普华经管

风险矩阵

在企业风险管理中的应用

——详解风险矩阵评估方法

李素鹏 著

人民邮电出版社
POSTS & TELECOM PRESS

风险矩阵在企业风险管理中的应用

——详解风险矩阵评估方法

李素鹏　著

人民邮电出版社
北　京

图书在版编目（CIP）数据

风险矩阵在企业风险管理中的应用：详解风险矩阵评估方法 / 李素鹏著. —北京：人民邮电出版社，2013.2

ISBN 978-7-115-30750-7

Ⅰ. ①风… Ⅱ. ①李… Ⅲ. ①企业管理—风险管理—研究 Ⅳ. ①F272.3

中国版本图书馆 CIP 数据核字（2013）第 003488 号

内 容 提 要

本书重点阐述了风险矩阵与风险准则的对应关系，详细解析了风险矩阵的定性应用、半定量应用及定量应用；特别推介了 Borda 方法和权值法，其中，Borda 方法用于打开定性和半定量风险矩阵产生的风险结，权值法用于估算定量风险矩阵的总风险值。本书还阐明了风险矩阵与风险评估各子过程的对应关系，以及风险图谱在风险管理监测与评审子过程中的应用情况。

本书适合专业风险评估人员、企业风险管理人员、风险管理评审或审计人员阅读使用，还可作为 NPO（非营利组织）风险管理人员和高校相关专业师生的参考用书。

风险矩阵在企业风险管理中的应用——详解风险矩阵评估方法

◆ 著 李素鹏

责任编辑 刘 盈

◆ 人民邮电出版社出版发行 北京市崇文区夕照寺街 14 号

邮编 100061 电子邮件 315@ptpress.com.cn

网址 http://www.ptpress.com.cn

三河市潮河印业有限公司印刷

◆ 开本：787×1092 1/16

印张：12.5 2013 年 2 月第 1 版

字数：100 千字 2013 年 2 月河北第 1 次印刷

ISBN 978-7-115-30750-7

定 价：30.00 元

读者服务热线：（010）67129879 印装质量热线：（010）67129223

反盗版热线：（010）67171154

广告经营许可证：京崇工商广字第 0021 号

前　言

各种类型及规模的组织在生存和发展的过程中都会面临各种各样的风险，这些风险有可能影响到其目标的实现。组织的目标可能涉及各类活动，包括战略规划、运行过程及项目等，也可能体现在社会、技术、环境和安全结果以及商业、财务和经济措施方面。

企业风险管理有两个基本前提，一是为利益相关方带来价值，二是正确面对不确定性。对企业管理者而言，其面临的挑战就是在帮助利益相关方实现增值的同时，还要应对各种不确定性。不确定性来源于无法明确的潜在事件，这些事件发生的可能性不确定，结果也不确定。企业经营过程中的许多因素都会给企业带来不确定性，如全球化进程加快、技术革新、企业重组、市场变化以及竞争加剧等。

作为 CEO（总经理），你肯定想知道自己的企业当前或未来某个时间将面临什么风险，这些风险有多大，其分布又是什么样的以及应该怎样应对它们。

作为 PM（项目经理），你也肯定想知道自己负责的项目在当前或未来某个时间将会面临哪些风险，这些风险有多大，它们是怎么分布的以及有哪些应对策略和方法?

企业可以通过评估不确定性和未来事项或环境变化的可能性及其对约定目标的影响，对各项活动中存在的风险进行有效管理。

风险评估为企业决策提供重要的参考依据。企业要不要跟踪某个“机会”，要不要针对某个“威胁”制定风险预案或风险控制措施，很大程度上取决于该“机会”是否符合企业的发展目标，该“威胁”是否超过了企业的风险容忍范围。企业只有关注风险、准确评估风险，才能在应对风险时处于最佳状态。

风险评估的方法和技术很多，风险矩阵方法以其简洁、直观等优点被广泛应用。中国国务院国资委 2006 年在《中央企业全面风险管理指引》的附录中也特别推荐了该方法，并要求各中央企业在之后每年的风险管理报告中应用这种方法绘制企业重大风险的风险矩阵图。

在 ISO/IEC 31010：2009《风险管理——风险评估技术》标准里，ISO 和 IEC 一共推荐了 31 种方法，本书着重讲述了第 29 种方法“Consequence / probability matrix”（后果/可能性矩阵）。

本书主要解决以下五个核心问题。

1. 揭示风险准则与风险矩阵的关系。
2. 用风险矩阵图揭示企业的风险分布以及各风险的风险等级。
3. 利用 Borda 方法打开定性和半定量风险矩阵图所产生的风险结。
4. 基于定量风险评估，用权值法估算组织（企业整体或某业务）的总风险值。
5. 用风险矩阵图监测与评审企业风险管理的状况和绩效。

为了方便读者理解和应用，本书提供了丰富的案例，并以大量的图表对风险矩阵法的各个细节进行了分解说明。本书介绍的各种方法和图表均适用于企业的风险管理实务。

本书在编写过程中得到了国务院国资委研究中心、中国风险管理与内部控制研究中心相关专家的支持和帮助，在此表示感谢！

李素鹏

2013 年 1 月于北京

目　录

第1章

风险矩阵概述

风险是指不确定性对目标的影响；风险管理是指针对风险所采取的协调活动。风险矩阵是从风险后果及其发生的可能性两个维度来分析风险的等级，并揭示风险的重要性。

定性分析关注事物的“质”，用语言文字表示其过程和结果；定量分析关注事物的“量”，用数据表示其结果。定性分析和定量分析相辅相成。风险矩阵适合定性分析和半定量分析，由风险矩阵演变而来的“风险坐标图”则适合定量分析。

1.1　风险

1.1.1　风险的由来

在我国，对于“风险”一词的由来，较为普遍的一种说法是：渔民们每次出海前都要祈祷，祈求神灵保佑自己能够满载而归。他们在长期的生活实践中，深深地体会到“风”会带给他们无法预测的危险，认为“风”即意味着“险”，于是就产生了“风险”一词。

还有一些人认为“风险（Risk）”一词是舶来品，他们中有人认为“风险”来自阿拉伯语，也有人认为这个词来源于西班牙语或拉丁语，但比较权威的说法是来源于意大利语的“Risque”一词。在早期的运用中，该词被理解为客观的危险，体现为自然现象或者航海遇到礁石、风暴等事件。还有人认为“Risk”一词来自古希腊单词“Rhiza”，该词表示靠近峭壁航行危险，有可能撞上礁石，有可能碰上暗流，还有可能遇上从崖上掉下来的石头。

17 世纪中叶，欧洲科学家帕斯科首先用“概率”理论说明了风险的内涵，并给予了科学的解释。保险公司开展人寿保险业务时，要用概率论算出人们的预期寿命，以决定是否接受投保，防止赔钱。大约到了 19 世纪，“风险”一词常常用法文拼写，主要用于与保险有关的事情。

现在，英语词典对 Risk 的解释为：

1. a source of danger; a possibility of incurring loss or misfortune.

一个危险源，一种招致损失和灾难的可能性。

2. a venture undertaken without regard to possible loss or injury.

一种不注意损失和伤害的冒险。

现代意义上的“风险”，已经大大超越了“遇到危险”的狭义含义，可以扩展为“遇到破坏或损失的机会”。这里的“机会”是指可能性，而不是指“机遇”。可以说，经过几百年的演绎，随着人类活动复杂性的加剧，风险一词也越来越被概念化，并被赋予了更广泛、更深层次的含义。“风险”与人们的决策和行为后果之间的联系越来越紧密，并逐步成为人们生活中出现频率很高的词汇。

在2009年11月国际标准化组织（ISO）发布《ISO Guide 73：2009 风险管理——术语》之前，各种组织、各个行业对“风险”一词有着各种各样的定义和描述。但它们往往强调风险的危害性和损失，很少兼顾风险的机遇性和收益。所以，在日常生活中，风险常常指发生不幸事件的概率。换句话说，风险就是一个事件产生的人们不希望的后果的可能性。

企业在实现其经营目标的过程中，会遇到各种不确定性事件，这些事件发生的概率及其影响程度往往是事先无法预知的。这些不确定的事件将对企业的经营活动产生影响，从而影响企业目标的实现。这种在一定环境下和一定限期内客观存在的、影响企业目标实现的不确定性就是“风险”。

造成“风险”定义各不相同的主要根源是由于人们对风险的理解和认识程度不同，或对风险的研究角度不同。下面列举几种有代表性的观点。

第一种观点：风险是损失发生的不确定性。

这种观点又分为主观学说和客观学说两类。主观学说认为不确定性是主观的，是个人对客观事物的主观估计，是个人心理上的一种感觉，不能以客观的尺度来衡量。主观学说认为不确定性的范围包括发生与否的不确定性、发生时间的不确定性、

发生状况的不确定性以及发生结果严重程度的不确定性。客观学说以风险客观存在为前提，以风险事故表现为基础，通过数学和统计学观点加以定义，认为风险可用客观的尺度来度量。

第二种观点：风险是指可能发生损失的程度的大小。

这种定义流行于保险行业，他们认为风险可以引申定义为“预期损失的不利偏差”，其不利是针对保险公司或被保险企业而言的。

第三种观点：风险是事件未来可能发生的不确定性。

该不确定性可通过收益分布的方差测度。由于方差计算的便捷性，风险的这种定义在实践中得到了广泛的应用。

第四种观点：风险是指损失的大小和发生的可能性。

风险是指在一定条件下和一定时期内，由于各种结果发生的不确定性，导致行为主体遭受损失的大小以及这种损失发生可能性的大小。风险是一个二维概念，通过损失发生的大小与损失发生的概率两个指标进行衡量。

第五种观点：风险是风险构成要素相互作用的结果。

风险因素、风险事件和风险结果是风险的基本构成要素。风险因素是风险形成的必要条件，是风险产生和存在的前提。风险事件是外界环境变量发生始料未及的变动从而导致风险结果的事件，它是风险存在的充分条件，在整个风险中占据核心地位。风险事件是连接风险因素与风险结果的桥梁，是风险由可能性转化为现实性的媒介。

1.1.2　保险行业对风险的定义

保险行业将风险定义为“一种客观存在的损失的发生具有不确定性的状态”。该定义认为：风险是一种客观存在的状态，是一种与损失相关的状态。

在保险行业，风险的组成要素包括风险因素、风险事故和损失。

风险因素是指增加损失发生的频率或严重程度的因素，包括有形（物质形态）的风险因素和无形（非物质形态）的风险因素，如道德风险因素等；风险事故是指发生损失的直接原因；损失是指价值的消灭或减少。

保险行业把风险分为可保风险和不可保风险。可保风险是保险人愿意承保并能够承保的风险。判定可保风险的条件如下。

1. 风险确实存在，并且有发生重大损失的可能。如果不存在风险就不需要保险，或者如果风险发生后导致的损失小，当事人自己就可以承担，也就没有必要寻求保险保障。

2. 风险必须是意外的。针对某个单独保险标的而言，风险的发生是偶然的，并且不是故意行为导致的。风险必须是大量标的均有损失的可能，但是大量标的没有同时损失的可能。否则，保险人的生存就成了问题。只有发生大量可能遭受同样风险的事件，保险人才能估算其损失。

3. 风险必须是非投机性的。如果保险人承保投机风险，则被保险人可能因发生风险而获得保险赔款等利益。

4. 风险具有现实可测性。被保风险有可测性，保险人才可能通过测度厘定费率。

5. 保险成本必须具有经济性。如果为了避免此项危险，其所需保险费用过高，则会造成被保险人的沉重经济负担，这并非保险的本意。保险在于提供保障，而非影响生产，更不可能创造收益。

6. 合法性。保险所承保的标的必须合法，否则均不可保。

1.1.3 COSO 对风险的定义

COSO 在《COSO ERM——Integrated Framework》中这样定义“风险”：风险是一个事件将会发生并给目标实现带来负面影响的可能性。

COSO 认为事件对目标的影响可能是正面的，也可能是负面的，其中负面的代表风险，正面的被称为机会。为此，COSO 也给“机会”下了定义：机会是一个事件将会发生并给目标实现带来正面影响的可能性。

在 COSO ERM 整合框架中，ERM 是指“企业风险管理”。为了准确描述该整合框架，COSO 在给“风险”下定义之后，也给“企业风险管理”明确了定义。COSO 认为“企业风险管理是企业的董事会、管理层和其他员工共同参与的一个过程，应用于企业的战略制定和企业的各个部门和各项经营活动，用于确认可能影响企业的潜在事项并在其风险偏好范围内管理风险，对企业目标的实现提供合理的保证”。

要想“确认可能影响企业的潜在事项并在其风险偏好范围内管理风险”，就需要企业对风险进行科学、准确的评估。要想具备这种评估能力，企业需要不断努力，除建立必要的评估模型外，还要进行充分的信息采集和必要的分析计算。

COSO 把企业风险管理的目标定义为以下四个方面。

- 战略目标
- 经营目标
- 报告目标
- 合规目标

其中，战略目标和经营目标的实现并不总在企业的控制范围之内；报告的可靠性、合法合规性这两类目标的实现都在企业的控制范围内，其实现取决于企业内部相关活动执行得好与坏。

1.1.4　国际标准化组织（ISO）对风险的定义

ISO 对“风险（Risk）”的认识也是逐步完善的，这通过 ISO Guide 73“风险管理术语”标准在 2002 年和 2009 年的两个不同版本即可看出。

1. ISO Guide 73：2002 对风险的定义

Risk：Combination of the probability of an event and its consequence.

NOTE 1. The term "risk" is generally used only when there is at least the possibility of negative consequences.

NOTE2. In some situations, risk arises from the possibility of deviation from the expected outcome or event.

NOTE 3. See ISO/IEC Guide 51 for issues related to safety.

该定义认为：风险是某一事件发生的可能性（或概率）与其后果的组合。

注1，术语"风险"通常仅应用于至少有可能会产生负面后果的情况。

注2，在某些情况下，风险起因于与预期的后果或事件偏离的可能性。

注3，与安全有关的概念，参见ISO/IEC Guide 51。

2. ISO Guide 73：2009 对风险的定义

Risk：Effect of uncertainty on objectives.

NOTE 1. An effect is a deviation from the expected —positive and/or negative.

NOTE 2. Objectives can have different aspects (such as financial, health and safety, and environmental goals) and can apply at different levels (such as strategic, organization-wide, project, product and process).

NOTE 3. Risk is often characterized by reference to potential events and consequences, or a combination of these.

NOTE 4. Risk is often expressed in terms of a combination of the consequences of an event (including changes in circumstances) and the associated like-