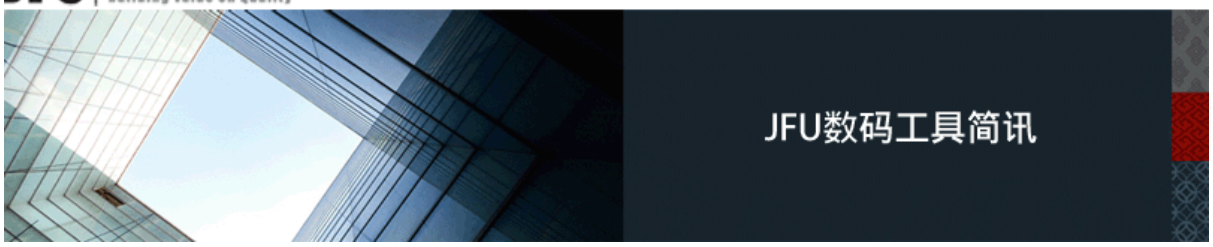

《JFU 注册会计师简讯》、《JFU 财税简讯》，以及《JFU 数字化工具简讯》，旨在分享我们针对执业过程中所遇问题的思考。免费订阅。如有垂询和评论，欢迎联系 JFU 简讯编辑邮箱，enquiries@jfuconsultants.com

我们即将开放自行研发的云端企业风险管理系统。倘贵机构有意藉此建立企业合规管控体系，请于 JFU 在线登记网页登记您的参与意向，可免费试用，名额有限。

订阅 JFU简讯　注册 风险管理系统　查询　分享 转发给别人

管理风险的方法
来源：JFU ｜ 数码工具
2021 年 9 月 28 日

正如我们在上期简讯里讨论的，企业可以用二维网格将企业具备的独特能力与其面临的风险匹配起来，以此规划发展方向。实现的方法有优势、劣势、机会和威胁分析、动态能力和企业风险管理。本期简讯重点讨论风险管理。风险来自于变化或不确定因素，可以是上升的机会，也可以是下滑的危险，取决于如何预测、应对和管理风险。

我们怎样发现、分析和监控风险？

直觉方法

不具备正式的企业风险管理系统的话，大部分企业会使用直觉方法。为阐明直觉方法，我们来看一下人体。

我们的身体是一个复杂但有条理的系统，能消解食物，将营养转化为能量，排出糟粕，完成必要的功能。眼、鼻、耳、口和皮肤整合在一起，组成了一个感官系统，能发现周围的变化。当有变化发生时，我们的大脑则收到警告，有意识或无意识地判断引起变化的因素。通过考虑和凭直觉作出的决定会发出命令，让肌肉做出反应，同时感官继续监督反馈。通过这个过程，我们一边学习、一边适应变化、一边进化，这是智能生物的特殊本领。

身体管理风险的方法是一个三阶段的直觉过程：（1）感官系统首先发现变化，然后发出警报，（2）相关的身体程序接收和分析警报，（3）最后再发配机制将指令发送给相应的器官，执行调整和监督反馈。

进化展示的是一个卓有成效，但效率极低的过程。依靠直觉的方法，取得进步要经历缓慢的试验和失误。人类的进化确实比其他动物的要成功，但在物竞天择的过程中，很多个体做出了牺

牲。把这个比喻用于企业，如果仅仅依靠缓慢的、增量的程序找寻恰当的应对方法，个别部门或整个企业都可能因不确定的市场因素而衰败。要避免消亡在这个过程中，唯一明智的做法是，通过重点学习、研究，以及配备精密的工具，进行技术革新，从而取得精细化的方法。

我们在执业过程中观察到，很多企业，包括资源丰富的跨国公司和上市公司，仍在依赖直觉和相对原始的工具管理企业风险，比如依靠指导原则、实操手册、员工纪律、老手经验和内部审计。

几年前，一些政府部门和知名企业被要求解释，为什么在承包商没有提交关键节点的审核或测量要求的情况下，仍然允许上马一些重大基建项目。就在几个月前，一家大开发商通知购房户推迟迁入新居。由于后期才发现工程使用了不合标准的材料，整个建成的高层建筑都需要拆毁重建。大量实例表明，学习是一个缓慢的过程，失误要付出沉重的代价，重建声誉不是一朝一夕的事情。

很多司法管辖区的监管部门强制规定，上市企业要设计和执行恰当的风险管理体系。是时候了，企业界应该开始认真地考虑建立风险管理框架。参考的技术标准已经具备，由制定标准的机构制定，包括 ISO31000 风险管理标准和 COSO 内部控制框架（2017），这些机构长期呼吁加强管理企业风险。

ISO31000 风险管理方法

ISO 31000 风险管理标准属于 ISO 标准的一部分，由国际标准化组织开发，旨在帮助提供高质量的服务，保护客户，降低风险和减少浪费，等等。该组织的网站将这些标准描述为“如求最佳做事方法的公式”。ISO 标准可以用于制造产品、管理程序、交付服务，或提供原料。我们特指的是 ISO31000 风险管理标准，内容包括运营的持续性、经济恢复力、专业声誉、环境和安全效果。

原则

ISO 31000 风险管理标准认为，风险管理应该是：

- 企业所有活动的整合体；
- 有架构的综合体系；
- 按企业的环境和目标定制；
- 包含所有利益相关者，可以使其提供观点，分享知识；
- 勇于发现和应对变化；
- 基于有关过去、现在和将来的信息，顾及局限性和不确定性；以及
- 清晰和及时地提供给有关利益相关者

人们认识到，风险管理在执行的各个层次和阶段，都会受到人的行为和文化的影响。ISO 31000 风险管理标准认为，风险管理是个互动的过程，需要通过学习和经历不断得到改善。达到风险管理的目的——保护和创造价值，坚持这样一套原则是根本。

框架

ISO 31000 风险管理标准是一个框架，指导企业将风险管理整合进整个企业的活动和功能中。

框架列出 5 阶段反复互动的程序，建立和维护风险管理业务。

1. 整合
2. 设计
3. 执行
4. 评估
5. 改进

有效的风险管理需要监管部门和领导层的投入，这样，资源得以运用在全公司范围内，工作、策略、目标可以统一起来。

程序

ISO 31000 风险管理标准提出，要将风险管理的程序整合成管理和决策不可分割的一部分，也要整合进企业所有层面的结构、运营和程序中，不管是策略方面，战术方面，运营方面，还是交易方面，贯穿所有程序和项目。**示意图 D** 显示，风险管理程序具有六个基本组成部分。

- 企业范围内的沟通将所有利益相关者整合在一起；
- 确定定制的范围和内容；
- 定义风险标准和统一的目标；
- 为发现、分析和评估风险的三步程序培养风险能力；
- 发展风险处理能力，设计处理风险的选项；以及
- 监督进展和反馈的能力。

COSO 内部控制框架（2017）方法

这里特指 COSO 对风险管理关注的中心点，又叫做 COSO 企业风险管理。COSO，或发起人委员会，负有使命，要帮助企业发展领先思想，用于加强内控，管理风险，改善管治，防止欺诈，从而提高企业的绩效。虽然 COSO 的风险管理理念和方法跟 ISO31000 风险管理标准提倡的类似，但 COSO 表达的方法颇为不同，使得风险管理同策略和绩效整合在一起的重要性更显而易见。

COSO 将企业风险管理定义为一个框架或程序，包括五个部分，排列在双螺旋线中，非常像 DNA 分子。大家知道，DNA 是存在于每个活细胞里的链状分子，引导生命体中细胞的形成、生长和再生。这个概念表明，风险管理必须嵌入企业的功能部门，运作在企业价值链的每一段。

- 愿景
- 策略
- 目标
- 绩效
- 绩效

只有通过这种整合，才能证明 COSO 的企业风险管理能够卓有成效地指导每个部门，支持企业的全部生产和发展。COSO 的企业风险管理概念和五个风险管理组成部分在**示意图 E** 里表示。

将概念付诸实践

从风险管理专业人员的角度看，结合 ISO31000 标准提倡的内容和 COSO 的概念和组成部分，有助于研究风险管理。二个方法目的相似，但表达的方式不同。

COSO 强调风险管理程序同管治、策略以及企业其他方面的整合。类似于 DNA 的比喻，COSO 方法的重点是，把风险管理贯穿于组织内的所有监管职能。

相反，ISO31000 风险管理框架具有很强的结构性。框架具有三步风险评估程序——发现、分析和裁定——结合另外的部分，风险应对、监控和报告。

本期简讯是企业风险管理概述，下一期我们将讨论如何将概念付诸实践。

示意图 D

ISO31000 风险管理流程

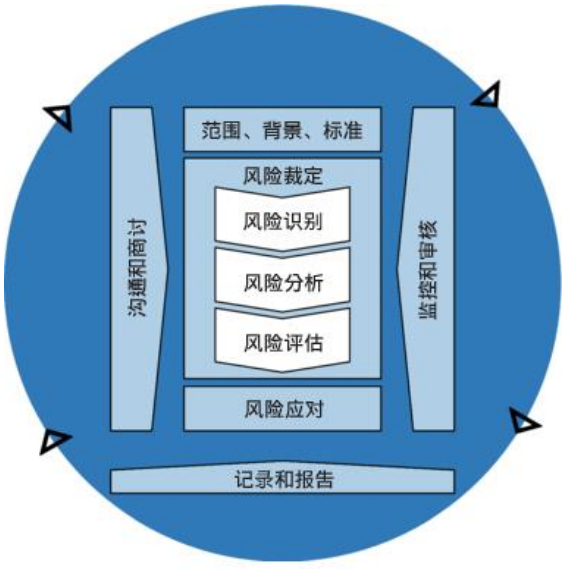

图 4 - 流程

示意图 E

COSO 企业风险管理组件