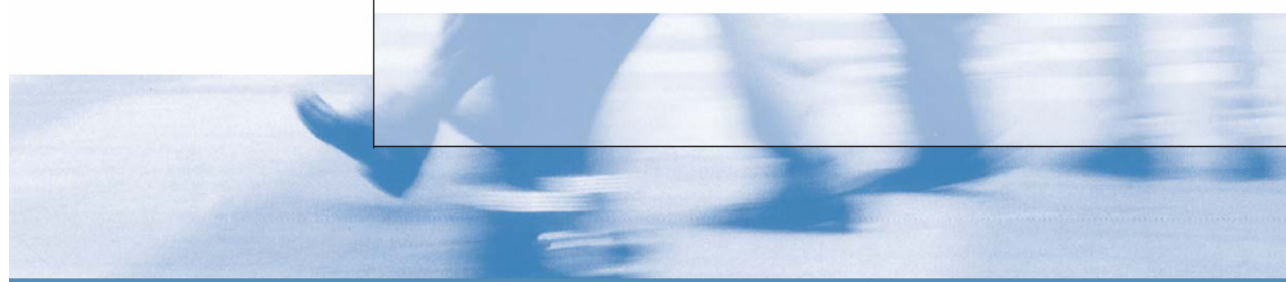




FEDERATION OF
EUROPEAN RISK
MANAGEMENT
ASSOCIATIONS

**A RISK MANAGEMENT
STANDARD**
(CHINESE VERSION)
Second version



前言

本风险管理准则是由英国主要风险管理机构的精英组成的团队所研拟出来的成果，这些机构包括风险管理学会、保险及风险管理人协会(AIRMIC)及政府部门的ALARM风险管理国家研讨会等。

此外，在长期的咨询过程中，该团队也向其他关注风险管理的专业团体极广泛地征询其观点及意见。

风险管理是一门正在快速发展的学科，对于风险管理的范围、实施方法以及目的等有很多不同的观点及描述，需要以准则来确保下列事项可达一致性：

- *相关的专门术语*
- *实施风险管理的步骤*
- *风险管理的组织架构*
- *风险管理的目的*

很重要的是，本准则认定风险有好有坏。

风险管理不只是企业或政府机构的事，它也涉及短期或者长期的各项活动。不能仅从活动的本身来考虑其利益及机会，许多可能受影响的各股东权益也当被考虑到。

达到风险管理目的有许多种方法，不可能尝试在单独一份文件中说明全部，因此我们并不打算以非常繁复的程序定出准则，也不会建立一套保证有用的步骤；但藉由达到此准则的各构成要素，纵使以不同的方法，机构仍可宣称其符合准则。本准则提供了最佳的实务，机构可以据此作自我评估。

本准则已尽量使用国际标准化组织(ISO)近期文件ISO/IEC风险管理指南73-字汇-准则使用指导方针中的风险专门术语。

有鉴于此一领域快速发展，若使用此准则的机构能有所回馈（在本准则的封底可以找到地址），作者群会非常感谢，本准则将例行作修订以反映最佳实务。

1. 风险

风险可定义为事件发生的可能性及其结果的组合(ISO/IEC指南73)。

在各种型态的企业中，事件及其结果可能带来获利的机会（正面）或威胁成功（负面）。

风险管理逐渐开始重视风险的正面及负面影响；因此，本准则也从这两方面做考虑。

在安全的领域，通常认为只带来负面的结果，因此，安全风险之管理都专注于损害的预防及降低。

2. 风险管理

风险管理是机构策略管理的核心部分，它是机构条理化处理活动中的风险的步骤，其目的是从各项活动及活动的组合中获得持续的利益。

好的风险管理专注于风险的界定及处置，目的是持续扩大机构的活动价值，它整理出可能带给机构正面及负面影响的因素，然后提升达成机构整体目标的可能性，并降低失败的可能性和不确定性。

风险管理应该是一项持续发展的步骤，持续运作于机构策略的制定及实施中，它应该条理化地处理机构活动在过去、现在尤其是未来所面临的风险。

它应该透过最高管理层有效的政策及所领导的计划整合于企业文化中，它应该将策略转换成战略性及营运性目标、将责任分配给负责管理风险的各经理及员工，并视其为职务说明的一部分，如此可作为责任、绩效评估及奖惩的依据，并提升所有阶层的营运绩效。

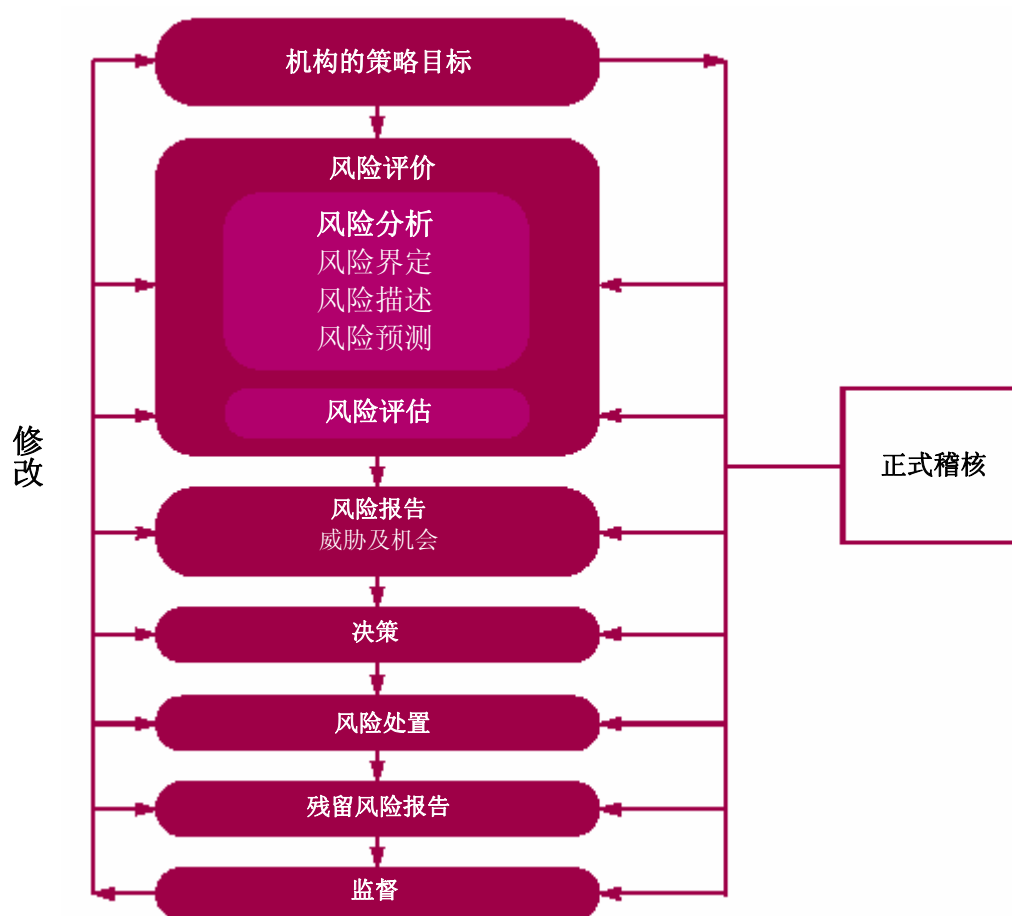
2.1 外部及内部因素

机构及其营运所面临的风险可能是由该机构外部因素，也可能是由内部因素所造成，下页图表总结了这些领域主要风险的例子，同时也显示出某些特定的风险可能同时受到外部及内部因素的驱动，而重复出现在这两个领域。它们可再细分为几种风险型态，例如：策略方面、财务方面、营运方面及突发事件方面等。

2.1 主要风险驱动因素案例



2.2 风险管理步骤



风险管理透过支持机构策略目标而为机构及其有关人士提供保障或增加价值，方法如下：

- 为机构提供一个让未来活动能以一贯且可掌控的方式来进行的架构
- 藉由广泛且结构性的了解业务活动、发展及项目所带及存的机会/威胁以改善决策订定、计划及排定优先级
- 在机构内更有效地使用/配置资金及资源
- 减少企业内非必要领域的开发
- 保障并强化资产及公司形象
- 开发并支持人员及机构的知识基础
- 提升营运效率

3. 风险评价

ISO/IEC 将风险评价定义为**风险分析及风险评估**的整体步骤。（请参阅附件）

4. 风险分析

4.1 风险界定

风险界定是界定机构所暴露的不确定性，必须对机构、其所经营的市场、其所处环境的法律、社会、政治及文化有深入的认识；同时必须彻底了解其策略性及营运性目标，包括成功的关键因素以及达成这些目标的相关威胁及机会。

应以有条理的方法来界定风险，确保机构内的活动都经过审视且定义出相关的风险，并应界定及分类伴随这些活动而来的变数。

可用不同的方法分类企业的活动及决策，例如：

- *策略性的 – 这些关系到机构的长期策略目标，可能会受到资本可用性、主管机关及政治风险、法律及规定变更、名誉及实际环境变更的影响。*
- *营运性的 – 这些关系到机构为实践其策略目标所面对的日常事务。*
 - *财务性的 – 这些关系到机构财务的有效管理及控制以及外部因素的影响，例如：可获得的信用、外币兑换率及利率变动以及其他市场风险。*
- *知识管理 – 这些关系到知识资源、生产、保护及相关的沟通的有效管理及控制，外部因素可能包括未经授权使用或滥用智能财产、区域性停电以及竞争的技术等；内部因素可能是系统故障或重要职员离职等。*
- *守法 – 这些关系到健康与安全、环保、交易记述、消费者保护、数据保护、雇佣关系及主管机关事务等*

虽然可以由外部顾问执行风险界定，但具备良好沟通、一贯且协调的步骤及工具（请参阅附件）的内部管道可能会更有效率。内部”主导”风险管理流程是必要的。

4.2 风险描述

风险描述的目的是将已界定的风险以结构性的形式呈现出来，例如用表列式。下一页的风险描述表可用来描述及评价风险。使用设计良好的架构是用来界定风险、描述及评价完整步骤所必须的，透过考虑表中所列各项风险的结果及可能性，就可排列出须作更详细分析的主要风险之优先级。

企业活动及决策订定所伴随的风险界定可以分为策略性、项目/战略性及营运性。

特定的项目在规划阶段以及整个生命周期都应该纳入风险管理。

表 4.2.1 – 风险描述

1. 风险名称	
2. 风险范围	对于事件之规模、型态、数量及关联物作本质上的描述。
3. 风险的本质	例如：策略的、财务的、知识的或守法的。
4. 股东	股东及他们的期望
5. 风险的量化	严重性及可能性
6. 风险容忍度/包容度	风险的潜在损失及财务影响 风险的价值 潜在损失/获利的可能性及规模 风险控制的目的及期望的绩效水平
7. 风险处置及控制机制	目前管理风险的主要方法 目前控制的信心水平 监督及检讨模式的界定
8. 改善的可能行动	降低风险的建议
9. 策略及政策的开发	界定负责开发策略及政策的职务

4.3 风险估计

风险估计是对发生的可能性及可能的结果所做的量化、准量化或质化的估计。例如结果的威胁性（不利风险）或机会（有利风险）可能很高、中等或很低（请参阅表 4.3.1），机率可能很高、中等或很低，但需对威胁及机会作出不同的定义（请参阅表

4.3.2及4.3.3)，下页中有一些例子。不同的机构会发现不同的结果及最可能符合其需求的可能性评估方法。

例如许多机构发现将结果及可能性评估为高、中等或低已可满足其需求，可以用3x3的矩阵来表达；而其他机构则可能觉得以5x5的矩阵来评估结果及可能性更为适合。

表 4.3.1 结果 – 威胁及机会

高	对机构的财务影响可能超过 £x 对机构的策略或营运活动有严重影响 股东严重关切
中	对机构的财务影响可能在 £x及 £y之间 对机构的策略或营运活动有中等程度的影响 股东关切的程度中等
低	对机构的财务影响可能不超过 £y 对机构的策略或营运活动影响程度很低 股东关切程度很低

表 4.3.2 发生的可能性 – 威胁

估计	描述	指标
高 (很有可能)	每年都很有可能发生或发生的机会大于 25%	在一定期间内 (例如 10 年) 可能发生许多次。 最近发生过。
中 (有可能)	在10年期间内很有可能发生或发生的机会小于25%	在一定期间内 (例如10年) 可能发生一次以上。 由于某些外部影响而难以控制。 曾发生过吗?
低 (微乎其微)	在 10 年期间内不太可能发生或发生的机会小于 2%	没发生过。 不太可能发生。

表 4.3.3 发生的可能性 – 机会

估计	描述	指标
高 (很有可能)	一年内很有可能达成所希望的结果, 或发生的机会大于 75%	有合理的必然性可以信赖的明确机率, 根据目前的管理流程在短期内会实现。
中 (有可能)	可合理期待一年内期望的结果或发生的机会在 25%至 75%之间	有实现的可能性, 但需要审慎管理。 有超越计划的可能性。
低 (微乎其微)	未来中期有一些机会得到期望的结果或发生的机会小于 25%	管理阶层尚未仔细研究其可能性。 以目前所使用的管理资源要成功的可能性很低。

4.4 风险分析方法及技术

分析风险所可使用的技术有很多, 有些是针对有利风险、有些针对不利风险, 而有些则适用于两者 (请参阅附件案例)。

4.5 风险概况

风险分析步骤的结果是产生风险的概况, 可以为每一项风险的严重性评比, 并提供依序处理风险的工具。

各项风险的排序可以让我们看清相对的重要性。

这个步骤可以将风险标示于企业受影响的领域、描述所实施的主要控制程序, 并指出哪些地方的风险管理投资水平应该增加、减少或重新分配。

职责区分可以帮助确认风险的” 管理者” 及适当分配管理资源。

5. 风险评估

完成风险分析步骤后就应该将所评估的风险与该机构所建立的风险标准互相对照，风险标准可能包括相关的成本及利益、法律规定、社会经济及环境因素、相关人士在意的问题等。

因此，风险评估是用来判断风险对机构的重要性以及决定各项特定风险是否应接受或处置。

6. 风险处置

风险处置是选择并实施降低风险之方法的步骤，风险处置的主要原理是风险控制/减轻，但可进一步衍生为风险回避、风险转移、风险资金等。

附注：在本准则中，风险资金系指为风险结果筹措资金的机制（例如保险计划），风险资金通常不是为实施风险处置之成本而是提供资金（如ISO/IEC指南73所定义者；请参阅附件）。

风险处置的任何系统至少应提供：

- 机构营运的效率及效果
- 有效的内部控制
- 遵守法律及规定

风险分析步骤界定出需要管理阶层注意的风险，可以帮助机构有效的营运，其必须根据对机构的潜在利益排定控制行动的优先级。

内部控制的效果就是以预定的控制方法将风险排除或降低的程度。

内部控制的成本效益就是实施控制的成本与风险降低的预期利益之相互关系。

建议的控制方法必须以假设不采取行动的潜在经济影响与采取建议行动的成本来衡量比较，这需要有更详细的信息及假设。

首先必须知道实施的成本，这需要精确计算，因为它很快就会成为衡量成本效益的基础；如果不采取行动的预期损失也必须估算出来，透过两者比较的结果，管理阶层便可决定风险控制方法是否须实施。

遵守法律及规定是没有选择性的，机构必须了解相关法令并据以实施控制系统，只有当降低风险的成本显然不适当的情况下才有一些弹性。

为风险的影响取得财务保障的方法之一是透过风险分摊，包括保险，但是必须了解有些损失或损失项目是无法投保的，例如与工作相关的健康、安全或环境意外的成本并不在保障范围，这些可能还包括员工士气及机构声誉的损失。

7. 风险报告及沟通

7.1 内部报告

机构内不同的层级需要不同的风险管理信息。

董事会应该：

- 知道机构所面临的最严重的风险
- 知道对股票价值与预期绩效范围差异的影响
- 让整个机构保持适当程度的警觉
- 知道机构管理危机的方法
- 知道机构内相关人士信心的重要性
- 知道如何在适当时机与投资大众的沟通
- 使风险管理步骤能有效运作
- 发布明确的风险管理政策，包括风险管理理念及责任。

营运单位应该：

- 了解自己责任领域所面临的风险、这些风险对其他单位的影响以及其影响带来的结果。
- 设绩效指标以便监督核心业务及财务活动、达成目标的进度以及界定介入的状况（例如预测及预算）。
- 有关预算及预测的差异，提供适当沟通系统及程序，以便采取行动
- 系统性地且实时向上级管理阶层报告新接触到的风险或未能履行现行控制方法

个人应该：

- 了解对个别风险所负的责任
- 了解如何持续改善风险管理因应机制
- 了解风险管理及风险警觉是机构文化的重要部份
- 系统性地且实时向上级管理阶层报告新接触到的风险或未能履行现行控制方法。

7.2 外部报告

公司必须定期向股东报告风险管理政策及其对达成目标的有效性。

股东越来越关注非财务绩效方面有效管理的事项，例如：小区事务、人权、聘雇关系、健康及安全以及环境。

好的公司治理要求公司采用条理化的风险管理方法：

- 保障股东利益
- 确保董事会可执行其职权引导策略、建立价值并监督机构之绩效
- 确保适当实施管理控制程序

应明确陈述风险管理正式报告的处理并让股东了解。

正式报告应针对：

- 控制方法 – 尤其是风险管理的管理职责
- 界定风险所采用的步骤以及风险管理系统执行方式
- 管理重大风险所采用的主要控制系统
- 所采用的监督及检讨系统

系统范围或系统本身如有重大缺失应与处理步骤一并报告。

8. 风险管理的架构及行政

8.1 风险管理政策

机构的风险管理政策应揭示公司对风险的态度及所能接受程度及其对风险的管理方法，同时应揭示机构内各部门及人员在风险管理方面的职责。

此外，政策说明应参考法令规定，例如健康及安全方面。

在风险管理步骤中应附有整套的工具及技术，以便在进行的不同阶段中使用。为能有效运作，风险管理步骤需要：

- *机构中首席执行官与执行管理阶层的沟通*
- *在机构中分派职责*
- *为有关人士强化风险警觉的训练及发展配置适当的资源*

8.2 董事会的角色

董事会应负责决定机构的策略方向并营造风险管理有效运作的环境及架构。

这可透过一个执行团队、非执行委员会、稽核委员会或其他部门，只要是适合机构的营运方法且能够担任风险管理的推动者即可。

董事会至少应参与评估内部控制系统：

- *公司在其特定业务中所能接受的坏的风险的本质及程度*
- *该风险成为事实的可能性*
- *应如何管理不能接受的风险*
- *公司降低风险可能性及其对业务影响的能力*
- *对风险所采取的控制活动的成本及效益*
- *风险管理步骤的效果*
- *对董事会所作决议的风险估计*

8.3 营运单位的职责

包括：

- 营运单位对风险管理日常事务负主要责任
- 营运单位管理阶层应负责在其营运范围内推广风险意识，将风险管理目标导入其业务
- 风险管理应是管理会议的例行项目，以便讨论暴露状况，并根据风险分析重新排定工作优先级
- 营运单位管理阶层应确保项目的规划阶段以及整个项目过程均考虑到风险管理

8.4 风险管理单位的职责

依机构的规模，风险管理单位可能是单独一个人、一个兼职的风险经理到一个完整的风险管理部门。

风险管理单位的职责应包括：

- 制定风险管理政策及策略
- 在策略及营运层次担任风险管理的主要负责人
- 在机构内建立风险认知的文化，包括适当的训练
- 为各业务单位建立内部风险政策及架构
- 设计并检讨风险管理步骤
- 协调机构内各部门有关风险管理事务的活动
- 设计风险因应程序，包括突发事故及危难事故营业继续计划
- 向董事会及股东的风险报告

8.5 内部稽核的职责

每个机构内部稽核的职责都不相同，实务上，内部稽核的职责包括下列部份：

- 专注于由管理阶层所界定的重大风险的内部稽核工作，同时稽核整个机构的风险管理步骤
- 对风险管理程序提供质量保证
- 积极支持并参与风险管理步骤
- 在风险管理及内部控制方面帮助界定风险/评价及教育之推动

- *协调对董事会及稽核委员会等单位的风险报告*

在为特定机构决定最适当的职责时，内部稽核应确保不违反独立性及客观性的专业要求。

8.6 资源及履行

履行机构政策所需的资源应明确建立于各管理阶层及各事业单位之间。

除了原有的营运职责之外，所有单位应明确定义其参与风险管理之协调政策/策略方面的职责。

而稽核及风险管理单位也应同样阐明其参与风险管理的职责。

风险管理应透过策略及预算程序深植于机构内，藉由新进员工训练及其他训练和发展计划来传达，就像其他营运程序一样，例如商品/服务发展项目。

9. 风险管理步骤的监督及检讨

有效的风险管理需要有报告及检讨架构，以有效界定与评价风险；同时确保实施控制及响应机制、定期稽核政策及标准的遵守情形、检讨标准绩效，以便掌握改善的机会。应记住机构是动态的、且在一个动态的环境中营运，需掌握机构及环境的变更，并对系统作出适当的修正。

监督步骤应能确定对机构的活动实施了适当的控制，同时了解所有的程序并据以遵守。需掌握机构及环境的变更并对系统作出适当的修正。

任何监督及检讨步骤应能判断：

- *所采用的方法能否得到希望的结果*
- *为执行评价所采用的程序及所搜集的信息是否适当*
- *所增加的知识是否有助于作出更好的决策，是否能为未来风险的评价及管理界定应学习的课题*

10. 附件

风险界定技术 – 举例

- 脑力激荡
- 问卷
- 营运研究，探讨营运的每个步骤并描述每个可能影响这些步骤的内部程序及外部因素
- 产业标竿
- 情境分析
- 风险评估研讨会
- 事故调查
- 稽核及检查
- *HAZOP* (威胁及机会研究)

风险分析方法及技术 – 举例

好的风险

- 市场调查
- 探勘
- 营销测试
- 研究及发展
- 业务影响分析

两者

- 依赖性模型
- *SWOT*分析 (优点、缺点、机会、威胁)
- 事件树状分析
- 紧急危难营运继续计划
- *BPEST* (政治、经济、社会、科技) 分析
- 真实选择模型
- 风险及不确定情况下作决策
- 统计推论
- 中央集中及分散之评估
- *PESTLE* (政治、经济、社会、技术、法律、环境)

坏的风险

- 威胁分析
- 过失树状分析
- *FMEA* (缺点型态及影响分析)



Head Office

FERMA a.i.s.b.l.

Avenue Louis Gribaumont 1, B 4

B-1150 Brussels - Belgium

Ph: +32 2 761 94 31

Fax: +32 2 771 87 20

info@ferma.eu

www.ferma.eu

ALARM - The National Forum for Risk Management in the Public Sector

Queens Drive, Exmouth - Devon, EX8 2AY

Tel: 01395 223399 - Fax: 01395 223304 - Email admin@alarm.uk.com - www.alarm-uk.com

IRM - The Institute of Risk Management

6 Lloyd's Avenue - London EC3N 3AX

Tel: 020 7709 9808 - Facsimile 020 7709 0716 - Email enquiries@theIRM.org - www.theirm.org