

第 52 讲-风险概念，风险类型，资本充足率

第四章 风险管理

授课顺序及分值分布

章名	权重分值
第一章 财务报表分析	20%
第三章 决策分析	25%
第五章 投资决策	10%
第二章 公司财务	20%
第四章 风险管理	10%
第六章 职业道德	15%

章节框架

- 风险管理
- 企业风险管理

主要考点

- 风险管理
- 风险概念、风险类型、资本充足率
- **风险管理、风险应对方法**
- 企业风险管理（ERM）
- **COSO 框架五大相关部分**
- 风险管理优点

第一节 风险管理

思维拓展：如果企业是一部车



风险和预期损失

- 在商业环境下，将风险定义为可能遭受损失的程度；它可能会阻止组织实现其目标。
- 组织需要管理风险，以保护资产、避免非预期损失等。

风险价值 Value at risk, VaR

- 风险价值(Value at risk, VaR)：在一个既定的置信区间(可确定的概率)或一个确定的时间段内，我们预期可能会发生的最大损失。

- 风险收益(Earnings at Risk) : 在一个既定的置信区间内，企业收益的极端负值。
- 风险现金流(Cash flow at risk): 在一个确定时间段内，在既定的置信区间里，对一家企业或事业部相对于其目标现金流的变化进行预测。

风险价值计算方法

- 历史模拟法
- 方差 - 协方差法
- 蒙特卡罗模拟

历史模拟法

- 历史模拟法假设过去发生过的风险会重演。
- 历史模拟法是基于一定时期内实际历史收益数据，通过将其由低到高进行排序，以此来评估风险。

方差 - 协方差法

- 方差-协方差法假设风险概率分布符合正态分布。
- 估算期望收益和标准差，并画出正态分布曲线，利用其函数关系来寻找最差情况的百分比。

蒙特卡罗模拟

- 蒙特卡罗模拟法是指任何随机进行试验的方法。
- 该方法包括针对未来收益建模，以及多重假设试验。

风险类型

- 战略风险 Strategic risk
- 运营风险 Operational risks
- 财务风险 Financial risks
- 灾害风险 Hazard risk

战略风险

- 战略风险通常是外部的、宏观的、指向未来的。
- 包括与战略、政治、经济、法规和全球市场条件相关的风险。
- 还包括美誉风险、领导风险、品牌风险和变化的顾客需求。

运营风险

- 运营风险通常是公司内部的、当前的
- 与业务职能部门和内部管理流程体系有关
- 包括财务部和财务管理系统

财务风险

- 财务风险通常指公司的融资风险
- 可能来自于外汇、利率和大宗商品价格波动所产生的风险；还包括信贷风险、流动性风险和市场风险。
- 注意：财务部门相关风险属于运营风险，不属于财务风险

灾害风险

- 灾害风险通常与自然灾害有关
- 灾害风险通常是可以被保险的
- 灾害风险三项环境测试：
 - ① 必须产生财务影响
 - ② 不必然会出现
 - ③ 必须是负面结果

资本充足率 Capital adequacy ratio

- 资本充足率用于测量金融机构偿付能力、流动性、储备和充足资本等方面的风险指标。
- 2010 年制定的《巴塞尔协议 III》(the Third Basel Accord, Basel III) 给商业银行规定了最低的资本充足率，即确定需要维持多少的资本水平才能使商业银行承担由现有风险所造成的损失，并且达到可接受的偿债能力水平，它旨在抑制风险资产的过度膨胀，保护存款人与债权人的利益。
- 资本充足率 = 一级资本 + 二级资本 风险加权资产 / 一级资本 + 二级资本 一级资本 + 二级资本 风险加权资产
- 一级资本：无须终止业务，用来吸收损失的资本
- 二级资本：业务清算时候，用来吸收损失的资本

- 风险加权资产：针对每项资产进行风险评估，计算加权平均值

第 53 讲-风险管理流程

第一节 风险管理

风险管理流程

- 风险识别
- 风险评估
- 风险应对
- 风险沟通与监督

风险识别 Risk identification

- 风险识别：需要通过有计划且细致的方法在运营的各个方面来查找潜在的风险，并确认那些重要的风险领域。
- 目的：列示出全部风险，然后给予评估，将风险范围缩小至组织所面临重大风险。

风险识别技术

1. 内部访谈与讨论

包括：访谈、问卷调查、头脑风暴、自我评估及其他协调讨论和 SWOT 分析。

2. 外部来源 (external sources)

包括：与其他组织比较、与同行讨论、标杆管理和风险顾问。

3. 工具、诊断和流程

包括：对照表、流程图、情景分析、价值链分析、业务流程分析、系统工程和流程绘制。

风险评估 Risk assessment

- 风险评估：分析已识别风险潜在影响的过程，并根据以下两大关键要素，进行风险排序，并识别出对企业影响最大的风险。

① 风险可能性：风险发生概率

② 影响程度：一旦发生风险，会产生怎样的影响

$$\text{● 风险} = \text{概率} \times \text{影响程度}$$

风险评估 计算

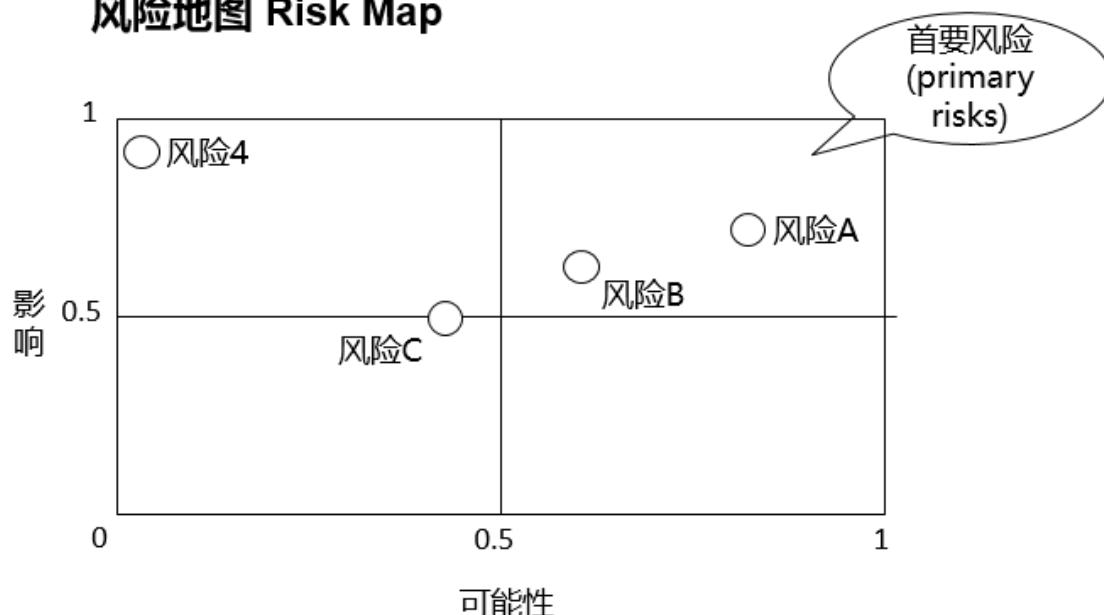
某公司预期有 70% 可能遭遇 \$1,000,000 的损失，有 30% 可能遭遇 \$500,000 的损失，则其预期风险损失为？

$$\text{预期风险损失} = 70\% \times \$1,000,000 + 30\% \times \$500,000 = \$850,000.$$

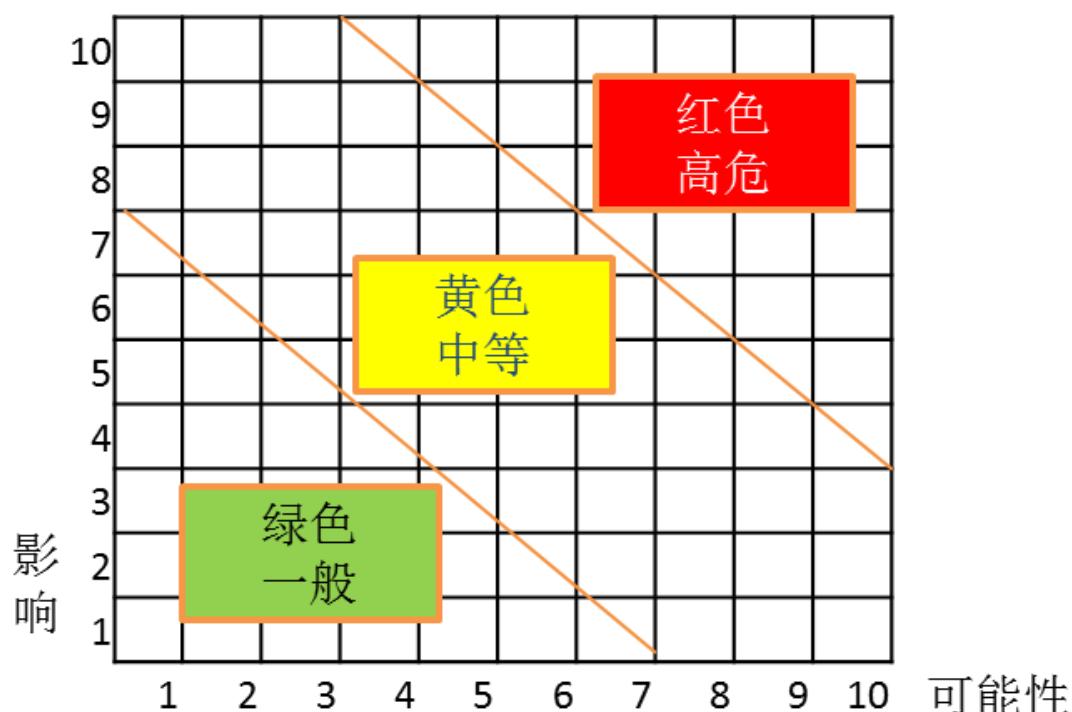
风险分值表（排序）

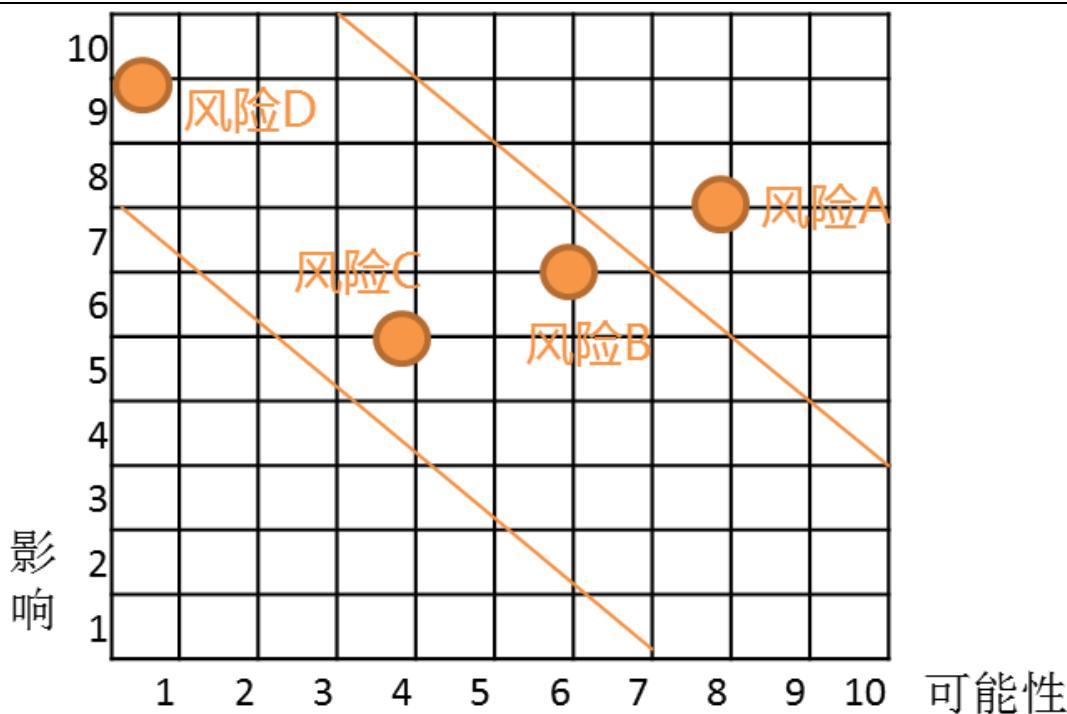
	影响程度	发生概率	风险值	排序
风险 A	0.7	0.8	0.56	1
风险 B	0.6	0.6	0.36	2
风险 C	0.5	0.4	0.2	3
风险 D	0.9	0.05	0.045	4

风险地图 Risk Map

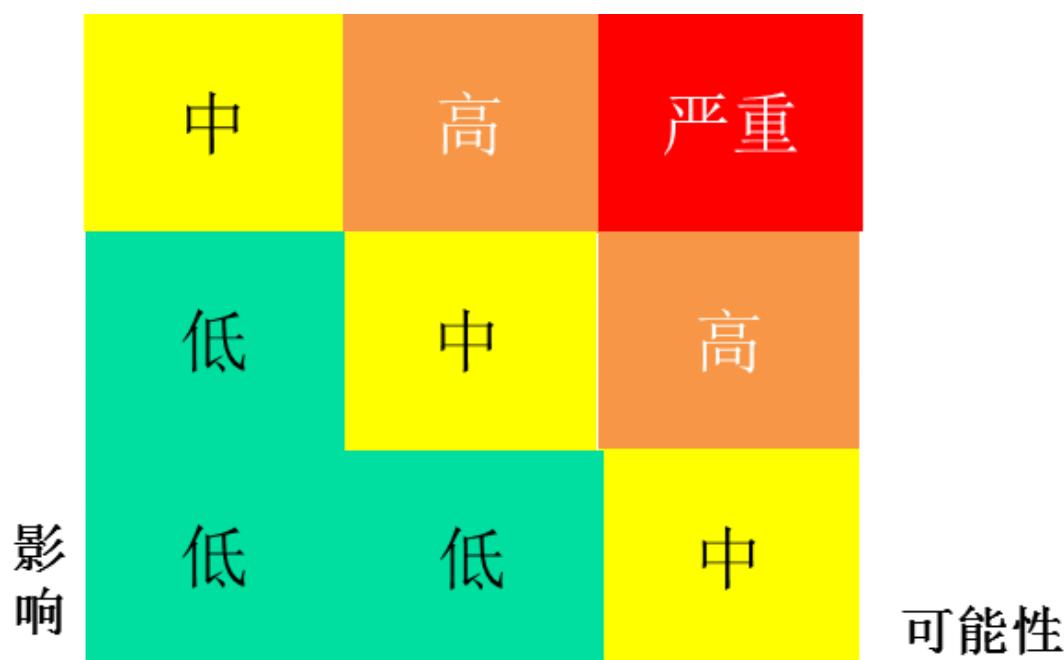


详细风险地图





热力图



风险评估 Risk assessment

- 固有风险 (Inherent risk): 在管理层没有采取任何措施来改变风险的可能性或影响的情况下，一个主体所面临的风险。
- 剩余风险 (Residual risk): 在管理层采取了风险应对措施之后所残余的风险。
- 风险偏好 (risk appetite): 在现有使命和业务模式下，组织愿意接受的风险水平
- 组织的风险偏好决定了管理层将如何管理风险。
- 风险容量: 组织可承受的风险幅度。

风险应对 Risk Response

- 回避 (avoidance)
- 降低 (reduction)
- 分担 (sharing)

- 承受(acceptance)

风险回避 Avoidance

- 企业退出会产生风险的活动。
- 触发条件：剩余风险 > 风险容量

风险降低 Reduction

- 企业采取措施来降低风险的可能性或影响，或者同时降低两者
- 触发条件：固有风险 > 风险容量
- 目标：剩余风险 < 风险容量

风险分担 Sharing

- 分担风险的实质就是转移风险，即通过合约的方式将风险转嫁给另一个机构；以此降低整体风险。
- 常见的技术包括购买保险产品、从事避险交易或外包一项业务活动。
- 触发条件：固有风险 > 风险容量
- 目标：剩余风险 < 风险容量

风险承受 Acceptance

- 企业不采取任何措施去干预风险，而是利用风险获得利益，也称为风险自留
- 触发条件：固有风险 < 风险容量

风险沟通与监督

- 与风险相关的沟通必须在组织内部全方位展开。
- 在一个管理良好的组织中，应使绩效和风险指标的监督工作常态化。

例题

财务主管 Wang 发现，公司新的财务管理系中，存在审批权限错位风险。根据 IMA 的《企业风险管理：框架、要素及其整合》，该主管发现的是什么风险（ ）。

- A. 财务风险
- B. 危害风险
- C. 运营风险
- D. 战略风险

【答案】C

【解析】题干信息属于公司内部业务职能（财务职能）系统运营的风险，属于运营风险。

注意：虽然是财务系统的风险，但不是财务风险。财务风险主要来自于外汇、利率和大宗商品价格波动所产生的风险；还包括信贷风险、流动性风险和市场风险。

例题

ABC 公司正在评估全球化战略，计划将生产迁移至越南。在经过风险评估之后，发现转移生产所产生的风险大于 ABC 公司可能承受的风险，以下各项都是 ABC 公司可能会采取的做法，除了（ ）。

- A. 回避风险
- B. 分担风险
- C. 承受风险
- D. 降低风险

【答案】C

【解析】由于转移生产所产生的风险大于 ABC 公司可能承受的风险，所以 ABC 公司不可能承受风险；而 ABC 公司有可能采取 回避风险、分担风险和降低风险的应对措施。

第 54 讲-企业风险管理

第二节 企业风险管理

企业风险管理 Enterprise risk management

- 企业风险管理（ERM）是对企业所面临的所有综合风险的分析和管理。
- 企业面临的风险包括：财务风险、营运风险、合规风险等。

企业风险管理的目标（IMA 管理会计公告）

- 通过管理对影响组织目标实现的不确定性，借此创造、保护和增加股东价值。
- 更加强有力的内部控制、更加行之有效的公司治理和 ERM 实施，能提升组织的稳定性和反应速度，增加股东价值。
- 从整体利全局的视角来看待组织面临的风险。

COSO 企业风险管理框架

- 企业风险管理是企业用来识别和管理风险，以及用适当措施应对风险的过程。
- 企业风险管理是涉及整个组织的、持续的、动态的过程。

企业风险管理的价值

- 价值创造：收益 > 成本
- 价值保持：收益 = 成本
- 价值实现：利益相关者获利
- 价值侵蚀：战略未达到预期

使命与愿景

- 使命和愿景协助组织构建边界，关注决策如何影响战略。
- 组织在充分理解自己的使命和愿景之后，其设定的战略能够形成一个理想的风险特征。
- 企业风险管理能协助组织避免战略错配。
- 企业需要评估所选的战略将如何影响组织的风险特征，特别是企业可能受到影响的风险的类型和数量。

风险和绩效

- 风险管理要求管理层去考察风险的类型、严重度和关联性，及其这些风险相对于战略和业务目标如何对绩效产生影响。
- 企业可以利用他们的风险特征来更好地理解风险、目标绩效和实际绩效之间的内在关联性。

企业风险管理的充分整合

- 在进行决策时，管理者和董事会必须持续地设身于动态的商业环境之中；这要求在任何时刻都把企业风险管理的思维整合到组织的各个方面。
- 需要将文化、实践和能力整合在一起并应用在整个企业的范围内，以此促使企业风险管理的充分整合。

第 55 讲-coso 框架五大相关部分（1）

第二节 企业风险管理

COSO ERM 五大关联部分

- ① 治理与文化
- ② 战略与目标设定
- ③ 绩效
- ④ 审阅与修正
- ⑤ 信息、沟通与报告

治理与文化

- 公司治理影响企业风险管理监督权责的建立和执行。
- 文化关系到组织内的价值观、预期行为和对风险的理解
- 公司应实施董事会风险监督，风险监管首要责任是对利益相关者的信托责任

治理与文化

原则	说明
实施董事会风险监督	风险监管首要责任： 即 对利益相关者的 信托责任
构建 运营结构; 设置 报告路径	界定责任、实施业务目标
界定理想文化	体现组织文化的理想行为 (风险规避与风险激进)
致力于核心文化	遵守核心价值与理想文化
吸引、培养和留住人才	人力资本的构建

治理与文化

对于风险规避与风险激进企业可能的影响		
例子	风险规避的企业	风险激进的企业
战略和业务目标的范围	采用保守的政策	采用激进的政策
应用在风险识别和评估中的严谨度	将潜在事件视为风险	将潜在事件视为机会
选择风险应对方式和分配资源	将更多的资源分配给增量风险，以此作为有利的风险应对措施	将更多的资源分配给增量风险，以此作为不利的风险应对措施
绩效评审	快速应对查实的绩效偏差	延迟应对查实的绩效偏差

战略与目标设定

- 组织进行未来规划时，必须结合企业风险管理、 总体战略和组织目标。
- 组织必须确定他们的风险偏好，同时风险偏好必须与组织战略保持一致。
- 目标可以帮助组织实现其战略和管理风险。

原则	说明
分析商业环境	外部环境：PESTEL 内部环境：四要素
定义风险偏好	风险偏好相关因素
评估风险不同的战略选项	识别潜在风险与机会： 风险偏好与战略目标一致 保持中立
制定业务目标	设定业务目标时，需要考虑到风险； 通过 业绩容忍度，了解风险是否可以接受

PESTEL 模型

外部环境要素	
类别	特征
政治 P	政府干预和影响的性质和范围，包括税收政策、劳工法规、环境法规、贸易限制、关税和政治稳定性
经济 E	利率、通胀、汇率、信贷可用性、GDP增长
社会 S	消费者的需求或预期；人口统计，比如人口分布、教育程度、财富分布
技术 T	研发活动、自动化和技术激励；技术变化或中断的速率
环境 E	自然或人为造成的灾害，持续的气候变化，能源消耗法规的变化，对待环境的态度
法律 L	法律（比如：就业、消费者、健康与安全），监管，和/或法律行业标准

内部环境要素

内部环境要素	
类别	特征
资本	现金、设备、不动产、专利
技术	新技术、调整的计算和/或采用的技术
人员	知识、技能、态度、关系、价值观和文化
流程	活动、政策或流程、管理、经营和支持流动的调整

第 56 讲-coso 框架五大相关部分（2），风险应对方法，风险管理优点

第二节 企业风险管理

风险偏好的相关因素

参数	说明
战略参数	新产品决策、资本投资、兼并与合并
财务参数	最大可接受的财务业绩的波动、资产回报率、风险调整资本回报率、目标债务评级、目标负债权益比
经营参数	环境要求、安全目标、品质目标、顾客集中度
风险特征	风险数量和分布、企业风险的不同类型
风险容量	最多能够承受的风险数量

绩效



- 针对可能影响到战略和目标的风险，组织必须予以识别和规划应对措施。
- 组织必须建立一个流程，向关键利益相关者报告组织风险状况

相关执行原则

原则	说明
识别风险	识别新的、正在出现的和变异的风险；风险清单；识别方法
评估风险的严重程度	影响和可能性；风险属性
风险排序	适应性，复杂性，速度，持续性，恢复
风险应对措施	回避、降低、分担、承受
开发风险组合视角	类别、严重度和风险之间的关联性

识别风险

- 新的、正在出现的和变异的风险，包括：
- 由业务目标变化所生产的风险
 - 由商业环境变化所产生的风险
 - 在此之前，企业尚未涉及该商业环境
 - 之前未知的风险
 - 之前已识别的风险，但这些风险已随着商业环境、风险偏好或支持假设的变化而变化

评估风险的严重度

- 影响：风险的结果或影响。
- 可能性：风险发生的机率。
- 管理层需要将风险的可能性与影响结合在一起考虑。

风险类型

- 固有风险：在管理层没有采取任何直接或集中行动来改变风险严重度时，企业有的风险。
- 目标剩余风险：在了解了管理层将要或已经采取了直接或集中行动来改变风险的严重度之后，企业在实施战略和业务目标时，所愿意承担的风险数量。（主观意愿）
- 实际剩余风险：在管理层已经采取了调整风险严重度的措施之后，依然剩下的风险。（客观实际）
- 实际剩余风险 \leq 目标剩余风险。
- 实际剩余风险 $>$ 目标风险：需要采取额外的行动调整风险的严重度。

风险排序需考虑的要素

- 风险适应能力
- 风险复杂程度
- 风险影响速度
- 风险持续性
- 风险恢复性

风险应对 Risk Response

- 回避（avoidance）
- 降低（reduction）
- 分担（sharing）
- 承受（acceptance）

影响风险应对措施选择的因素

- 商业环境
- 责任与预期
- 成本与收益
- 风险排序

- 风险偏好
- 风险严重度

审阅与修正

- 企业风险管理是一个更新和迭代的过程。
- 不断审阅和修订企业风险管理的内容，可以帮助组织更好的管理业务中不断变化的风险环境。

信息、沟通与报告

- 企业风险管理的关键能力，就是快速、准确、确定地沟通风险相关信息。
- 这种沟通必须在组织内外的各方之间进行。

COSO ERM 的优点

- 增加机会的范围。通过考虑所有的可能性，管理层可以识别与当前机会相关的新机会和独特的挑战。
- 在整个实体范围内识别和管理风险。
- 增加积极结果和优势，同时减少负面意外。
- 降低绩效波动性，实现损失最小化和机会最大化。
- 增强企业韧性。
- 改进资源部署，优化配置。

例题

企业风险管理是企业用来识别和管理风险，以及应对风险的过程。这是一个涉及整个组织的持续动态的过程。COSO 企业风险管理框架提出五个关联组成部分，以下不属于这五大部分的是（ ）。

- A. 公司治理与文化
- B. 战略和目标设定
- C. 控制环境
- D. 信息、沟通和报告

【答案】C

【解析】COSO 企业风险管理框架提出五个关联组成部分，包括：

治理与文化，战略与目标设定，绩效，审阅与修正，信息、沟通与报告。

第 57 讲-第四章风险管理复习

第四章 风险管理复习

授课顺序及分值分布

章名	权重分值
第一章 财务报表分析	20%
第三章 决策分析	25%
第五章 投资决策	10%
第二章 公司财务	20%
第四章 风险管理	10%
第六章 职业道德	15%

章节框架

- 风险管理
- 企业风险管理

风险和预期损失

- 在商业环境下，将风险定义为可能遭受损失的程度；它可能会阻止组织实现其目标。
- 组织需要管理风险，以保护资产、避免非预期损失等。

风险价值 Value at risk, VaR

- 风险价值(Value at risk, VaR)：在一个既定的置信区间(可确定的概率)或一个确定的时间段内，我们预期可能会发生最大损失。
- 风险收益(Earnings at Risk)：在一个既定的置信区间内，企业收益的极端负值。
- 风险现金流(Cash flow at risk)：在一个确定时间段内，在既定的置信区间里，对一家企业或事业部相对于其目标现金流的变化进行预测。

风险价值计算方法

- 历史模拟法
- 方差 - 协方差法
- 蒙特卡罗模拟

风险类型

- 战略风险 Strategic risk
- 运营风险 Operational risks
- 财务风险 Financial risks
- 灾害风险 Hazard risk

战略风险

- 战略风险通常是外部的、宏观的、指向未来的。
- 包括与战略、政治、经济、法规和全球市场条件相关的风险。
- 还包括美誉风险、领导风险、品牌风险和变化的顾客需求。

运营风险

- 运营风险通常是公司内部的、当前的
- 与业务职能部门和内部管理流程体系有关
- 包括财务部和财务管理

财务风险

- 财务风险通常指公司的融资风险
- 可能来自于外汇、利率和大宗商品价格波动所产生的风险；还包括信贷风险、流动性风险和市场风险。
- 注意：财务部门相关风险属于运营风险，不属于财务风险

灾害风险

- 灾害风险通常与自然灾害有关
- 灾害风险通常是可以被保险的
- 灾害风险三项环境测试：
 - ① 必须产生财务影响
 - ② 不必然会出现
 - ③ 必须是负面结果

资本充足率 Capital adequacy ratio

- 资本充足率用于测量金融机构偿付能力、流动性、储备和充足资本等方面的风险指标。
- 2010年制定的《巴塞尔协议 III》(the Third Basel Accord, Basel III)给商业银行规定了最低的资本充足率，即确定需要维持多少的资本水平才能使商业银行承担由现有风险所造成的损失，并且达到可接受的偿债能力水平，它旨在抑制风险资产的过度膨胀，保护存款人与债权人的利益。

一级资本 + 二级资本

➤ 资本充足率 = 风险加权资产

- 一级资本：无须终止业务，用来吸收损失的资本
- 二级资本：业务清算时候，用来吸收损失的资本
- 风险加权资产：针对每项资产进行风险评估，计算加权平均值

风险管理流程

- 风险识别
- 风险评估
- 风险应对

- 风险沟通与监督

风险识别 Risk identification

- 风险识别：需要通过有计划且细致的方法在运营的各个方面来查找潜在的风险，并确认那些重要的风险领域。
- 目的：列示出全部风险，然后给予评估，将风险范围缩小至组织所面临的主要风险。

风险识别技术

1. 内部访谈与讨论

包括：访谈、问卷调查、头脑风暴、自我评估及其他协调讨论和 SWOT 分析。

2. 外部来源 (external sources)

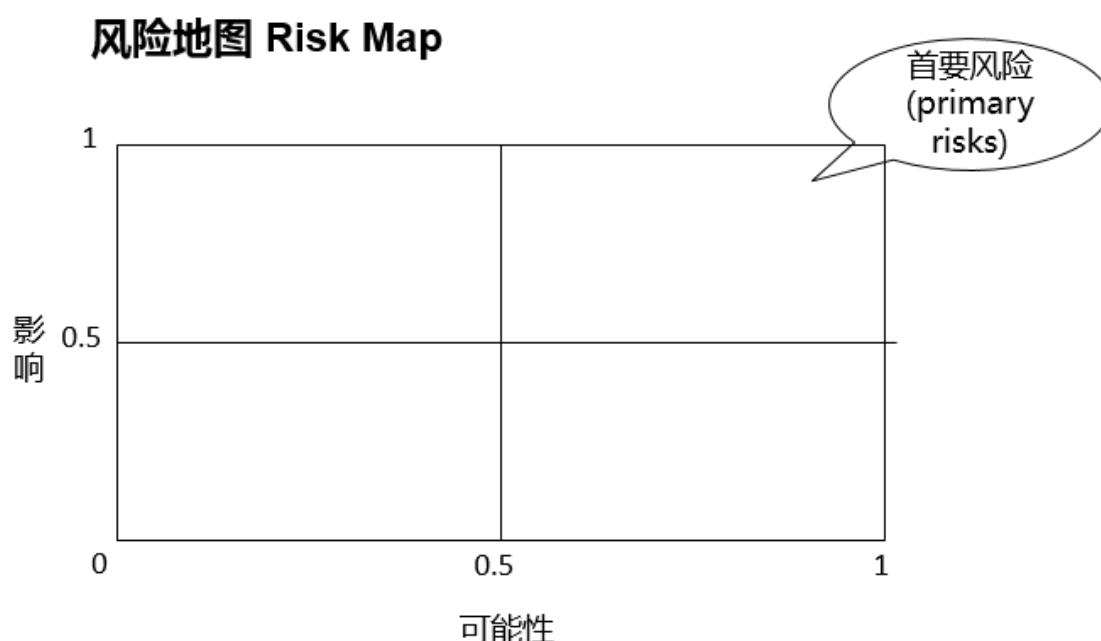
包括：与其他组织比较、与同行讨论、标杆管理和风险顾问。

3. 工具、诊断和流程

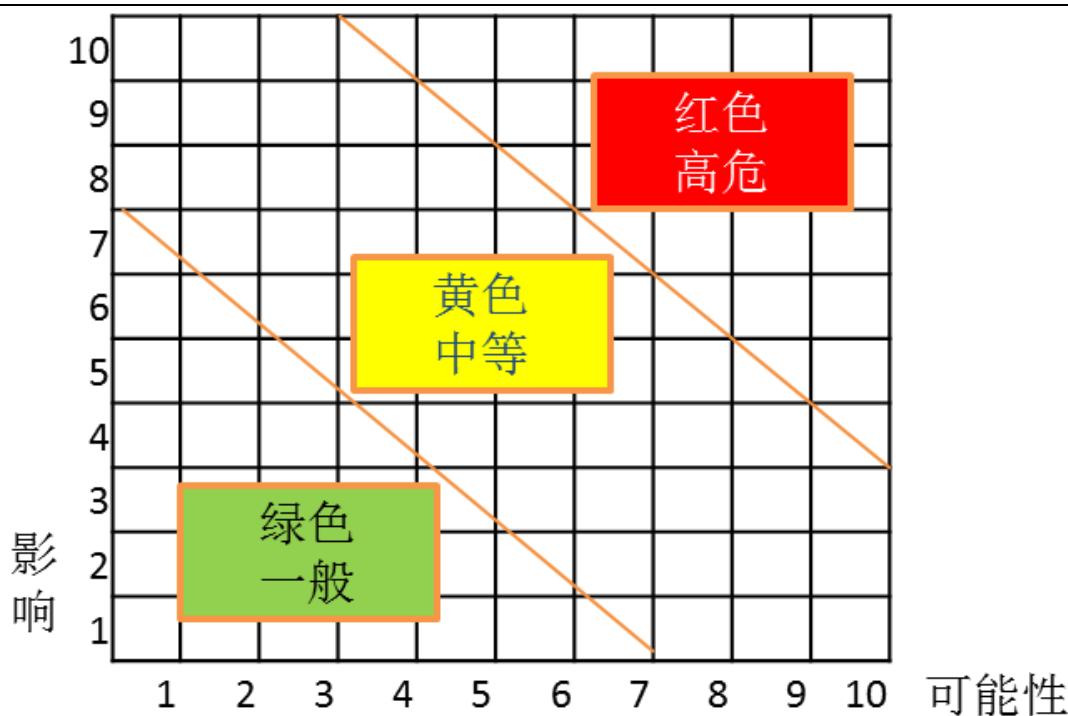
包括：对照表、流程图、情景分析、价值链分析、业务流程分析、系统工程和流程绘制。

风险评估 Risk assessment

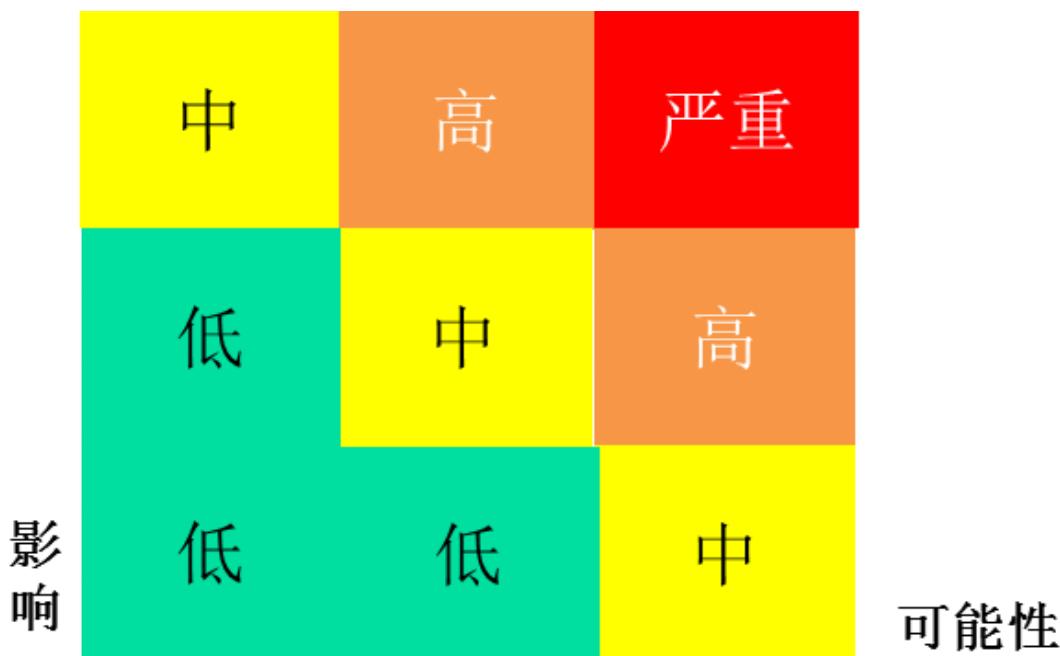
- 风险评估：分析已识别风险潜在影响的过程，并根据以下两大关键要素，进行风险排序，并识别出对企业影响最大的风险。
 - ① 风险可能性：风险发生概率
 - ② 影响程度：一旦发生风险，会产生怎样的影响
- 风险 = 概率 × 影响程度



详细风险地图



热力图



风险评估 Risk assessment

- 固有风险 (Inherent risk): 在管理层没有采取任何措施来改变风险的可能性或影响的情况下，一个主体所面临的风险。
- 剩余风险 (Residual risk): 在管理层采取了风险应对措施之后所残余的风险。
- 风险偏好 (risk appetite): 在现有使命和业务模式下，组织愿意接受的风险水平
- 组织的风险偏好决定了管理层将如何管理风险。
- 风险容量: 组织可承受的风险幅度。

风险应对 Risk Response

- 回避 (avoidance)
- 降低 (reduction)
- 分担 (sharing)
- 承受 (acceptance)

风险回避 Avoidance

- 企业退出会产生风险的活动。
- 触发条件：剩余风险 > 风险容量

风险降低 Reduction

- 企业采取措施来降低风险的可能性或影响，或者同时降低两者
- 触发条件：固有风险 > 风险容量
- 目标：剩余风险 < 风险容量

风险分担 Sharing

- 分担风险的实质就是转移风险，即通过合约的方式将风险转嫁给另一个机构；以此降低整体风险。
- 常见的技术包括购买保险产品、从事避险交易或外包一项业务活动。
- 触发条件：固有风险 > 风险容量
- 目标：剩余风险 < 风险容量

风险承受 Acceptance

- 企业不采取任何措施去干预风险，而是利用风险获得利益，也称为风险自留
- 触发条件：固有风险 < 风险容量

风险沟通与监督

- 与风险相关的沟通必须在组织内部全方位展开。
- 在一个管理良好的组织中，应使绩效和风险指标的监督工作常态化。

企业风险管理 Enterprise risk management

- 企业风险管理(ERM)是对企业所面临的所有综合风险的分析和管理。
- 企业面临的风险包括：财务风险、营运风险、合规风险等。

企业风险管理的目标 (IMA 管理会计公告)

- 通过管理对影响组织目标实现的不确定性，借此创造、保护和增加股东价值。
- 更加强有力的内部控制、更加行之有效的公司治理和 ERM 实施，能提升组织的稳定性和反应速度，增加股东价值。
- 从整体利全局的视角来看待组织面临的风险。

COSO 企业风险管理框架

- 企业风险管理是企业用来识别和管理风险，以及用适当措施应对风险的过程。
- 企业风险管理是涉及整个组织的、持续的、动态的过程。

企业风险管理的价值

- 价值创造：收益 > 成本
- 价值保持：收益 = 成本
- 价值实现：利益相关者获利
- 价值侵蚀：战略未达到预期

使命与愿景

- 使命和愿景协助组织构建边界，关注决策如何影响战略。
- 组织在充分理解自己的使命和愿景之后，其设定的战略能够形成一个理想的风险特征。
- 企业风险管理能协助组织避免战略错配。
- 企业需要评估所选的战略将如何影响组织的风险特征，特别是企业可能受到的影响的风险的类型和数量。

风险和绩效

- 风险管理要求管理层去考察风险的类型、严重度和关联性，及其这些风险相对于战略和业务目标如何对绩效产生影响。
- 企业可以利用他们的风险特征来更好地理解风险、目标绩效和实际绩效之间的内在关联性。

企业风险管理的充分整合

- 在进行决策时，管理者和董事会必须持续地设身于动态的商业环境之中；这要求在任何时刻都把企业风险管理的思维整合到组织的各个方面。
- 需要将文化、实践和能力整合在一起并应用在整个企业的范围内，以此促使企业风险管理的充分整合。

COSO ERM 五大关联部分

- ① 治理与文化

- ② 战略与目标设定
- ③ 绩效
- ④ 审阅与修正
- ⑤ 信息、沟通与报告

治理与文化

- 公司治理影响企业风险管理监督权责的建立和执行。
- 文化关系到组织内的价值观、预期行为和对风险的理解
- 公司应实施董事会风险监督，风险监管首要责任是对利益相关者的信托责任

原则	说明
实施董事会风险监督	风险监管首要责任： 即 对利益相关者的 信托责任
构建 运营结构； 设置 报告路径	界定责任、实施业务目标
界定理想文化	体现组织文化的理想行为 (风险规避与风险激进)
致力于核心文化	遵守核心价值与理想文化
吸引、培养和留住人才	人力资本的构建

战略与目标设定

- 组织进行未来规划时，必须结合企业风险管理、 总体战略和组织目标。
- 组织必须确定他们的风险偏好，同时风险偏好必须与组织战略保持一致。
- 目标可以帮助组织实现其战略和管理风险。

原则	说明
分析商业环境	外部环境：PESTEL 内部环境：四要素
定义风险偏好	风险偏好相关因素
评估风险不同的战略选项	识别潜在风险与机会； 风险偏好与战略目标一致 保持中立
制定业务目标	设定业务目标时，需要考虑到风险； 通过 业绩容忍度，了解风险是否可以接受

PESTEL 模型

外部环境要素	
类别	特征
政治 P	政府干预和影响的性质和范围，包括税收政策、劳工法规、环境法规、贸易限制、关税和政治稳定性
经济 E	利率、通胀、汇率、信贷可用性、GDP 增长
社会 S	消费者的需求或预期；人口统计，比如人口分布、教育程度、财富分布
技术 T	研发活动、自动化和技术激励；技术变化或中断的速率

环境 E	自然或人为造成的灾害，持续的气候变化，能源消耗法规的变化，对待环境的态度
法律 L	法律（比如：就业、消费者、健康与安全），监管，和/或法律行业标准

内部环境要素

内部环境要素	
类别	特征
资本	现金、设备、不动产、专利
技术	新技术、调整的计算和/或采用的技术
人员	知识、技能、态度、关系、价值观和文化
流程	活动、政策或流程、管理、经营和支持流动的调整

风险偏好的相关因素

参数	说明
战略参数	新产品决策、资本投资、兼并与合并
财务参数	最大可接受的财务业绩的波动、资产回报率、风险调整资本回报率、目标债务评级、目标负债权益比
经营参数	环境要求、安全目标、品质目标、顾客集中度
风险特征	风险数量和分布、企业风险的不同类型
风险容量	最多能够承受的风险数量

绩效

- 针对可能影响到战略和目标的风险，组织必须予以识别和规划应对措施。

- 组织必须建立一个流程，向关键利益相关者报告组织风险状况

相关执行原则

原则	说明
识别风险	识别新的、正在出现的和变异的风险；风险清单；识别方法
评估风险的严重程度	影响和可能性；风险属性
风险排序	适应性，复杂性，速度，持续性，恢复
风险应对措施	回避、降低、分担、承受
开发风险组合视角	类别、严重度和风险之间的关联性

识别风险

➤ 新的、正在出现的和变异的风险，包括：

- 由业务目标变化所生产的风险
- 由商业环境变化所产生的风险
- 在此之前，企业尚未涉及该商业环境
- 之前未知的风险

- 之前已识别的风险，但这些风险已随着商业环境、风险偏好或支持假设的变化而变化

评估风险的严重度

- 影响：风险的结果或影响。
- 可能性：风险发生的机率。
- 管理层需要将风险的可能性与影响结合在一起考虑。

风险类型

- 固有风险：在管理层没有采取任何直接或集中行动来改变风险严重度时，企业有的风险。
- 目标剩余风险：在了解了管理层将要或已经采取了直接或集中行动来改变风险的严重度之后，企业在实施战略和业务目标时，所愿意承担的风险数量。（主观意愿）
- 实际剩余风险：在管理层已经采取了调整风险严重度的措施之后，依然剩下的风险。（客观实际）
- 实际剩余风险 \leq 目标剩余风险。
- 实际剩余风险 $>$ 目标风险；需要采取额外的行动调整风险的严重度。

风险排序需考虑的要素

- 风险适应能力
- 风险复杂程度
- 风险影响速度
- 风险持续性
- 风险恢复性

影响风险应对措施选择的因素

- 商业环境
- 责任与预期
- 成本与收益
- 风险排序
- 风险偏好
- 风险严重度

审阅与修正

- 企业风险管理是一个更新和迭代的过程。
- 不断审阅和修订企业风险管理的内容，可以帮助组织更好的管理业务中不断变化的风险环境。

信息、沟通与报告

- 企业风险管理的关键能力，就是快速、准确、确定地沟通风险相关信息。
- 这种沟通必须在组织内外的各方之间进行。

COSO ERM 的优点

- 增加机会的范围。通过考虑所有的可能性，管理层可以识别与当前机会相关的新机会和独特的挑战。
- 在整个实体范围内识别和管理风险。
- 增加积极结果和优势，同时减少负面意外。
- 降低绩效波动性，实现损失最小化和机会最大化。
- 增强企业韧性。
- 改进资源部署，优化配置。