ACCESSING IT RISKS

评估 IT 风险

Dutch Fayard and Nishani Edirisinghe Vincent
丁成宁 译，詹庆娥 校

管理会计师拥有充足的经验和能力，能够对监测和评估 IT 风险进行绩效评价。

大多数公司利用技术收集、处理、存储、访问和交流对战略决策有用的信息。保持信息安全是至关重要的，优步（Uber）、艾克飞（Equifax）、塔吉特（Target）、美国民主党全国代表大会（the Democratic National Convention）、摩根大通（JPMorgan Chase）等许多大公司的网络安全事件被广泛报道就证明了这一点。然而，网络安全只是诸多信息技术（IT）风险之一。其他重要的 IT 风险可能源于丧失利用技术获取竞争优势的机会、技术缺陷、内部控制缺失，以及雇员疏忽。

IT 风险可能来自不同职能领域的各种内外部环节。IT 风险中只有一小部分是由技术故障造成的。大多数信息系统漏洞来自整个公司范围内严密控制的活动中的忽视或疏忽，如未能防止未经授权就进入保密领域，或雇员将个人智能手机连接到公司的 Wi-Fi 网络中。像富国银行（Wells Fargo）的员工创建欺诈帐户这样的内控失败，就是一个 IT 的应用增加了业务和 IT 风险的案例。而达美航空（Delta Airlines）因亚特兰大火灾造成系统故障，取消了 1,800 多个航班，这是其他功能区域故障如何增加 IT 风险的例子。

通过适当的关注，管理层可以主动衡量 IT 风险，在实现 IT 提供的众多价值优势的同时降低其风险。

许多企业目前采用的两个风险评估框架是 COSO（美国反虚假财务报告委员会下属的发起人委员会）的《内部控制——综合框架》（*Internal Control—Integrated Framework*），以及由 ISACA（美国信息系统审计和控制协会）制定的“信息和相关技术控制目标”(COBIT) 框架。（参见 50 页的专栏“风险框架”。）虽然这两个框架都验证了我们的建议，即公司应该主动评估它们的 IT 风险，但他这两个框架都没有提供切实可行的方法。

我们建议，管理会计掌握必要的技能来实施并监控整个企业现有或新开发的 IT 风险评估，从而在辅助 IT 风险管理方面发挥重要作用。这一任务利用了管理会计师在绩效评估方面的专长，又同时绕过了公司可能使用的各种 IT 平台所需的特定知识。依据 COSO 框架的建议，通过管理细分后的价值链区域，可以实现公司运营的实体风险管理。下面，我们提供了与价值链主要活动和支持活动相关的 IT 风险评估基本表。

主要活动

主要的价值链活动包括内向物流、运营、外向物流、市场营销和销售以及服务。表 1 包含了这些领域绩效评估的目标和管理会计师可以实施的建议指标，以帮助评估这些领域的 IT 风险。

内向物流包括与接收、存储和分配操作输入有关的所有活动。这项活动的一个关键成功因素是公司与供应商的关系。在供应商管理的库存系统和 / 或电子数据交换 (electronic data interchange，EDI) 等领域使用信息技术来与供应商进行沟通，这就需要评估内部物流的 IT 风险。管理层可能希望监控 IT 在供应商关系管理和理解风险方向的有效性。

运营包括将投入转化为产出的活动。IT 是标准化

实施绩效评估

建议实施的措施涉及与管理会计师在其他职能领域采取措施时经常做的工作类似的工作和流程识别关键领域（主要和 / 或次要活动、与业务相关的流程、使用的应用程序，以及在活动中存储的数据和信息）。

- 确定的关键业务、流程、应用程序、数据和信息进行优先级。
- 制定关键领域的绩效目标清单。
- 评估是否可以扩充或修改现有的绩效指标以达到绩效目标。
- 制定新的绩效衡量标准，以实现绩效目标。
- 评估建议的新的或修改后的绩效衡量标准的成本和收益。
- 识别数据收集点，建立收集数据的流程。
- 识别数据所有者，并建立一个向 IT 报告数据的流程。
- 收集、监测和改进绩效评估。
- 使用相同的实施流程，在不太关键的领域建立绩效评估标准。

表 1: 主要活动的绩效评估

活动类型

目标

■绩效评估

内向物流

衡量供应商的绩效，确保供应商在满足当前的业务需求的同时解决 IT 风险。

■经 EDI 发送、与采购订单相关的交付错误百分比

■采购订单发送到供应商与每个供应商按照期限使用 EDI、电子邮件、传真等方式交货之间的平均滞后时间

■与存货移动频率相比，每个时期从供应商到库存系统的访问尝试次数，以确定供应商对库存的监控是否充分。

衡量在供应链管理中使用技术的准确性、完整性、真实性和可靠性

■在一段时间内使用 EDI 失败的通信次数

■每个周期出现错误的采购订单的数量

■每个周期从供应商到库存系统的访问失败次数

■每个周期对库存系统的不明身份外部访问次数

衡量 IT 依赖度及对内向物流的影响

■与系统故障有关的缺货数量

■手工采购过程导致的错误百分比与 EDI 或供应商管理库存采购导致的错误百分比

运营

衡量使用 IT 的运营效率

■比较每个产品 / 作业 / 订单的预算与实际成本

■系统停机时间对生产延迟（生产的产品数量、延迟交付的小时数、天数等）的影响

■由于数据输入错误造成的缺陷数量；由于系统故障 / 校准引起的缺陷数量。

衡量内部控制的适当性

■在正常工作时间之后，从不同的工作站等远程访问应用程序的人数

■在正常工作时间内从不同工作站远程访问工作站、网络、应用程序等失败的次数

外向物流

衡量 IT 性能

■每个时期在线订单百分比

■每个时期的不完整在线订单百分比

■由于系统故障造成的运输延迟的百分比

■由于在采摘和包装产品中使用技术，减少的时间百分比

■计划与系统故障相关的装运错误百分比

■每个时期取消的在线订单数量

■处理订单的时间

衡量敏感数据的安全性

■每个周期系统中的主管 / 手动覆盖次数

■尝试访问运输和库存系统的失败次数

■在正常工作时间以外访问敏感数据的次数

市场营销和销售

识别潜在的数据泄露，并评估数据泄露对客户信息的影响

■从不同的工作站，办公时间之后等远程访问客户主数据的失败次数

■变更员工、日期、变更类型等客户主数据的次数

■基于丢失的事务数量和恢复系统所用时间的系统故障成本

■正常工作时间内和之后的数据库表访问模式的偏差

■使用敏感数据访问数据库表的事务、雇员和设备的数量 / 百分比

评估 IT 对营销工作的影响

■在线销售百分比

■与在线销售 / EDI 相关的收益百分比

■来自社交媒体站点的网站流量：每站网站 / 周期 / 产品

■来自社交媒体广告的销售订单百分比

■基于大数据分析确定的新模式进行的营销工作的销售量

■与在线营销活动相关的特殊定价谈判客户的百分比

服务

评估 IT 风险漏洞

■每个周期通过移动设备登录账户的平均客户数

■每个周期客户通过移动设备访问账户的平均频率

■已下载移动应用程序（APP）的客户百分比

■来自移动设备的查询百分比

■显示按时间段使用移动应用程序的地理图

表 2: 支持活动的绩效评估

活动类型

目标

■绩效评估

公司基础架构

衡量 IT 相关问题的沟通效果以及 IT 功能的有效性

■ CEO 和 CIO 之间的沟通数量

■每个项目、每个时期的业务部门经理和 IT 经理之间的沟通次数

■提交 IT 帮助平台的 IT 问题数量与部门内处理的 IT 问题数量比

衡量管理层（和 / 或董事会）对 IT 风险的监管是否足够

■管理议程中与技术有关的项目百分比（与项目总数相比）

■与讨论技术相关问题的时间相比，花费在管理会议上的总时间所占的百分比

■跟策略有关的技术项目百分比与跟风险有关的技术项目百分比

衡量合规要求

■合规性要求每个周期更新的次数

■每期的正式申报数量

■因技术问题产生的延迟申请百分比

■不符合要求的技术相关项目百分比

衡量系统故障时恢复的能力

■目标恢复时间（公司在没有信息系统的情况下愿意运营的时间长度是多少？以小时数 / 交易笔数计）

■恢复目标值（公司能丢失多少数据？以小时数 / 交易笔数计）

■灾难恢复计划所涵盖的应用程序数量

■将模拟中恢复的时间与目标恢复时间比较

技术开发

衡量业务单元的参与度

■ IT 项目中非 IT 人员的数量

■与非 IT 项目成员会议的次数

■与业务部门的会议 / 沟通次数

控制 IT 投资

■比较迄今为止发生的成本百分比和项目完工进度百分比

■ IT 预算和预测：责任会计报告

采购

衡量第三方 IT 供应商的表现

■每个 IT 供应商每个周期、每个应用程序的预定和意外系统停机数量

■与正式供应商沟通的百分比

■与第三方应用程序相关的安全问题的数量

■与第三方应用程序相关的内部控制缺陷的数量

■与第三方应用程序关联的不合规项目数量

人力资源

衡量储备的 IT 知识水平

■在知识管理系统中具有解释 / 解决方案的完整工作的数量

■每个项目里程碑的文档修订频率

■每个用户每个时期为解决问题，访问知识管理系统的频率

衡量 IT 专业人才的充分性

■每个项目、每项技术、每个周期的 IT 专家数量

■因 IT 专家调度冲突导致的项目调度延迟数量

■每个项目、每个周期的 IT 人员数量

■因缺少 IT 人员而导致的调度延迟数量

衡量培训需求

■在受聘的第一周所需 IT 相关培训课程的数量

■需要在随后完成的重复训练课程百分比

■需要后续培训课程的频率

■对公司所使用的 IT 员工教育与现有技术培训的差距分析

衡量来自员工活动的漏洞

■每个电子邮箱中的垃圾邮件数量

■每名员工、每个周期的网站流量和下载使用公司网络的频率

和自动化流程的重要推动者，可以降低成本，提高效率。管理层可以通过衡量 IT 支出如何帮助实现企业和运营目标来获益。此外，寻求《萨班斯—奥克斯利法案》合规的管理层可以评估是否存在任何重大的内部控制缺陷，以及控制缺陷对管理决策的影响。因此，管理会计师应当了解内部控制的重要性，并提供绩效措施来监控和使用生产计划、预算编制和预测有关的业务申请。

出厂物流包括订单处理、存储、运输、向客户分配产品或服务等活动。在出厂物流方面，管理层一般都着眼于降低仓储和运输成本。与出境物流相关的两大风险是性能不佳和未经授权披露敏感数据。为了解决这两种风险，管理会计师应该全面了解数据获取和存储的时间、地点和方式。这将为数据库查询提供适当的知识，以获取决策需要的必要信息，并保护敏感数据。

市场营销和销售与说服客户购买商品或服务以及从客户那里收取现金的流程相关联。公司面临的挑战是使用新兴技术，如社交媒体、大数据、移动营销等，以吸引潜在和现有的客户。因此，管理层希望尽量减少对公司信息系统潜在威胁的影响和可能性，同时利用新兴技术吸引新老客户，管理会计师可以实施所建议的绩效衡量标准，以通知管理层 IT 在营销和销售方面的状态。

服务是与产品质保和售后服务相关的活动。服务包括提供客户支持、保修服务、响应客户查询和培训等活动。这些活动的目标是提升客户体验，从而增加未来的销售额、提高客户满意度以及推荐。卓越的客户支持的能力取决于提供给客户的服务质量。许多公司正在引入在线账户管理、聊天服务以及访问客户账户的移动应用程序，以提高客户满意度。尽管这些服务可能会对客户体验产生积极影响，但通过未知网络连接的客户、安装未知的其他移动应用程序以及在设备上设置较低的安全级别会给公司网络、操作系统和数据库造成漏洞。

支持活动

价值链的支持活动包括公司基础架构、技术、采购和人力资源。表 2 包含了绩效衡量目标和这些领域的建议指标。

风险框架

ISACA 发布的 COBIT

COBIT 由 ISACA 开发，是领先的 IT 治理和管理框架。 COBIT 将 IT 标准（如 ITIL，CMMI 和 ISO 17799）整合到一个全面的 IT 治理框架中，定义了七个 IT 启动器（enabler）：

（1）准则、政策和框架；
（2）流程；
（3）组织结构；
（4）文化、道德和行为；
（5）信息；
（6）服务、基础设施和应用程序；
（7）人员、技能和能力。

COBIT 建议，通过提出四个问题，公司可以评估和监控 IT 启动方案的绩效并监控 IT 风险：

1. 利益相关者的需求是否被解决?
2. 是否实现了促成者的目标?
3. 启动器的生命周期是否被管理?
4. 良好实践是否得到应用?

请访问网址 **www.isaca.org** 了解更多信息。

COSO 的《内部控制——综合框架》

内部控制整合框架最初于 1992 年由 COSO 发布，并于 2013 年更新，为设计、实施和实施内部控制及评估内部控制的有效性提供指导。

该框架包含了内部控制的核心定义，并详细说明了评估内部控制系统有效性的五个要素：**控制环境、风险评估、控制活动、信息和沟通，以及监控活动。**

它还概述了 17 个原则和支持属性，这些原则和支持属性进一步支持组织开发决策，以在快速变化的环境中管理风险和提高绩效。请访问 **www.coso.org** 了解更多信息。

公司基础架构包括所有支持功能，如会计、法律（如合规）、行政管理和一般管理。这些相同的功能被 COBIT 确定为 IT 推动者的“组织架构”，它们代表了公司的关键决策实体。当这些支持部门的经理积极考虑 IT 如何为公司增加价值时，公司可以获得竞争优势。但是，当管理人员无法有效地考虑所有风险因素时，支持部门的经理们单独考虑 IT 选用和 IT 风险的程度以及与其他管理者的沟通能够影响公司的 IT 风险。功能支持部门之间强大的沟通渠道以及公司管理层或董事会提供强有力监督承诺提高关键决策者的风险意识，形成更有效的政策和流程，将最终降低 IT 风险。一旦出现问题，强有力的沟通渠道也能够提高公司的快速恢复能力，并修改政策以避免将来出现的问题。

技术开发涉及通过有效利用技术来管理 IT 投资和提高效率。管理层可以跟踪当前项目的状态，以确定公司是否将 IT 与其业务战略结合起来。影响项目成功的一个重要因素是 IT 经理为满足业务需求与业务部门经理有效沟通 IT 目标的能力。建议的性能指标可以用来查找 IT 项目的当前状态，识别遇险项目，并查看该公司是否正在实现业务与 IT 的整合。

采购包括公司用于获取运营所需资源的流程。监测第三方 IT 供应商的表现是涉及采购的主要活动。由于对第三方的依赖性增加，公司不能忽视与供应商相关的主要活动风险。因此，高级管理层应关注主要 IT 供应商相关的风险，以及这些风险对企业目标的影响。

人力资源包括招聘、培训、激励、奖惩和留住员工。管理层将担心 IT 专业人员的充分性，员工对 IT 风险的意识，以及 IT 风险问题培训的必要性。随着企业对信息资产的保护，对技术的依赖性日益增长，对信息系统的威胁也越来越大，这给企业带来了沉重的负担。技术的复杂性及其不断的变化不仅需要特定的技术知识，而且需要跟上这些变化的能力。即使在实施了最新的安全技术之后，人为因素也使得信息系统容易受到网络钓鱼、垃圾邮件、欺骗、病毒等安全漏洞的攻击。员工应该接受关于电脑滥用技术的教育，以便他们意识到自己的行为可能会导致安全破坏活动的实现。

随着对 IT 日益依赖，IT 对日常运营的影响增加，IT 风险管理的责任已经成为整个公司面临的一个问题，

全公司层面的关注

随着对 IT 日益依赖，IT 对日常运营的影响增加，IT 风险管理的责任已经成为整个公司面临的一个问题，这不仅仅是 IT 人员的责任。管理会计师应该在设计、执行和监控绩效措施中利用他们的专业知识，并报告 IT 风险。我们提供的建议措施应当是管理会计师所熟悉的，并且可以很容易地用来评估和监控整个公司的 IT 风险。我们要强调的是，这并不是一个详尽的清单。正如 COBIT 所建议的那样，通过识别价值链活动中的风险问题，并提出一些绩效评估方法，从整体角度出发审视，但这些措施可能因公司的 IT 运用水平、管理层的风险承受能力和风险偏好而有所不同。鉴于管理会计师在衡量 IT 风险方面可能一开始并不乐观，该列表旨在考虑类似绩效指标如何扩展、修改，以捕捉技术性能各方面的信息，从而及时识别并定位 IT 风险领域。**SF**

Dutch Fayard，博士，美国田纳西大学查塔努加分校的会计学助理教授，也是 IMA 查塔努加分会的会员。联系方式：dutch-fayard@utc.edu。

Nishani Edirisinghe Vincent，博士，美国田纳西大学查塔努加分校的会计学助理教授。

联系方式：surani-vincent@utc.edu。