG / 气候与声誉 ESG, Climate & Reputation				
☐ 1	☐ 2	☐ 3	☐ 4	☐ 5	☐ N/A
G9	欺诈与腐败 Fraud & Corruption				
☐ 1	☐ 2	☐ 3	☐ 4	☐ 5	☐ N/A
G10	技术与数字化转型 Technology & Digital				
☐ 1	☐ 2	☐ 3	☐ 4	☐ 5	☐ N/A

H 日常风险管理工具化 | Daily Risk Management as a Tool

H1	一线管理者是否将风险检查嵌入周会/班前会？				
☐ 1 几乎不	☐ 2 较少	☐ 3 一般	☐ 4 较好	☐ 5 卓越	
H2	是否有简明「风险一页纸」供管理层决策使用？				
☐ 1 几乎不	☐ 2 较少	☐ 3 一般	☐ 4 较好	☐ 5 卓越	
H3	跨部门风险升级路径是否在 24 - 72 小时内可闭环？				
☐ 1 几乎不	☐ 2 较少	☐ 3 一般	☐ 4 较好	☐ 5 卓越	
H4	本问卷计划复评频率：				
☐ 月度	☐ 季度	☐ 半年度	☐ 年度	☐ 重大变更时	

I 改进行动登记册（本轮必填） | Improvement Action Register

请根据前述低分项（≤2）或矩阵红区风险，列出至少 3 项可执行改进。完成后由风险管理部门跟踪。

No.	风险议题 / 缺口	优先级	责任人	截止日期	状态
1		H / M / L			☐ Open ☐ Done
2		H / M / L			☐ Open ☐ Done
3		H / M / L			☐ Open ☐ Done
4		H / M / L			☐ Open ☐ Done
5		H / M / L			☐ Open ☐ Done
6		H / M / L			☐ Open ☐ Done
7		H / M / L			☐ Open ☐ Done
8		H / M / L			☐ Open ☐ Done

J 声明与签核 | Declaration & Sign-off

本人确认以上信息基于所知如实填写，可作为本组织风险管理诊断与改进依据。本文件属内部管理工具，不含对外保证或审计意见。

填表人签字	部门负责人	风险管理负责人
日期 _____	日期 _____	日期 _____

Document Control: ERM-QS-UNIVERSAL-2026 | Framework alignment: ISO 31000 / COSO ERM / ISO 22301 | Issued for management use | Next review: annual or upon material change