BS7799标准及其在中观信息系统审计中的运用

刘国城

(南京审计学院 金审学院,江苏 南京 211815)

[摘 要]在分析中观信息系统风险与损失的成因基础上,借鉴BS7799标准,一方面从物理层次与逻辑层次两个方面研究中观信息系统固有风险的评价模式;另一方面从一般控制与应用控制两个层面探索中观信息系统内部控制的评价机制。基于BS7799标准对中观信息系统审计进行研究,旨在为IT审计师有效实施中观信息系统审计提供应用指南。

[关键词]BS7799标准;中观审计;信息系统审计;内部控制;中观信息系统;中观信息系统风险

[中图分类号]F239.4 [文献标识码]A [文章编号]1004-4833(2012)03-0050-07

所谓中观信息系统审计就是指审计主体依据特定的规范,运用科学系统的程序方法,对中观信息系统网络的运行规程与应用政策实施的一种监督活动,旨在增强中观经济主体特定信息网络的有效性、安全性、机密性与一致性,以保障中观信息系统的高效运行[1]。中观信息系统的审计主体即IT审计师需要重视中观信息系统审计的复杂性,且有必要借助BS7799标准,构建并完善中观信息系统审计的实施流程,优化中观信息系统审计工作,提高审计质量。之所以需要借助BS7799标准,是因为BS7799标准的众多功能可以满足中观信息系统审计工作的需求。在尚未有详细信息系统审计(以下简称"IS审计")规范的条件下,中观信息系统审计对信息安全管理策略的需求巨大,而BS7799标准恰恰是问世较早且相对成熟的信息安全管理标准,它能够确保在计算机网络系统进行自动通信、信息处理和利用时,在各个物理位置、逻辑区域、存储和传媒介质中,较好地实现保密性、完整性、有效性与可用性,能够在信息管理与计算机科学两个层面加强信息安全管理向中观信息系统审计的理论转化,中观信息系统审计的需求与BS7799标准的功能具备整合的可行性。

一、BS7799标准

1995年,英国贸工部制定了世界首部信息安全管理体系标准"BS7799-1:1995《信息安全管理实施规则》",并作为各类组织实施信息安全管理的指南[2],由于该标准采用建议和指导的方式编写,因而不作为认证标准使用;1998年,英国又制定了信息安全管理体系认证标准"BS7799-2:1998《信息安全管理体系规范》",作为对组织信息安全管理体系进行评审认证的标准[3];1999年,英国再次对信息安全管理体系标准进行了修订,形成"BS7799-1:1999"与"BS7799-2:1999"这一对配套标准;2000年12月,"BS7799-1:1999"被ISO/IEC正式采纳为国际标准"ISO/IEC17799:2000《信息技术:信息安全管理实施规则》",此外,"BS7799-2:1999"也于2002年底被ISO/IEC作为蓝本修订,成为可用于认证的"ISO/IEC《信息安全管理体系规范》";2005年,BS7799-1与BS7799-2再次改版,使得体系更为完善。BS7799

[收稿日期]2011-03-24

[基金项目]教育部人文社会科学研究规划项目(10YJA790182);南京审计学院校级一般项目(NSK2009/B22);江苏省优势学科"审计科学与技术"研究项目

[作者简介]刘国城(1978—),男,内蒙古赤峰人,南京审计学院讲师,硕士,从事审计理论研究。

标准体系包含 10 个管理要项、36 个管理目标、127 个控制目标及 500 多个管理要点。管理要项如今已成为组织实施信息安全管理的实用指南;安全控制目标能够帮助组织识别运作过程中影响信息安全的因素。BS7799 - 1 几乎涵盖了所有的安全议题,它主要告诉 IT 审计师安全管理的注意事项与安全制度。BS7799 - 2 详细说明了建立、实施和维护信息安全管理的要求,指出组织在实施过程中需要遵循的风险评估等级,从而识别最应该控制的对象并对自身需求进行适当控制。BS7799 - 1 为信息系统提供了通用的控制措施,BS7799 - 2 则为 BS7799 - 1 的具体实施提供了应用指南。

国外相对成熟的信息安全管理理论较多,它们各有千秋,彼此之间相互补充且有交叉。BS7799 标准仅是众多信息安全管理理论中的一种,与传统审计方法相比,仅适用于 IS 审计范畴。然而,BS7799 标准的特别之处表现在:其一,它是一部通用的信息安全管理指南,呈现了较为全面的系统安全控制措施,阐述了安全策略和优秀的、具有普遍意义的安全操作方法,能够为 IT 审计师开展审计工作提供全程支持;其二,它遵循“计划 - 行动 - 控制 - 改善方案”的风险管理思想,首先帮助 IT 审计师规划信息安全审计的方针和范围,其次在审计风险评估的基础上选择适当的审计方法及风险控制策略并予以实施,制定持续性管理规划,建立并运行科学的中观信息系统审计执行体系。

二、中观信息系统的风险与损失

中观信息系统风险是指成功利用中观信息系统的脆弱性或漏洞,并造成系统损害的可能性。中观信息系统风险极其庞杂且非常普遍,每个中观信息系统面临的风险都是不同的,这种风险可能是单一的,也可能是组合的[4]。中观信息系统风险包括:人员风险、组织风险、物理环境风险、信息机密性风险、信息完整性风险、系统风险、通信操作风险、设施风险、业务连续性风险、法律风险及黏合风险(见图 1),它们共同构成了中观信息系统的风险体系,各种风险除具有各自的特性外,有时还可能相互作用。

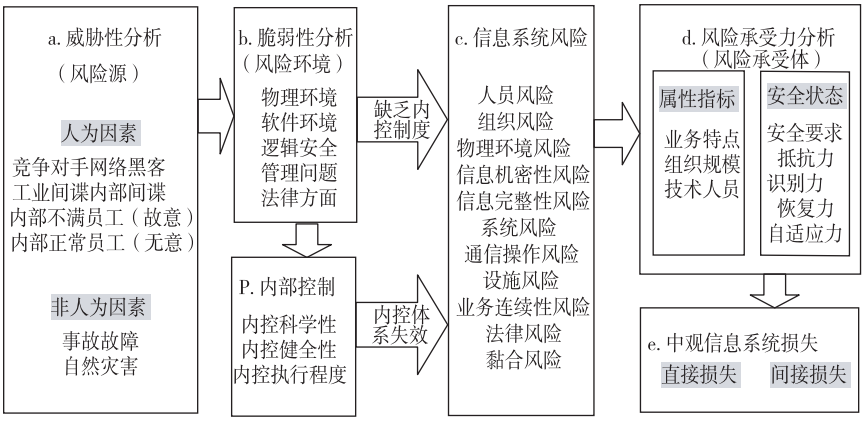

图 1　中观信息系统风险的作用机制

中观信息系统风险的成因离不开外来威胁与系统自身的脆弱性,且风险的最终后果就是损失。图 1 中的“a. 威胁性”是系统的“风险源”,它是由于未授权访问、毁坏、数据修改以及拒绝服务等给系统造成潜在危害的任何事件。中观信息系统的威胁来自于人为因素及非人为因素两个方面。人为因素是对中观信息系统造成威胁的决定性力量,人为因素造成威胁的主体有竞争对手、网络黑客、不满员工或正常员工。图 1 中的“b. 脆弱性”是指在系统安全程序、管理控制、物理设计中存在的、可能被攻击者利用来获得未授权信息或破坏关键处理的弱点,由物理环境、技术问题、管理问题、法律问题四个方面组成。图 1 中的“d. 风险承受力”是指在中观信息系统遭遇风险或受到攻击时,维持业务运行最基本的服务和保护信息资产的抵抗力、识别力、恢复力和自适应能力。

中观信息系统风险的产生有两种方式:一是遵循“a→b→c”路径,这条路径形成的风险为中观信息系统“固有风险”,即假定中观信息系统中不存在内部控制制度,从而造成系统存在严重错误与不法行为的可能性。该路径的作用形式为人为因素或非人为因素是风险源,对中观信息系统构成威胁,该威胁产生后寻找并利用系统的脆弱点(假定中观信息系统对该脆弱点没有设计内控制度),当威胁

成功作用于脆弱点后，就对系统进行有效攻击，进而产生中观信息系统风险。二是遵循“a→b→P→c”路径，该路径所形成的风险为中观信息系统的“控制风险”，即内部控制制度体系未能及时预防或发现系统中的某些错误或不法行为，以致中观信息系统遭受损失的可能性。与“a→b→c”路径比较，该路径多出“P. 内部控制”过程，这说明当威胁已产生并将利用系统的脆弱点时，中观经济主体已经对该脆弱点设计了内控制度体系，但是由于内部控制制度设计的不科学、不完善或没有得到有效执行，从而造成内部控制未能阻止“威胁”，致使中观信息系统形成风险。中观信息系统损失的形成遵循“c→d→e”路径。然而，由于中观信息系统自身具有一定的风险防御能力（即“d. 风险承受力”），因而并非所有风险都将造成损失。当中观信息系统识别并抵抗部分风险后，最终未能消除的风险通过对系统的负面作用，会给中观信息系统造成间接或直接的损失。

三、中观信息系统固有风险的评价模式

表 1　BS7799 标准在中观信息系统审计中的应用分析

BS7799 要项	BS7799 目标与措施	中观信息系统固有风险的评价					中观信息系统内部控制的评价						
		物理层次		逻辑层次			一般控制的评价				应用控制的评价		
		物理环境安全风险	物理设备环境风险	软件环境风险	系统生命周期风险	逻辑安全风险	组织管理的控制	数据资源管理控制	环境安全管理控制	系统运行管理控制	输入控制	处理控制	输出控制
A. 安全方针		X	X	X	X	X	X	X	X	X	X	X	X
B. 安全组织	B_1. 信息安全组织机构	X	X	X	X	X	X	X	X	X	X	X	X
	B_2. 第三方访问安全	X	X	X	Z	X	Z	X	X	X	X	X	X
	B_3. 外包控制	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z
C. 资产分类与控制	C_1. 资产责任		X	X			X	X	X	X			
	C_2. 信息分类					X		X					
D. 人员安全	D_1. 工作职责与人员考察	X	X	X	X	X	X	X	X	X	X	X	X
	D_2. 用户培训		X	X		X		Z	Z	X	X	X	X
	D_3. 安全事故与安全故障反映	X	X	X	X	X	X	X	X	X	X	X	X
E. 实物与环境安全	E_1. 安全区域	X		Z	Z	Z	X	Z	Z	Z	Z	Z	Z
	E_2. 设备安全	X	X		Z		X		X				
	E_3. 通用控制	X	X	X	X	X	X	X	X	X	X	X	X
F. 通信和运作管理	F_1. 操作程序与职责			X	X	X	X	X	X	X	X	X	X
	F_2. 系统策划与验收			X	Z	Z	X		Z	X	X	X	X
	F_3. 恶意软件与控制			X	Z	X	X	Z	X	X	X	X	X
	F_4. 内务管理			X	Z	Z	X	X	X	X	Z	Z	Z
	F_5. 网络管理			X		X	X	X	X	X	X	Z	X
	F_6. 媒体处理与安全		Z	X	Z	X	X	X	X	X			
	F_7. 信息与软件交换			X	X	X	X	X	X	X	X	X	X
G. 访问控制	G_1. 访问控制方针			X	X	X	X	X	X	X	X	X	X
	G_2. 用户访问管理			X	X	Z	X	X	X	X	X	X	X
	G_3. 用户职责		Z	Z	X		X	Z	Z	X			
	G_4. 网络访问控制			X	X	X	X	X	X	X	X	Z	X
	G_5. 操作系统访问控制			X	X	X	X	X	X	X	X	X	X
	G_6. 应用访问控制			Z	X	X	X	X	X	X	X	X	X
	G_7. 系统访问与使用的监控			X	Z	X	X	X	X	X	X	X	X
	G_8. 移动式计算与远程工作	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z
H. 系统开发与维护	H_1. 系统安全要求			Z	X	X	X	X		X	X	X	X
	H_2. 应用系统的安全			Z	X	X	X	X	X	X	X	X	X
	H_3. 加密技术的控制			Z	X	X	X	Z	Z	Z	X	X	X
	H_4. 系统文件的安全			Z	X	X	X	X	X	X	X	X	X
	H_5. 开发和支持过程的安全	Z	Z	X	X	X	X	X	X	X	X	X	X
I. 业务持续管理		Z	Z	X	X	X	X	Z	Z	Z	Z	Z	Z
J. 符合性	J_1. 依从法律法规要求	Z	Z	X	X	X	X	X	X	X	X	X	X
	J_2. 安全技术依从评审	X	X	X	X	X	X	X	X	X	X	X	X
	J_3. 系统审核考虑因素	X	X	X	X	X	X	X	X	X	X	X	X

注：表 1 中“X”表示“有借鉴 BS7799 标准的可能性与必要性”；“Z”表示“有借鉴 BS7799 标准的可能性则但是否借鉴则根据中观经济主体自身情况而定”；“空格”表示“不会涉列到 BS7799 标准”。

图 1 中的“a→b→c”路径是中观信息系统固有风险产生的路径，固有风险形成的条件是“假定不存在内部控制制度”。评价固有风险是中观信息系统审计准备阶段的一项基础工作，只有正确评价固有风险，才能合理评估审计风险，准确确定审计范围并制定审计计划[5-6]。笔者认为，BS7799 标准之所以能够有效评价中观信息系统的固有风险，是因为 BS7799 标准的管理要项、管理目标，控制措施与管理要点组成了信息安全管理体系，这个体系为 IT 审计师确定与评价系统固有风险提供了指南[7]。BS7799 标准对 IT 审计师评价固有风险的贡献见上表 1。

（一）物理层次的风险评价

物理层次的内容包括物理环境安全与物理环境设备[7]，其中，物理环境安全包括硬件接触控制、预防灾难措施和网络环境安全；物理环境设备包括支持设施、硬件设备和网络物理环境。针对上述分类，下面对物理层次风险评价进行具体分析。

首先是物理环境安全风险评价。在评价物理环境安全风险时，可以借鉴 BS7799 标准 A、B、D_1、D_3、E、G_8、H_5、I、J。例如，IT 审计师在了解被审中观信息系统的“预防灾难措施”时，可参照“A. 安全方针”，依据 BS7799 对“安全方针”进行阐述，了解被审系统的“信息安全方针”，关注被审系统在相关的“方针与策略”中是否估计到了系统可能遭遇的所有内外部威胁；当威胁发生时，是否有具体的安全保护规定及明确的预防措施；对于方针的执行，是否对每位员工都有所要求。假若 IT 审计师在审计中未找到被审系统的“安全方针”，或找到了但“安全方针”并未涉及有关“灾难预防”方面的安全措施，则 IT 审计师可直接认定被审系统在这方面存在固有风险。其次，物理环境设备风险评价。在评价物理环境设备风险时，可以借鉴 BS7799 标准 A、B、C_1、D、E_2、E_3、F_6、G_3、G_8、H_5、I、J。例如，IT 审计师在了解被审系统有关“硬件设备”的情况时，可参照“C1. 资产责任”。BS7799 标准对“资产责任”的说明有“组织可根据运作流程与系统结构识别资产，列出清单”，“组织的管理者应该确定专人负责相关资产，防止资产的被盗、丢失与滥用”。借鉴 C1 的信息安全管理目标与措施，IT 审计师可以关注被审单位是否列出了系统硬件设备的清单，是否有专人对资产负责。如果相关方面的管理完备，则说明“硬件设备”在责任方面不存在固有风险，IT 审计师也不需要再对此方面的固有风险进行评价。再如，IT 审计师在确认“硬件设备”方面的固有风险时，还可参照“E_3. 通用控制”。BS7799 标准对“通用控制”的说明有“定期进行资产清查”，“未经授权，资产不能随便迁移”等。借鉴这一措施，IT 审计师需要了解被审系统的有关资产清查记录以及资产转移登记手续，如果相关记录不完整或手续不完备，则 IT 审计师可直接认定“硬件设备”在控制方面存在固有风险。

（二）逻辑层次的风险评价

逻辑层次的内容包括软件环境、系统生命周期和逻辑安全[7]。其中，软件环境包括系统软件、网络软件与应用软件；系统生命周期包括系统规划、分析、设计、编码、测试、试运行以及维护；逻辑安全包括软件与数据接触、数据加密机制、数据完整性、入侵检测、病毒与恶意代码以及防火墙。针对以上分类，下面对逻辑层次风险评价进行具体分析。

首先是软件环境风险评价。在评价软件环境风险时可以借鉴 BS7799 标准 A、B、C_1、D、E_1、E_3、F、G、H、I、J。例如，IT 审计师在掌握被审系统有关“网络软件”的情况时，可借鉴“G2. 用户访问管理”标准。BS7799 对该标准的阐述包括“建立用户登记过程，对用户访问实施授权”，“对特权实行严格管理”，“对用户口令进行严格管理”等。借鉴 G_2 下相关信息安全管理措施，IT 审计师可以详细核查被审网络软件是否建立了用户注册与登记过程、被审软件的特权管理是否严格、是否要求用户秘密保守口令。假若 IT 审计师发现用户并未得到访问网络软件的权限却可以轻易访问网络软件，则该软件必然存在风险，IT 审计师就可通过与 BS7799 标准比照并发表评价结论。又如，IT 审计师在评价“系统软件”固有风险时，可借鉴“G_5. 系统访问与使用的监控”标准。该标准的阐述有“使用终端安全登陆程序来访问信息服务”，“对高风险的不活动终端采取时限措施”。IT 审计师在评价“系统软件”自身风险时，可套用上述安全措施，逐项分析被审系统软件是否完全达到上述标准并作出合理的风险评价。其次是系统生命周期的风险评价。在评价系统生命周期风险时，可借鉴 BS7799 标准 A、B、D_1、D_3、E、F_1、F_2、F_3、F_4、F_6、F_7、G、H、I、J。如 IT 审计师在检查被审系统的“系统设计”时，可参照“H1. 系统安全要求”。H1 的解释为“系统设计阶段应该充分考虑系统安全性，组织在项目开始阶段需要识别所有的安全要求，并将其作为系统设计开发不可或缺的一部分进行调整与确认”。因而，IT 审计师在检查系统设计有关资料时，需要分析被审单位是否把上述解释融入系统设计中，或是否全面、有效

地融入设计过程，如果被审单位考虑了诸因素，IT 审计师就可以确认被审系统的设计环节在此方面不存在风险。假若 IT 审计师发现在系统设计阶段被审单位没有考虑到需要“引入控制”，且在系统运营期间对系统的“控制”也不够重视，则 IT 审计师可以作出系统自身安全及系统设计开发过程存在风险的结论。第三是逻辑安全的风险评价。在评价逻辑安全风险时，可以借鉴 BS7799 标准 A、B、C_2、D、E_1、E_3、F、G_1、G_2、G_4、G_5、G_6、G_7、G_8、H、I、J。IT 审计师在检查被审系统的“病毒与恶意代码”时，可借鉴“G4. 网络访问控制”。BS7799 对该标准的阐述有“建立并实施网络用户服务使用方针”，“从用户终端到网络服务的路径必须受到控制”以及“对外部链接的用户进行身份鉴别”等。IT 审计师在审计过程中，应该关注被审系统在上述方面的执行思路与执行程度，假若被审单位对上述方面缺乏重视，则恶意用户未经授权或未受限制就能轻易访问系统，系统遭受病毒或恶意代码损害的风险会相应加大。再如，IT 审计师在评价系统“数据完整性”的风险时，可借鉴“F1. 操作程序与职责”。该标准的描述有“在执行作业的过程中，提供差错处理及例外情况的指导”，“进行职责分离，减少出现非授权更改与数据信息滥用的机会”等。结合上述措施，IT 审计师应该关注被审单位是否通过外键、约束、规则等方式保障数据的完整性，如果被审单位没有按照上述方法操作，则被审系统将会在“数据完整性”方面存在风险。

需要强调的是中观信息系统固有风险的评价较为复杂。在理论研究中，本文仅选取 BS7799 的某些标准举例进行阐述，但在实践中，IT 审计师不应只借鉴 BS7799 标准的单个或部分标准，就做出某方面存在“固有风险”的结论。如仅从 C_1 看，“硬件设备”无固有风险，但从 E_3 看，“硬件设备”确实存在固有风险。鉴于此，IT 审计师应由“点”及“面”，全面借鉴 BS7799 标准的整个体系。只有如此，才能更科学具体地进行物理及逻辑层次的风险评价。

四、中观信息系统内部控制的评价机制

图 1 中的“a→b→P→c”路径是中观信息系统控制风险产生的路径，控制风险的形成条件是“假定存在内部控制制度，但是内控制度不科学、不健全或执行不到位”，产生控制风险最主要的原因是内部控制机制失效，即“P”过程出现问题。评价内部控制是 IT 审计师防范审计风险的关键，也是中观信息系统审计实施阶段的一项重要工作。然而，当前我国信息系统审计方面的标准与规范仅有四项，因而 IT 审计师对信息系统内部控制的评价还处于摸索阶段，急需详细的流程与规范进行指导。笔者认为，BS7799－1《信息安全管理实施细则》与 BS7799－2《信息安全管理体系规范》能够为 IT 审计师评价中观信息系统的内部控制提供思路。BS7799 是一套完备的信息安全管理体系，IT 审计师完全可以借鉴其体系与框架来设计中观信息系统内部控制评价流程，构建适用于中观信息系统的审计流程。BS7799 标准的具体借鉴思路见表 1，具体阐述如下。

（一）一般控制的评价

1. 组织管理的内部控制评价

在评价组织管理的内控时，可借鉴 BS7799 标准 A、B、C_1、D_1、D_3、E、F、G、H、I、J。IT 审计师可将 BS7799 标准体系作为信息系统组织管理内部控制的衡量标准，并以此确认被审系统组织管理内控制度的科学性与健全性。假若某中观经济主体将信息系统的部分管理活动外包，则 IT 审计师可借鉴 BS7799 中的“B_3. 外包控制”标准，检查外包合同的全面性与合理性。如果被审单位在外包合同中规定了信息系统的风险、承包主客体各自的系统安全控制程序，并明确规定了“哪些措施必须到位，以保证涉及外包的所有各方关注各自的安全责任”，“哪些措施用以确定与检测信息资产的完整性和保密性”，“采取哪些实物的和逻辑的控制以限制和限定授权用户对系统敏感信息的访问”以及“发生灾难时，采用怎样的策略来维持服务可用性”，则 IT 审计师就可确认被审系统在外包方面的控制设计具有科学性与全面性，只需再对外包控制条款的执行效果进行评价就可以得出对被审单位外包活动评

价的整体结论。

2. 数据资源管理的内部控制评价

在评价数据资源管理的内控时,可以借鉴 BS7799 标准 A、B、C、D、E1、E_3、F、G、H、I、J。信息系统数据包括数据字典、权限设置、存储分配、网络地址、硬件配置与系统配置参数,系统数据资源管理有数据存放、备份、恢复等,内容相对复杂。IT 审计师在评价数据资源管理的内部控制时,也需要借鉴 BS7799 标准体系。例如,IT 审计师可借鉴"F_1. 操作程序与职责"或"G_6. 应用访问控制"评价数据资源管理。F_1 与 G_6 的阐述有"识别和记录重要数据的更改"、"对数据更改的潜在影响作出评估"、"向所有相关人员传达更改数据的细节"、"数据更改不成功的恢复措施"、"控制用户的数据访问权,如对读、写、删除等进行限制"、"在系统共享中,对敏感的数据实施高级别的保护"。IT 审计师在审计时,有必要根据上述思路对系统数据管理的控制制度进行深层次评价。在当前缺乏信息系统审计规范的情况下,以 BS7799 体系作为评价数据资源管理内部控制的指南,不失为一种好的审计策略。

3. 环境安全管理的内部控制评价

在评价环境安全管理的内控时可以借鉴 BS7799 标准 A、B、C_1、D、E、F、G、H、I、J。信息系统的环境安全管理包括物理环境安全管理与软件环境安全管理,系统环境是否安全决定着危险因素对脆弱性的攻击程度,进而决定着信息系统风险。IT 审计师在审计系统环境的安全管理过程时,需要关注设备、网络、软件以及硬件等方面。在评价系统环境安全管理的内部控制时,IT 审计师有必要借助上述 BS7799 标准体系。例如,BS7799 的"E_1. 安全区域"标准与"E_2. 设备安全"标准的解释有"信息处理设施可能受到非法物理访问、盗窃、泄密等威胁,通过建立安全区域、严格进入控制等控制措施对重要的系统设施进行全面保护","应该对信息处理设施运作产生不良影响的环境条件加以监控,如,湿度与温度的影响"。类似上述的 BS7799 系列标准都为 IT 审计师如何确认环境安全管理的内控提供了审计指导,且其指导思路清晰、全面。IT 审计师通过借鉴 BS7799 系列标准,可以深层次挖掘系统环境安全管理规章制度中存在的疏漏以及执行中存在的问题,从而有效评判环境安全管理的控制风险。

4. 系统运行管理的内部控制评价

在评价系统运行管理的内控时,可以借鉴 BS7799 标准 A、B、C_1、D、E_1、E_3、F、G、H、I、J。中观经济主体对运行系统的管理相对复杂,涉及到系统组织、系统维护、系统完善等多个方面。由于系统运行中需要管理的环节繁多,而且目前也没有规范与流程可以参考,因而,评价系统运行管理的内控也有必要借鉴上述 BS7799 标准体系。例如,BS7799 标准"D_2. 设备安全"与"H_5. 开发与支持过程中的安全"的阐述有"信息系统操作者需要接受安全意识培训,熟悉与系统运行相关的安全职责、安全程序与故障制度","系统运行中,建立并实施更改控制程序"以及"对操作系统的更改进行技术评审"等方面。IT 审计师采用询问、观察、检查、穿行测试等方法评审系统运行管理的内部控制,需要有上述明细的、清晰的信息安全管理规则予以指导,这些标准可以指导 IT 审计师了解被审系统是否有健全的运行管理规范及是否得到有效运行,借此,IT 审计师可以作出全面的内控判断,进而出具正确的审计结论。

(二) 应用控制的评价

信息系统的应用控制包括输入控制、处理控制与输出控制。在评价系统输入控制、处理控制以及输出控制三者的内控时,同样有必要借鉴 BS7799 标准,且 BS7799 标准中 A、B、D、E_1、E_3、F_1、F_2、F_3、F_4、F_5、F_7、G_1、G_2、G_4、G_5、G_6、G_7、G_8、H、I、J 相对应的信息安全管理目标与措施能够在 IT 审计师对三者进行内控评价时提供相对详尽的审计框架。为确保信息系统输入、处理与输出的信息完整、正确,中观经济主体需要加强对信息系统的应用控制。IT 审计师在中观信息系统审计的过程中,需要做到对被审系统应用控制进行正确评价。

在 IT 审计师对应用控制的符合性测试过程中,上述 BS7799 标准体系可以对应用控制评价进行

全程指导。例如,BS7799 标准中“H_2. 应用系统的安全”提到“数据输入的错误,可以通过双重输入或其他输入检查侦测,建立用于响应输入错误的程序”,“已正确输入的数据可因处理错误或故意行为而被破坏,系统应有确认检查功能以探测数据的破坏”,“为确保所存储的信息相对于各种情况的处理是正确而恰当的,来自应用系统的输出数据应该得到确认”等控制策略,并提出了相对详细的控制措施。应用控制环节是信息处理的脆弱集结点,IT 审计师在进行应用控制的符合性测试环节时有必要考虑周全,详尽规划。IT 审计师可以遵循 H_2 全面实施针对应用控制的审计,依照 BS7799 标准体系,检查被审系统对于超范围数值、数据区中的无效字符、丢失的数据、未经认可的控制数据等系统输入问题的控制措施以及应急处理能力;检查是否对系统产生的数据进行了确认,系统的批处理控制措施、平衡控制措施等,以及相关控制行为的执行力度;检查信息输出是否实施了可信性检查、一致性控制等措施,如果有相关措施,那么执行力度如何。BS7799 标准体系较为全面,对于 IT 审计师评价系统的应用控制贡献很大,如果 IT 审计师能够创造性借鉴该标准,必可做好符合性测试,为实质性测试夯实基础,也定会提高审计质量。

五、结束语

表 1 是笔者在分析某商业银行信息系统与某区域物流信息系统的基础上,对“BS7799 标准如何应用于信息系统审计”所进行的设计,当针对其他行业时,或许需要对表 1 进行适当调整。不同行业、不同特性的中观经济主体在信息系统审计中运用 BS7799 标准时侧重点会有所不同。本文以分析中观信息系统风险为着手点,沿用 BS7799 标准对中观信息系统审计进行研究,旨在抛砖引玉。

参考文献:

[1]王会金,刘国城. 中观经济主体信息系统审计的理论分析及实施路径探索[J]. 审计与经济研究,2009(5):27-31.

[2]BSI. ISO/IEC17799-2000 Information technology-code of practice for information security management[S]. London: British Standards Institation,2000:179-202.

[3]BSI. BS7799-2-2002 information security management-specification for information security management systems[S]. London: British Standards Institation,2002:267-280

[4]孙强. 信息系统审计[M]. 北京:机械工业出版社,2003.

[5]刘国城,王会金. 中观信息系统审计风险的理论探索与体系构架[J]. 审计研究,2011(2):21-28.

[6]王会金. 中观信息系统审计风险控制体系研究——以 COBIT 框架与数据挖掘技术相结合为视角[J]. 审计与经济研究,2012(1):16-23.

[7]科飞管理咨询公司. 信息安全管理概论-BS7799 理解与实施[M]. 北京:机械工业出版社, 2002.

[责任编辑:刘　茜,高　婷]

BS7799 Criterion and Its Application in Meso-information Systems Audit

LIU Guocheng

(Jinshen College of Nanjing Audit University, Nanjing 210029, China)

Abstract: Starting with the genetic analysis of meso-information system risks and losses, this paper first studies the evaluation model of meso-information system inherent risks from both physical and logical levels based on the BS7799 standards, and then explores the inner control evaluation model of meso-information system from two levels of general control and application control, in order to provide an application guidance for IT auditors in their practice of meso-information system audit.

Key Words: BS7799 criterion; meso-audit; information system audit; internal control; meso-information system; meso-information system risks