商业银行信息系统安全审计免疫体系的构建
——基于信息系统安全风险的实证估计

刘国城

（南京审计大学 会计学院，江苏 南京 211815）

[摘 要]当前，信息系统风险为商业银行的稳定带来巨大威胁，由此，商业银行如何正确开展信息系统安全风险估计，并有效构建自身的安全审计免疫机制，将变得无比重要。以“审计免疫”为理论指导，以“信息熵”为关键技术，结合商业银行信息系统运营风险的递阶层次结构，建立安全风险估计的“信息熵”模型，分析该模型对信息系统安全审计免疫的贡献，并基于“免疫监视”“免疫自稳”与“免疫防御”视角，提出构建商业银行信息系统安全审计免疫体系的建设性思路。

[关键词]商业银行；信息系统审计；安全审计；免疫体系；安全风险；信息熵；审计免疫

[中图分类号]F239.45 [文献标志码]A [文章编号]1004－4833(2017)05－0042－10

2016年7月，银监会发布《中国银行业信息科技“十三五”发展规划监管指导意见》，提出以互联网、大数据、云计算以及位置服务等为代表的新兴信息技术与银行运营业务深度融合，对银行组织的系统构架、数据治理、系统开发、基础设施、运行维护、风险管控等领域都提出了更高的要求，银行业亟待加强信息系统安全管理，全面提升网络与信息安全水平，健全与完善银行业安全防护体系。然而，当前我国银行业运营信息系统的安全状况不容乐观。近年来，我国发生一系列银行信息系统瘫痪事件，从案例比较来看，商业银行信息系统承载的功能日趋繁杂，所面临的风险日益增加，且更为隐蔽。为此，商业银行应该熟悉信息系统的构造原理，明晰大数据与云计算等新兴智能科技所带来的冲击，熟知信息系统安全风险的运行规律，切实加强对自身信息系统安全的风险管理与审计免疫。

一、相关理论回顾与概述

Trydid等认为，商业银行信息系统安全风险是指在特定运行环境下，商业银行信息系统由于行动路径偏离目标状态而出现某种损失的可能性，当系统风险作用于特定脆弱点时，银行运营损失必将发生[1]。商业银行信息系统安全从属于信息系统安全范域。袁小勇归纳理论界关于审计本质的论述，发现其中一种观点是审计保险论。该理论认为审计是分担风险的一项服务，审计的本质在于抑制风险，通过防范错弊风险进而避免灾难性损失[2]。审计是风险控制决策的关键需求之一，安全审计也不例外。信息系统安全审计是特别针对信息系统安全所开展的审计活动，它旨在对网络用户行为开展监督管理，对计算机工作过程实施详尽跟踪，对信息系统的设计、规划与维护进行查遗补漏，记录系统管理，记载用户行为，捕捉与监控各类安全事件，维护管理审计记录与审计日志，最大程度提升信息系统的安全性、可靠性与保密性[3]。国内关于信息系统安全风险的研究文献相对较多，其中，付钰等基于模糊理论分析信息系统安全风险的评价方法[4]；付沙基于熵权视角建立信息系统安全风险的检测模型[5]；马刚等通过构架威胁传播树探索复杂信息系统安全风险估计模式[6]。国内有关信息系统安全审计方面的文献相对较少，尤其是基于审计保险论，以审计为风险控制手段直面探究风险与审计之

[收稿日期]2016－05－22

[基金项目]国家社会科学基金一般项目(16BJY022)

[作者简介]刘国城(1978—)，男，内蒙古赤峰人，南京审计大学会计学院副教授，硕士生导师，从事信息系统审计理论研究。

间正向演绎规则的文献更为稀缺,其中,刘国城等探讨了日志视角下信息系统的安全风险及其审计控制[7],曾建光等研究了因信息系统安全漏洞而引发的安全风险、内控有效性以及审计师行为三者之间的作用关系[8]。但它们仅是宏观层面的定性研究,难成体系。

融合彭友等人的观点[9],商业银行开展安全审计应涵盖:(1)检查与评价安全防护体系运行的有效性;(2)发现超越权限的访问用户;(3)判断越权用户的行为及性质;(4)监测越过安全防护机制而进行的反复性测试活动;(5)对越权行为及时制止;(6)对越权行为取证;(7)系统遭受侵袭时,评估系统损失,并提出修复方案。由上文可知,商业银行信息系统安全审计的重心应该是网络安全审计与信息安全审计。截至2017年1月,中国知网有关"网络安全审计"的期刊论文46篇,核心期刊7篇;有关"信息安全审计"的期刊论文22篇,核心期刊5篇,其中,杨丹采用领域工程方法架构领域模型,提出基于领域构件的信息安全审计系统的体系结构[10];包捷等结合云计算与日志审计等技术,设计云环境下信息安全审计的功能模块,并建立验证模型[11]。通过文献梳理,我们发现,我国学界对于信息系统安全风险评估的理论研究趋于成熟,既有逻辑分析法、Delphi法等定性研究,又有AHP法、模糊评价、D-S证据理论、灰色理论以及机器学习等定量研究[12]。然而,对于信息系统安全审计方面的研究,尚待完善,相关文献缺少微观层面的实证归纳,且因"互联网"等所引发的安全风险治理困境,很少有文献基于风险为本源,探寻信息系统安全审计的深层次变革之路。当前,我国亟须一系列成熟的信息系统安全审计理论体系,且针对商业银行领域,学者们还需做如下努力:(1)遵循系统论理念与重要性原则,在基础理论建设方面纵向深化,在实践应用研究方面广泛延伸;(2)追溯风险根源,依托成熟方法,基于风险导向审计与审计保险论,推进商业银行信息安全审计取证,创新审计技术,促进审计管理的科学化。

二、商业银行信息系统安全风险估计的递阶层次结构

商业银行信息系统的运行离不开网络、计算机、信息与数据等关键资源,当人为的误用与滥用或意外故障与灾害作用于相关资源的脆弱点时,将对系统产生威胁,并很可能造成系统损失。商业银行信息系统安全风险估计是指运用概率统计等方法对特定风险事件发生的概率与损失进行定量估计的过程。为明确商业银行信息系统安全风险的影响因素,本文构建了递阶层次结构模型(图1),采用层次分析法对商业银行信息系统的总体风险进行分解分析。第0层表示基于物理、网络、系统、应用以及管理层面所存在的商业银行信息系统总体安全风险 Y;第1层为商业银行信息系统安全风险的两个管理要项,其概率权重由 α_i 表示;第2层阐述商业银行信息系统安全风险每个管理要项下所对应的若干个控制目标,其概率权重由 β_{ij} 表示;第3层阐释了第 i 个管理要项下第 j 个控制目标中的若干个风险控制措施,其符合度概率权重由 γ_{ijk} 表示。第3层次的控制措施由18项构成(图1),它们是规避信息系统安全风险与优化信息系统免疫机制的关键所在。

风险控制措施的符合度 γ 表示信息系统的安全状态与风险控制措施的符合程度。图1中,第3层次有关风险控制18项措施的符合度可分为6类等级范围(表1)。级域 $\pi 1$ 反映系统无任何相应的安全控制措施,系统绝对不安全;级域 $\pi 6$ 反映相应安全措施的设计与执行完全符合安全基线的要求,系统绝对安全。$\pi 2$—$\pi 5$ 介于 $\pi 1$ 与 $\pi 6$ 两项极值之间,表示具有特定数量的风险控制措施,系统在特定程度上具有特定的安全特性。此外,对商业银行信息系统进行风险估计还需要界定风险的等级。表2界定了系统风险的5个级别,由表2可知,当 $0 < \Phi \leqslant 0.35$ 时,风险较低,稍微注意防范即可;当 $0.35 < \Phi \leqslant 0.55$ 时,风险中等,需要加强防范与控制;当 $0.55 < \Phi \leqslant 0.75$ 时,风险较大,要求相关部门进行有针对性的重点控制;当 $0.75 < \Phi \leqslant 1.00$ 时,风险极高,要求相关部门全面采取措施控制风险或更换系统。

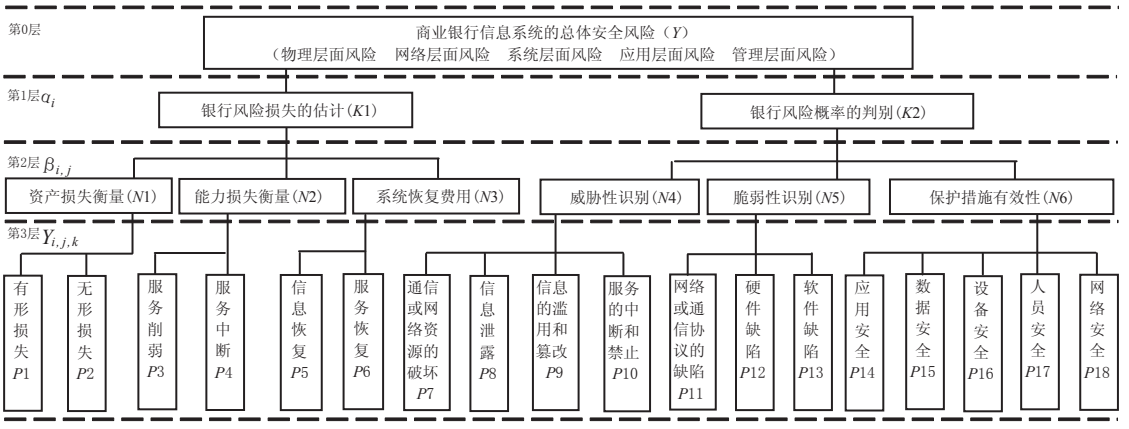

图1　商业银行信息系统风险估计的递阶层次结构

表1　符合度的量化及描述

符合度	量化值与范围	符合程度措施
π1 不符合	$\pi=0$	无任何相应的安全控制措施
π2 不太符合	$0<\pi\leqslant 0.25$	有少数安全控制措施，但达不到安全基线的要求，或仅起到极小作用
π3 基本符合	$0.25<\pi\leqslant 0.50$	有一定安全控制措施，达到少量安全基线的要求，或仅起到部分作用
π4 较好符合	$0.50<\pi\leqslant 0.75$	有较好的安全控制措施，但未能起到较好的效果
π5 完全符合	$0.75<\pi<1.00$	安全措施基本上能达到安全基线的要求，或者起到较好的效果
π6 完全符合	$\pi=1.00$	安全措施完全符合安全基线的要求，并完全按照安全控制措施进行

表2　风险等级的界定及描述

等级	量化值与范围	影响描述
Φ1 可以忽略	$\Phi=0$	危害程度微乎其微，可以不予考虑
Φ2 较小	$0<\Phi\leqslant 0.35$	危害会造成一些很小的影响，只需较小的努力就可以弥补
Φ3 程度中等	$0.35<\Phi\leqslant 0.55$	直接影响系统的运行，或是对系统资源或服务信任程度的降低
Φ4 较大	$0.55<\Phi\leqslant 0.75$	可导致数据的较大损失，即使付出很大的努力也难于弥补
Φ5 极为关键	$0.75<\Phi<1.00$	可引起灾难性的损失，或直接导致业务的中断或关闭
Φ6 完全风险	$\Phi=1.00$	系统安全几乎处于瘫痪状态，业务随时中断与关闭

三、商业银行信息系统安全风险估计模型的构建与例证

（一）信息熵安全风险估计模型的建立

1948年，美国应用数学家Shannon撰写了《通讯的数学理论》，该文章为“信息熵”理论诞生的标志[13]。Shannon通过“信息熵”概念，解决了信息的量化度量问题，其辅以数学表达式，描述了有关信息的特定假设下经典概率分布的不确定性。Shannon对信息熵的定义为：“若系统有 n 种不同的状态，即 $S_1,S_2,\cdots,S_n$，$P(S=S_i)=p_i$ 表示信息系统处于状态 S_i 的概率，则信息系统具有不确定信息量 H（熵）为 $H=-C\sum_{i=1}^{n}p_i\ln p_i$，公式中，$p_i$ 满足 $0\leqslant p_i\leqslant 1(i=1,2,\cdots,n)$，且有 $\sum_{i=1}^{n}p_i=1$。”

$H=-\sum_{i=1}^{n}p_i\ln p_i$ 用以衡量系统信息的有序稳定程度。对 H 求导数并取极值可知，当 $p_1=p_i=p_n$ 时，信息熵 H 的数值最大，风险因素 Y 对信息系统风险影响的非确定性最大。假定商业银行信息系统风险估计中需要衡量 n 类风险因素，针对某个具体因素 K，若 K 要素评判集中指标的支持度为 $\lambda_1,\lambda_2,\cdots,\lambda_j,\cdots,\lambda_m$，则可运用信息熵计算各指标的权重，并满足 $\sum_{j=1}^{m}\lambda_{ij}=1,(i=1,\cdots,n;j=1,\cdots,m)$。且具

体风险因素 K_i 的相对重要性熵值为:

$$H_i = -\sum_{j=1}^{m} \lambda_{ij} \ln \lambda_{ij}$$

对风险因素 K_i 的相对重要性作归一化处理,可推导出 K_i 的相对重要性熵值为:

$$e_i = -\frac{1}{\ln m} \sum_{j=1}^{m} \lambda_{ij} \ln \lambda_{ij}$$

根据极值原理,当 $\lambda_{ij}(j = 1, \cdots, m)$ 取值相等,即 $H_{max} = \ln m$ 时,熵值 $e_i = 1$(最大值),且 $0 \leqslant e_i \leqslant 1$。当 $e_i = 1$ 时,风险因素 K_i 对信息系统风险影响的非确定性最大,对系统风险估计的贡献最小。为了使计算值正向的反映该方法的重要程度,可借用 $1 - e_i$ 确定风险因素 K_i 的权值,并归一化处理,进而导出 K_i 的权值 θ_i 为:

$$\theta_i = \frac{1}{n - \sum_{i=1}^{n} e_i}(1 - e_i) \quad \text{且} \ 0 \leqslant \theta_i \leqslant 1, \sum_{i=1}^{n} e_i = 1。$$

结合上述信息熵的基本原理,本文建立商业银行信息系统信息熵风险估计模型的具体步骤如下。

1. 确定商业银行信息系统风险估计的递阶层次结构

图 1 将系统的总体风险 Y 划分为 K 层次、N 层次与 P 层次,层级之间存在着逻辑关联与因果关系。其中,P 层次的所属要素是 N 层次的关键控制措施,N 层次的所属要素是 K 层次的关键控制目标,而 K 层次的 K_1 与 K_2 又是 Y 层次的关键计量要素。

2. 选取 P 层次下风险控制措施符合度的数量值

符合度数量值的选取有两种方式,即主观赋值法与客观赋值法。主观赋值法又称专家赋值法,是指依据估计者的经验判断来计算符合度权重的原始数据,如专家调查法以及模糊统计法等;客观赋值法是指计算符合度权重的原始数据由测评指标在测评过程中的实际数据总结得出,如主成分分析法以及均方差法等。

3. 计算 N 层次下 6 个控制目标的熵权系数 $\beta_{i,j}$ 与风险权向量 $\Phi_{i,j}$

$$\beta_{i,j} = -\frac{1}{\ln o} \sum_{k=1}^{o} \gamma_{i,j,k} \ln \gamma_{i,j,k}$$

$$\Phi_{i,j} = (1 - \beta_{i,j}) / \left(m - \sum_{j=1}^{m} \beta_{i,j} \right)$$

且 $0 \leqslant \Phi_{i,j} \leqslant 1, \sum_{j=1}^{m} \Phi_{i,j} = 1$。

4. 计算 K 层次下两个管理要项的熵权系数 α_i 与风险权向量 Φ_i

$$\alpha_i = -\frac{1}{\ln m} \sum_{j=1}^{m} \beta_{i,j} \ln \beta_{i,j}$$

$$\Phi_i = (1 - \alpha_i) / (n - \sum_{i=1}^{n} \alpha_i)$$

且 $0 \leqslant \Phi_i \leqslant 1, \sum_{i=1}^{n} \Phi_i = 1$。

5. 计算商业银行信息系统总体风险的熵权系数 ρ 与总风险权向量 Φ

$$\rho = -\frac{1}{\ln n} \sum_{i=1}^{n} \alpha_i \ln \alpha_i$$

$\Phi = 1 - \rho$,且 $0 \leqslant \rho, \Phi \leqslant 1$。

6. 确定风险控制级别,制定行动方案

参照表2的“风险等级的界定及描述”,结合总体风险的权向量数据确定商业银行信息系统的风险控制级别,并制定相应级别下风险防御、自稳与监视的行动方案。

(二) 风险估计熵模型的实例分析

针对南京银行某支行的特征系统,我们邀请信息科学、银行运营与安全审计等领域的专家开展学术讨论,以图1为对象,依据专家知识,提炼出该支行图1中第3层次18个控制措施的符合度 $\gamma_{i,j,k}$ 取值(见表3),相关取值合理表现了该支行当前风险现状与控制措施的符合状况。

表3 南京银行某支行信息系统安全风险权向量的赋值与计算

第0层	总体风险 $\Phi=0.1627$																	
第1层	$\Phi_1=0.4538$						$\Phi_2=0.5462$											
第2层	$\Phi_{1,1}=0.3752$	$\Phi_{1,2}=0.3100$	$\Phi_{1,3}=0.3148$				$\Phi_{2,1}=0.3029$				$\Phi_{2,2}=0.3711$				$\Phi_{2,3}=0.3260$			
第3层	$\gamma_{1,1,1}$	$\gamma_{1,1,2}$	$\gamma_{1,2,1}$	$\gamma_{1,2,2}$	$\gamma_{1,3,1}$	$\gamma_{1,3,2}$	$\gamma_{2,1,1}$	$\gamma_{2,1,2}$	$\gamma_{2,1,3}$	$\gamma_{2,1,4}$	$\gamma_{2,2,1}$	$\gamma_{2,2,2}$	$\gamma_{2,2,3}$	$\gamma_{2,3,1}$	$\gamma_{2,3,2}$	$\gamma_{2,3,3}$	$\gamma_{2,3,4}$	$\gamma_{2,3,5}$
	0.72	0.73	0.69	0.70	0.65	0.74	0.73	0.70	0.64	0.61	0.76	0.67	0.59	0.63	0.71	0.80	0.66	0.74

计算图1中第2层次该支行6个控制目标的 $\beta_{i,j}$ 与 $\Phi_{i,j}$,过程如下:

$\beta_{1,1}=-(0.72\times\ln0.72+0.73\times\ln0.73)/\ln2=0.6727$

$\Phi_{1,1}=(1-0.6727)/(3-2.1277)=0.3752$

同理:$\beta_{1,2}=0.7296$,$\beta_{1,3}=0.7254$,$\Phi_{1,2}=0.3100$,$\Phi_{1,3}=0.3148$

$\beta_{2,1}=-(0.73\times\ln0.73+0.70\times\ln0.70+0.64\times\ln0.64+0.61\times\ln0.61)/\ln4=0.7694$

$\Phi_{2,1}=(1-0.7694)/(3-2.2385)=0.3029$

同理:$\beta_{2,2}=0.7175$,$\beta_{2,3}=0.7517$,$\Phi_{2,2}=0.3711$,$\Phi_{2,3}=0.3260$

计算图1中第1层次该支行两个管理要项的 α_i 与 Φ_i,过程如下:

$\alpha_1=-(0.6727\times\ln0.6727+0.7296\times\ln0.7296+0.7254\times\ln0.7254)/\ln3=0.6641$

$\Phi_1=(1-0.6641)/(2-1.2599)=0.4538$

同理:$\alpha_2=0.5958$,$\Phi_2=0.5462$

计算图1中第0层次该支行信息系统总体风险的 ρ 与 Φ,过程如下:

$\rho=-(0.6641\times\ln0.6641+0.5958\times\ln0.5958)/\ln2=0.8373$

$\Phi=1-\rho=0.1627$

Φ 值反映了信息系统的风险等级与状态,该支行 Φ 系列数据见表3。其中,该支行总体安全风险权值(第0层)为0.1627,处于 Φ_2 等级,说明风险较小,审计主体需稍作努力即可弥补。第1层中,K_1 为0.4538,K_2 为0.5462,属于中等风险,它们都是系统的主要风险来源,审计主体需持续加强对此方面风险的关注。K_2 的风险程度高于 K_1,K_2 由 $N_{4\text{-}6}$ 构成,其中,N_5 与 N_6 的 Φ 值分别为0.3029与0.3260,属于风险较小,然而,N_5 为0.3711,属于中等风险,这说明 N_5 所对应 $P_{11\text{-}13}$ 的部分措施存在更大程度的不完善,审计主体应积极查找“脆弱性”问题,并尽快完善。

四、信息系统安全风险估计对商业银行信息系统安全审计免疫的贡献

“免疫”属于医学术语,是人体的一种生理功能,人体依赖该功能判断“自己”与“非己”物质,进而破坏和排斥进入人体的抗原物质或人体自生的恶性细胞,旨在维持肌体的健康。免疫具有防御、自稳、监视三个基本功能。2007年12月,时任审计长刘家义在全国审计工作会议上首次提出“审计免疫系统”论观点,并将“审计”比作“免疫系统”。“审计免疫”国内文献理论研究基本聚焦于国家层面,对于商业银行等具体行业的中微观“审计免疫”研究成果较少。研究证实,以“信息熵”为模型的信息系统安全风险评估方法与商业银行信息系统审计免疫体系的构建模式具有融合性。

结合前例,将“信息熵”融合于商业银行的安全审计免疫,需要关注如下方面。(1)运用“信息熵”模型自下而上估计多层级下每一层级内部各个风险因素的风险等级,通过对层级内部风险因素的权向量排序,自上而下依次递推挖掘层级体系中“程度中等”风险与“程度严重”风险所属层级的因果联系,进一步挖掘最低层级所属风险控制措施中的“不力者”。表3中第1层级K_2的风险权值大于K_1,两者风险适中。K_1所属下一层级的风险权值$N_1 > N_3 > N_2$,因而,需要更为关注N_1所属风险策略P_1与P_3的不完善性。同样,K_2所属下一层级的风险权值排序为$N_5 > N_6 > N_4$,因而,应更为关注N_5所属风险策略$P_{11} - P_{13}$的不完备性。(2)对“程度中等”风险及其所属具体控制措施建立动态预警机制。“程度中等”风险将降低系统资源或是服务信任程度,但不至于导致运营数据产生较大的损失。然而,“程度中等”风险是向更深风险层次演化的前提,审计主体需要对该类风险建立科学的动态预警机制。动态预警至少包括风险数据预处理、业务过程挖掘、业务过程取证、超高并发访问数据持续服务交付、动态持续检测与审计以及警度评估与报告等环节。(3)对“程度严重”风险及其所属具体控制措施建立持续监测机制。“程度严重”风险随时会造成运营数据重大损失,或者系统灾难与瘫痪。因此,审计主体应对该类风险建立持续监测机制。在监测数据的采集中,审计主体有必要采用多源多模态信息集成、异构数据智能转化以及整合信息的可用性评估等步骤,在监测数据的管理上,需要综合运用高效元数据管理技术、数据动态调度与优化等关键技术。前述过程是以信息系统安全风险的“熵”模型估计为根本的,并依此进一步深化商业银行信息系统的“预警与监测”策略。此外,以前述三项过程为基础,审计主体还需增补如下四个过程:(4)基于“预警与监测”经历实施商业银行信息系统安全风险的审计、控制与记忆;(5)以“预警与监测”为切入点,基于“免疫监视”视角,完善审计预防工作;(6)以“审计与控制”为切入点,基于“免疫自稳”视角,完善审计揭露工作;(7)以“审计与记忆”为切入点,基于“免疫防御”视角,完善审计抵御工作。

商业银行信息系统安全审计免疫研究符合在银行运行系统中,信息具有不确定性、信息需要量化度量以及随机事件组合的法则性、组织性与有序性持续增减等系列特点,这些恰恰与“信息熵”的思想与性质相吻合。免疫重在强调“预防”“揭露”与“抵御”,审计免疫的重点不是全面免疫,而是根据重要性、一致性与谨慎性的原则,有针对性地确定究竟该“免疫什么”以及“如何免疫”。以“信息熵”为模型的信息系统安全风险评估方法恰恰为商业银行审计主体提供了安全审计免疫的思路,运用定量的方法解决审计免疫的“什么”与“如何”问题,准确界定商业银行信息系统风险估计的递阶层次结构下每一层次内部各个因素的风险权向量和风险重要性程度排序,同时清晰确定递阶层次结构下各个层级之间所属要素相应风险等级与相应风险策略的完备程度。以“信息熵”为模型的信息系统安全风险评估方法依次挖掘出商业银行信息系统安全风险层级结构下各个层级的“脆弱点”以及最底层风险控制策略的“失策点”,且在层级中“自上而下”“直击要害”“自成体系”。对于商业银行信息系统安全审计免疫体系的构建,其本质是以“免疫系统论”为指导,以“信息熵”为关键技术,通过“熵模型风险估计”建立轴心,创新审计程序,进而推进安全审计免疫策略的理论建设。但对“信息熵”估计模型的运用需要关注两点:一是尽可能使不同层级下结构指标权重的确定由主观转为客观;二是尽可能使信息熵原理下信息系统安全风险的估计分析由静态走向动态。

五、商业银行信息系统安全审计免疫机制的建立与运行

为高效实现自身系统的安全性、可靠性、保密性以及一致性,商业银行审计主体在安全审计免疫机制的建立与运行方面需要密切关注基础工作的切实性与免疫模式的优化性。

(一)强化商业银行信息系统安全审计免疫机制的基础建设

商业银行审计主体应该做好免疫机制建设的基础工作,它们是审计免疫子系统持续发挥效力的根本,只有基础工作完善,后续子系统才能有机协调,整个系统才能动态协同。

1. 正确界定商业银行信息系统安全风险，科学规划风险估计的递阶层次结构

商业银行审计主体应该明确界定自身信息系统所蕴藏的各项风险，并在安全审计免疫工作中做到有的放矢、目标明确。商业银行信息系统的安全风险主要蕴含于物理、网络、系统、应用以及管理等五个层面，具体包括人员风险、组织风险、物理环境风险、信息机密性与完整性风险、系统自身风险、业务操作与连续性风险、设施风险以及法律风险。商业银行信息系统安全风险的存在具有普遍性，不可避免，为此，审计主体应该实时追踪安全风险的走向并抑制风险，否则，当风险作用于相关脆弱点时，商业银行信息系统的稳定性将会受到严重威胁。此外，审计主体在明晰自身信息系统安全风险的基础上，还需要科学规划风险估计的递阶层次结构。图1为商业银行提供了可参照的“递阶层次结构”样板，但图1的结构并非唯一的，因为商业银行涵盖若干业务，且不同业务之间运行机制有所不同，因此，审计主体应该基于自身安全风险的特点，借鉴图1，正确设计适用于自身特色的递阶层次结构，全方位挖掘自身风险的管理要项与控制措施，以便从根本上实现对自身信息系统安全的风险估计与审计免疫。

2. 合理运用熵模型对商业银行信息系统安全风险控制措施实施持续评价

商业银行审计主体需要以“免疫系统论”为基本前提，借鉴信息熵模型，对信息系统安全风险控制措施进行实时评价，具体步骤包括：(1)建立“信息系统安全风险控制措施评价”小组，成员需要以理论专家为主体，同时还需纳入业务实操人员、审计理论学者、外部金融顾问以及相关信息安全管理专家等多方专业人士，以求专业互补、经验共享；(2)“定期”判断商业银行信息系统安全风险的发展趋势，将特定信息系统的控制措施细化为具体的评价要点，分析各控制要素在系统中所处的地位，对具体控制要点在小组成员个体间开展独立评价并进行符合度赋值，依据加权平均算出各项控制措施的综合符合度；(3)依据熵模型依次计算各层次下的 Φ 值，结合表2对各层次下具体管理要项的安全风险进行描述，判断总体风险与各层次风险的级别，找出高风险的管理要项，标记该类要项下的安全风险控制措施；(4)对高风险管理要项下的控制措施重点改进，加强对此方面控制措施的管理。同时，还需要对第(2)步中的个体评价进行总结，关注有价值的线索并予以修正。商业银行信息系统安全风险的发展是动态的，其控制措施是静态的，这就要求审计主体对商业银行信息系统安全风险控制措施的研判与评价必须及时，并持续根据自身特点合理设计评价周期，争取将商业银行信息系统安全风险控制措施的实时评价落到实处。

在基于熵权估计的商业银行信息系统安全审计过程中，最为关键的是第(2)步。熵模型估计的实质是利用专家“定期”对递阶层次结构中具体风险打分评价。但是，“定期”究竟如何界定，打分与赋值如何体现客观性、实时性与动态性相统一，将是审计主体所面临的现实性问题。为此，本文提供针对专家组打分的系列流程，仅供参考。①建立网络学习平台。针对不同领域与地域的专家成员，审计主体需要建立网络学习平台，分别将专家组既有经验，与系统安全相关的政策、规范、国内外动态以及信息安全态势分析等及时发布至平台，供成员交流与分享。②建立网络互动平台。该平台是审计主体与专家个体互动的平台，在打分与符合度赋值前，审计主体需要针对某一议题，以“一对一”方式广泛争取成员的经验与见解。③定时开放运营系统。为使专家打分更为客观，在与专家成员签订保密协议的基础上，审计主体有必要截取核心业务片段、选取各类业务中的一部分，定时向成员开放权限。④建立网络测试平台。审计主体需要针对某一议题设计若干题目，以网络问卷的方式在该平台中对专家成员进行测试，把握专家的熟悉度。熟悉程度越高的成员，对议题的认识越为深刻，赋值的客观性越高。对于对议题把握程度不高的成员，需要及时从团队中剔除。⑤建立网络打分平台。如何“定期”开展网络打分，商业银行根据自身实际进行确定。常规情况下，打分与赋值需要以每周一次的方式在由内部成员组成的临时小组中展开，同时还要以每月一次的方式在由内外部成员组成的整个团队中展开。对于特殊情况，审计主体需要随时成立临时小组进行打分评价。⑥定期见面深入研讨。由于专家团队受时空限制，不能随时见面交流。但是，审计主体可以采用内部临时小组每月一

次以及整体专家团队每半年一次的方式,以会议的形式组织专家见面,研讨专家赋值在自身安全风险估计运用中的不足、未来的调整策略以及努力方向。

(二)优化商业银行信息系统安全审计免疫机制的运行模式

“审计免疫”借鉴预警性与修复性等特征,重在强调审计预防、揭露与抵御三者的分工与协作[14]。借鉴免疫学理论,审计主体在商业银行审计免疫机制运行模式构建中需做以下努力。

1. 合理构建“免疫监视”运行平台

免疫监视是机体免疫系统及时识别和清除机体内畸变或突变细胞以及异常病毒感染细胞的一种功能,是免疫系统最基本的功能之一。审计主体需要合理构建“免疫监视”平台,及时消除信息系统因自身原因而意外突发的异常事故风险,积极做好信息系统安全的“审计预防”工作。在构建该平台时,审计工作应涵盖:(1)建立安全风险自动报警体系。在报警体系的构建中,商业银行需要根据自身特点做好数据读取模块、数据分析模块以及消息传送模块的架构。数据读取主要关注如何优化数据库连接配置与数据查找策略;数据分析主要关注如何优化编程语言选择策略、数据排序策略以及安全指标确定策略;消息传送主要关注如何优化报警工具选择策略。(2)完善安全风险的实时预警机制,做好相关风险的成熟度分析。商业银行应以内外部审计主体为主导,评价现有信息系统安全控制措施与现实银行业务运营的差距以及产生突发风险的可能性,借鉴信息熵模型,挖掘存在严重问题的安全控制措施,并对潜在安全风险的成熟度予以分析,建立对异常风险预先识别的一套流程。“熵”模型下信息系统安全风险评估对信息系统“免疫监视”的贡献不可低估,其恰恰为“免疫监视”提供了“脆弱点”与“风险源”,通过定量研究归纳商业银行可能发生灾害的前兆,及时向审计部门发出紧急预警,以便持续监视安全风险成熟度的动态演化。(3)对信息系统自身突发风险及时予以清除。“免疫监视”是商业银行信息系统正常运行的基础,加强对自身突发事件的持续预警与及时预防,是安全审计发挥免疫作用的根本前提。

“免疫监视”运行平台是商业银行安全风险评估、风险监测、风险预警以及风险应对的管理系统,在该平台下,审计主体有必要建立信息科技风险特征库,包含风险数据、检查信息与审计策略,以便为安全风险的“免疫监视”提供全面的、有针对性的支持,进而确保风险点数据库的精确性、动态性与实时性,制定科学的安全风险关键指标体系,设定关键风险指标并建立阈值,构建业务运维、风险监测、安全预警与即时应对“四位一体”的“免疫监视”动态协同治理模式。

2. 有效构建“免疫自稳”运行平台

免疫自稳是机体免疫系统维持内环境稳定的一种生理功能,及时将机体内损伤、衰老与死亡的细胞和其他异物识别并予以清除。审计主体需要有效构建“免疫自稳”平台,对原有商业银行信息系统安全风险控制策略体系中因事物发展而连续“滞后”的、有问题的控制措施予以及时识别、修正与清理,努力做好信息系统的“审计揭露”工作。为有效构建该平台,审计工作应予关注:(1)对既有的商业银行信息系统安全风险控制措施进行全面评价。这里的“全面”包括两层含义,一是评价每项风险控制措施设计的科学性与健全性,二是评价每项风险控制措施执行的有效性与全面性[15]。(2)结合评价小组有关控制措施的符合度赋值,定期运用信息熵模型与层次分析法,依据因果关联对不同层级下不同要项的安全风险等级进行例证描述,判别有关要素风险级别的高低,通过重要性原则对风险级别较高的管理要项及其控制措施实施重点审计。(3)基于上述步骤审计结论,对图1中第3层级的安全风险控制措施按照完善程度并结合 Φ 值体系,予以分级,其中,Ⅰ表示“问题重大”,Ⅱ表示“极不完善”,Ⅲ表示“较不完善”,Ⅳ表示“基本完善”,Ⅴ表示“完善”。审计主体同评价专家一起,通过互动平台或专题研讨等形式,快速完善Ⅰ—Ⅲ级控制措施并持续监控,定期检测Ⅳ—Ⅴ级控制措施并评价修正,切实做好安全风险控制策略的“审计揭露”。(4)开发“免疫自稳”软件,频繁检测漏洞与缺陷,及时修补与升级。该软件的研发理念是根据原有控制措施、目标控制标准以及既往运行经历,构

造自有“记忆”,当原有银行业务拓展附带产生深层次风险或原有控制措施最近一次失效时,会给予原有“记忆”刺激,此时该“记忆”会条件反射式地通过效应器做出响应,要求立即修正。

“免疫自稳”有被动自稳与主动自稳之分,除上述查找既有问题并被动性修正与自稳外,审计主体还应该借助于“免疫自稳”运行平台,完备商业银行运营系统全生命周期的安全防护机制,基于前瞻视角,积极做好主动性“免疫自稳”工作。审计主体开展主动自稳可从若干方面着手,如培育需求、规划、开发、测试、运维、下线的全流程安全自稳机制,基于审计经历保障商业银行信息系统安全功能的标准化、服务化与参数化,增强安全功能模块部署的自稳性、灵活性与一致性。此外,加大对敏感信息的审计力度,尤其要加强账户信息、客户数据等核心电子信息的审计保护,采用信息熵等既有成熟的安全风险评估实证模型,深层次估价银行用户敏感数据在创建、存储、运用、传导与销毁等环节中的风险程度,灵活采用泄密检测、数据脱敏、密码算法、边界防护、多因素认证以及访问控制等安全审计策略,辅助商业银行提升用户身份鉴别与认证的强度,依托审计力量切实防控敏感信息丢失、篡改、泄露与恶意访问等潜在风险。另外,审计主体需要协同商业银行共同制定信息系统全生命周期的安全防护要求,辅助商业银行完善新技术应用、新系统研发等安全自稳机制,做好新系统运营的审计自稳评估。总之,借助“免疫自稳”运行平台,审计主体应与商业银行一起,将“风险审计”与“免疫抑制”贯穿于商业银行信息科技活动全生命周期下的各个过程,强化风险应急处置的快速策应、修正与自稳程度,全方位覆盖风险评价、审计响应、问题揭露、应急自稳、处置恢复等各项环节。

3. 科学构建“免疫防御”运行平台

“免疫防御”是机体免疫系统通过正常免疫应答,阻止和清除外来入侵病原体及其毒素的一种功能,即抗外来感染免疫功能。审计主体需要科学构建“免疫防御”平台,对应信息系统不同形式的首次外来威胁及时制定控制措施,切实做好“审计抵御”。“免疫防御”分为非特异性免疫防御与特异性免疫防御两类,商业银行信息系统“免疫防御”也需从两方面入手。第一,从非特异性免疫防御分析,因其是机体在种系进化过程中形成的天然防御功能,是与生俱来的功能,所以,商业银行在成长的每一阶段都必须关注如何持续树立这一天然屏障。商业银行在规划组织制度时应该具有前瞻性,将内生性的信息系统安全风险控制规划融合于组织各项规章与制度的设计之下,将信息系统安全风险控制寓于组织的全面风险管理之中,仅有此,当外来威胁侵袭信息系统时,信息系统才能依赖天然屏障做好天然防御。第二,从特异性免疫防御分析,因其属于后天不断与病原体发生作用而使机体获得抗感染能力,因此,审计主体面对因商业银行信息系统运行范围拓展而出现的新问题,应该建立特定的流程对新风险进行初次鉴别与特定应答,科学制定安全控制措施。

审计人员的问题诊断、经验分析以及知识创造都将形成“新记忆抗体”,并纳入“免疫防御”平台下的“安全控制措施记忆库”,旨在为以后的同类外来威胁贡献有力的“免疫自稳”力量。商业银行的“免疫防御”工作,重在突出当运营系统面对危险与灾害时快速做出正确反应的策应能力。商业银行的“防御”与“自稳”,需要借助如下连续的行为过程实现。(1)变异。此过程下,审计主体通过既有经验、制度与文化的挖掘,重新配置资源,基于熵模型等手段,寻求可供选择的策略建议,基于方案的多样性进而强化系统的稳定性与适应性。(2)选择。此过程要求审计主体对多样化控制策略予以评价,检验各项安全策略究竟提升了现有“防御”模式的效应,还是重新提供了构建全新“防御”机制的机会,进而寻找特定议题下的最优答案。(3)记忆。该过程是一个抽象的过程,其是在“选择”的最优解下,对“免疫监视”与“免疫自稳”等过程的行为进行记录与经验总结。记忆的存储可以是书面的,如风险控制手册,也可以是隐性的,如专家成员的直觉、系统控制惯例或安全管理规则。

“免疫防御”有被动防御与主动防御之分,审计主体在实施“变异”“选择”与“记忆”等系列被动防御策略的基础上,还应借助“免疫防御”运行平台,积极开展主动防御活动。主动性“免疫防御”的方式有很多,如针对高级持续威胁(APT)、分布式拒绝服务(DDOS)等攻击手段,伪基站、网络钓鱼等

欺诈手段,审计主体需要定期开展攻防演练,培植重大安全威胁的挖掘、研判与处置能力,运用量子保密通信技术,增强系统安全防御水平。再如,由于当前商业银行信息科技安全风险的传导性持续强化,用户信息的全方位网络化与移动化促使第三方信息科技风险向商业银行传导的概率急剧攀升,为此,审计主体需要正确认知大数据、云计算、物联网等智能技术与商业银行业务运营相融合的本质规律,主动探索智能技术在商业银行应用的技术标准、安全指南以及实施规范,完善新兴智能科技的系统安全防御策略,强化移动互联网金融风险传导的安全抵御。此外,审计主体还要关注"协同防御"策略,加强运维管理与安全防控的协同运作,强化信息安全领域与网络安全领域的协调合作,在指标设计、制度规划、策应处置等方面实施流程共享,力争培植商业银行信息系统全生命周期"免疫防御"的长效机制。

参考文献:

[1]Trydid O M, Kavun S V, Goykhman M I. Synthesis concept of information and analytic support for bank security system[J]. Actual Problems of Economics, 2014, 11(161): 449 - 461.

[2]袁小勇. 论审计的本质[J]. 中国注册会计师, 2010(5): 33 - 39.

[3]张相锋. 安全审计与基于审计的入侵检测[D]. 北京:中国科学院, 2004.

[4]付钰, 吴晓平, 叶清, 等. 基于模糊集与熵权理论的信息系统安全风险评估研究[J]. 电子学报, 2010(7): 1489 - 1494.

[5]付沙. 一种基于信息熵的信息系统安全风险分析方法[J]. 情报科学, 2013(6): 38 - 42.

[6]马钢, 杜宇鸽, 荣江, 等. 基于威胁传播的复杂信息系统安全风险评估[J]. 清华大学学报:自然科学版, 2014(1): 35 - 43.

[7]刘国城, 王会金. 日志视角下信息系统安全审计的模型构建与风险控制[J]. 山东社会科学, 2012(9): 147 - 150.

[8]曾建光, 张英. 信息安全风险、内部控制有效性与审计师行为[J]. 山西财经大学学报, 2014(11): 112 - 124.

[9]彭友, 王延章. 信息系统内部安全审计机制[J]. 北京交通大学学报, 2009(4). 112 - 116.

[10]杨丹. 信息安全审计领域的领域分析和构件提取研究[J]. 现代计算机, 2011(4): 49 - 52.

[11]包捷, 吕智慧, 华锦芝, 等. 私有云环境下安全审计系统的设计与实现[J]. 计算机工程与设计, 2014(11): 3708 - 3712.

[12]张利, 彭建芬, 杜宇鸽, 等. 信息安全风险评估的综合评估方法综述[J]. 清华大学学报:自然科学版, 2012(10): 1364 - 1369.

[13]Shannon C E. A mathematical theory of communication[J]. The Bell System Technical Journal, 1948, 27(5): 378 - 656.

[14]赵丽芳, 于亚琼. 基于生物熵视角的国家审计"免疫系统"功能分析[J]. 审计研究, 2011(4): 53 - 57.

[15]刘国城, 杨丽丽. 面向内部威胁的中观信息系统内控管理研究[J]. 审计与经济研究, 2014(6): 49 - 55.

[责任编辑:刘　茜]

The Establishment of Security Audit Immune System about Commercial Bank Information System: from the Perspective of Empirical Estimate of Information System Security Risks

LIU Guocheng

(School of Accounting, Nanjing Audit University, Nanjing 211815, China)

Abstract: At present, the information system risk represents a serious threat to financial stability, it would become very important as to how to carry on an effective risk assessment and audit management for financial information system. This paper takes the theory of "audit immunity" as the theoretical guidance, and the "information entropy" as a key technology, and combines the hierarchical structure of financial risk information system. Then, the paper constructs an entropy model of risk assessment of financial information system on which the construction strategies of audit immune mechanism for financial information system are based and explored from the perspectives of "immune surveillance", "immune homeostasis" and "immune defense".

Key Words: commercial bank; information system audit; security audit; immune system; security risks; information entropy; audit immunity