利用COBIT工具包做基于风险的抽样审计

文／RuneJohannessen　译／崔梦漫

在本文中，我把自己在工作中利用COBIT(“信息与相关技术控制对象”，ControlObjectivesforInformationandrelatedTechnology的缩写工具包获得的一些有用的经验介绍给大家。我介绍经验并不是想使之成为基于风险的审计执行模板，我是针对一种可能的审计方法提出一种尝试性的建议。

目前，有很多公立和私立机构使用COBIT工具包，并且，我可以相当自信地说，任何使用过此工具的人都认为它相当全面，而它的使用也相当耗时，这与我们日常工作的情形相左。在我们的工作中，时间是一个关键的因素，我们往往没有多少时间执行委派给我们的任务。所以说，在我们给定的时间框架内，选择最重要的范围和过程并且确定最高的风险，以便为我们的客户提供最大的附加价值，这是很重要的。

我认为，COBIT工具包并未针对如何执行全面的(或高级的审计风险评估，或者说如何选择最重要的范围和(或过程进行审计提供清楚的指导。所以，我用执行审计周期的一个通用模型来说明我的解决方案。我的方法是基于定性评估，相对于审计客户来说，它具有相当的灵活性，表示如下：

第一阶段基于目标、过程、资源做出选择

这一阶段包括确定焦点对准什么,哪一个会成为范围、过程、IT资源的样本和(或信息条件的样本。根据所选择的优先级，审计人员获得一个可能与更深层次的审查有关的过程列表。在下面的例子中，我想就“资料获取与审计执行”这一领域来说明这一点。在这个领域，“改变管理”与“软件的获得与维护”这两个过程对审计客户非常重要，所以它们作为与审计相关的过程被选择。

第二阶段对所选择的过程做风险评估

作为第一阶段选择的结果，审计人员现有一个赋予了不同优先级的过程样本。在上面的例子中，A12和A16被认为是在“资料获取与审计执行”这一领域内相关的。由于时间和资源受限的结果，往往有必要进一步限制工作量。在第二阶段，审计人员再一次对第一阶段选择的过程排列优先级，然后选择那些具有最高风险的过程。我举案例A16的情况说明这一点，在这个例子中，审计人员对于在第一阶段中选择的每一个过程都要完成下面的表格。

这张表格列出了与每个过程有联系的一些控制问题。这些问题可以从每个过程的第一页上“值得考虑的问题”标题下列出的各种问题中得到。以一个样本为基础，审计人员阐明一些一般性的控制问题。这些问题旨在对于这一领域中所使用的程序、文档和过程有一种“感性认识”。回答样本问题所需要的信息可以通过面谈和对正在使用的程序的观察收集到。在这一阶段，审计人员并不对可用资料的内容和质量进行评估。

控制程序栏目应标记为“已归档、未归档、未知”。以下条件可被用于回答这些问题：

等级控制程序已归档被审计的实体有处理此事的程序、过程或文档。未归档被审计的实体没有处理此事的程序、过程或文档。

下一步涉及到对在一个过程中存在错误、漏洞的可能性做全面评估。在开始，这个评估会对过程有一个初步的回顾，有审计人员自己的观点，审计人员应该把可能产生负面影响内部和外部的因素包括进去。结果用具有以下级别的矩阵来表示：

等级 可能性

高级 这个过程会受到内部或外部事件的负面影响的可能性很大。

中级 这个过程有可能受到内部或外部事件的负面影响。

低级 这个过程会受到内部或外部事件的负面影响的可能性不太大。

下一步是评估产生负面影响的事件的后果。除任何金钱损失以外，诸如荣誉、工作环境等因素也应该加以考虑。

等级 可能性

高级 预计有负面影响的内部和外部事件会对此过程有主要影响。

中级 预计有负面影响的内部和外部事件会对此过程有中等程度的影响。

低级 预计有负面影响的内部和外部事件会对此过程有次要影响。

用这种方法，通过把可能性与后果一起考虑，每个过程都能得到风险评估。在给过程定风险等级(高、中、低)的基础上，选择一个样本用在下面的IT审计阶段。

第三阶段IT审计

利用COBIT“审计指南”，对认为有最高风险的过程执行IT审计。

我希望这些观察和建议会有助于用COBIT工具包进行基于风险的审计方法的开发。我也希望我的这篇文章会鼓舞其他人介绍他们的经验，描述他们使用此工具的情况。

作者简介：

本文作者RuneJohannessen是挪威审计署高级审计顾问，他在挪威审计署从事IT审计和审计方法的开发。Rune在内部审计、财政审计、IT审计和IT项目中的质量保证等领域有7年的工作经验。在进入挪威审计署之前，他在一家从事系统开发项目和IT安全质量保证的机构(PricewaterhouseCoopers作高级顾问。Rune从挪威管理学校获得管理学士学位、从奥斯陆大学获得更高的学位，他还获得了CISA和CIA认证。

COBIT:

ISACA开发的COBIT工具包，为管理人员、用户、信息系统(IS审计、控制和安全从业人员提供一个参考框架，对于良好的信息技术安全和控制业务来说，它是普遍可用、可接受的标准。

COBIT包含以下主要产品：

框架：一个成功的机构是建立在数据与信息的坚实框架基础上的。这个框架诠释了IT过程如何分发企业为实现其目标所需要的信息。此分发是通过34个高级控制对象来控制，一个IT过程有一个控制对象，这些控制对象包含在4个域中。此框架识别哪一个信息条件以及哪一种IT资源对于IT过程完全支持企业目标是重要的。

管理指南：要确保一个成功的企业，你必须有效地管理商业过程和信息系统的一致。这个新的管理指南由成熟模型、关键的成功因素、关键的目标指示器和关键的性能指示器组成。这些管理指南将有助于回答所有与企业成功休戚相关的那些人最关心的问题。

详细的控制对象：在一个技术上不断变化的环境中维持盈利的关键是你能在多大程度上保持控制能力。COBIT的控制对象为IT控制提供描述一个清楚的策略和好的做法所需要的洞察力。此工具中还陈述了通过实施318个特别详细的控制对象，实现想要达到的目标等有关内容。

审计指南：有分析、评估、解释、做出反应与实施等几部分内容。要实现你想要的目标，你必须不断地、始终如一地审

计你的程序。审计指南略述并建议当控制对象的风险条件不满足时，执行相应于每一个高级IT控制对象的实际活动。

实施工具集：一个实施工具集，包含管理意识和IT控制诊断、实施指南、经常提出的问题、来自正在使用COBIT的机构的案例研究和可用于把COBIT介绍给机构的幻灯演示。设计此工具集为有利于COBIT的实施，便于向快速而成功地应用。COBIT在其工作环境中的机构学习相关的经验，并且可在选择实施选项过程中起辅助管理作用。

摘自《国际审计纵横》

协会地址：北京市海淀区中关村南大街4号
联系电话：010-82199846/47 电子邮件:xinxibu@263.net