国家审计理论建设专栏

大数据时代政务云安全风险估计及其审计运行研究

王会金[a],刘国城[b]

(南京审计大学 a.南京审计大学;b.会计学院,江苏 南京 211815)

[摘 要]云计算实践推进了政府以云技术为支持与多源大数据相融合的政务服务云建设。然而,政务云面临着严峻的安全问题,大数据泄露、内部滥用、外部侵袭以及技术漏洞等诸多风险因素制约着政务云的正常运行,基于风险导向模式开展政务云安全审计势在必行,其通过监控威胁行为与挖掘安全事件进行审计取证,促进云模式在电子政务领域的广泛应用。在理论回顾基础上,分析大数据下政务云安全风险评估方式并例证阐释,通过云提供商和云租户之间的责任划分建立政务云安全审计运行框架,基于管理、技术以及标准三个维度探索政务云安全审计的运行保障,旨在为大数据时代政务云安全管理实践提供建设性思路。

[关键词]大数据;云计算;电子政务;政务云审计;安全审计;云风险;熵权估计

[中图分类号]F239.43 [文献标志码]A [文章编号]1004-4833(2018)05-0001-11

当前,我国电子政务安全形势异常严峻。2014 年 10 月,国家互联网信息办公室主任鲁炜指出,我国 80% 的政府网站都曾受到过攻击,每个月有 1 万多个网站被篡改,地方政府网站成为黑客篡改的“重灾区”。2016 年 11 月,中国电信北京研究院发布的《2016 年上半年中国网站安全报告》指出,政府存在较多网络安全问题,漏洞的行政属性较为明显,区县及以下单位问题最多,合计有 25 万个高危漏洞,其次是各省市级单位,共曝出 10 万个高危漏洞,可以明确看到区县及以下级别单位的漏洞数量要明显高于部委、集团、省市级单位。在大数据时代,政府公共管理信息呈现数据量大、非结构数据占比增加以及数据类型繁多等特点,政务云处理日益复杂。Crowd Research 发布的《2017 年云安全报告》指出,安全人员不合格、安全工具滞后以及多样化安全问题对云安全管理提出挑战,数据泄露事件达到历史最高水平。2016 年至今,《国家电子政务“十三五”规划》以及国家标准《云计算数据中心基本要求》相继发布,其目的是建立完善政府信息系统安全管理制度规范,防范和化解云技术应用带来的潜在风险,制定政务部门计算机安全配置和审计制度,建立云安全检查制度,加强信息安全检查工作力度,大力提高电子政务信息安全保障水平,提升云安全保障能力。基于此,在网络信息安全以及云计算安全受到极大威胁的今天,政务云安全审计问题亟待国内学者深入重视。

一、相关理论回顾

政务云是政府行业以电子政务为中心,依托云计算技术,将单个政务“信息孤岛”进行资源整合,实现集中存储、调度灵活、资源共享、统一监管与资源节约而建立的电子政务资源协同互

[收稿日期]2018-06-10

[基金项目]国家社会科学基金项目(17BJY213)

[作者简介]王会金(1962—),男,浙江东阳人,南京审计大学党委副书记、副校长,教授,博士生导师,博士,从事审计理论与实务研究,E-mail:whjwc@nau.edu.cn;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,从事信息安全审计研究。

动，并向电子政务用户推送按需服务的集约化云服务平台[1]。政务云安全是云环境下电子政务稳健运行的根本保障，其关键目标是确保政务云系统自身的可控性、可靠性、安全性与一致性以及政务云服务资源的完整性、机密性、可用性与可核查性。近年来，有关云安全的理论研究主要集中于以下几方面：(1)云安全威胁。云管理员内部滥用可利用的安全漏洞以及不当的访问接口等诸多因素对云安全造成严重威胁[2-4]，可以通过贝叶斯网络、网络层次分析和自适应数据分类等方法建立模型评价相关云威胁[5-7]。(2)云安全技术。Lee 等和张晓娟等分析国外云安全技术标准建设[8-9]，林果园等与王于丁等研究基于云环境的访问控制技术框架，建立访问控制安全管理模型[10-11]，Kim 等、冯朝胜等与马友忠等分别探索基于云存储以及云数据索引等方面的安全技术和方法[12-14]。(3)云安全服务。Gilbert 等和闫莉等建立基于移动云计算的完整性检测模型，提出应用程序自动安全检测思路[15-16]，Oberheide 等和张伟等针对云环境发现蠕虫传播模型，提供 N－版本云端反病毒服务[17-18]，Chow 等和王中华等设计云端与用户之间双向身份认证的实现方案，构架基于云用户的隐式认证框架[19-20]。

我国有关政务云安全的理论研究相对缺乏，文献主要有姜茸等分析政务云的安全风险[21]，程桂枝和章谦骅探索政务云安全技术[22-23]，胡俊等设计电子云政务访问控制体系[24]，李卫东等研究云政务资源的安全保障机制[25]。政务云安全审计是以现代审计理念为核心，对政务云的内外在用户行为实施监督管理，对政务云处理步骤实施全过程追踪，记录政务云用户轨迹，检测滥用行为与安全漏洞，捕捉与监控各类政务云安全事件，提升政务云安全控制，完善政务云安全管理机制。目前，针对政务云安全审计的理论研究在我国尚未起步，如何将现代审计思想科学融入政务云安全理论建设之中，已成为 DT 时代审计学界亟待关注的问题。未来，政务云安全审计证据将大批量地以图片、音频、图像、视频以及 HTML 等方式呈现，且具有海量化特性，异构化大数据将对政务云安全审计的预处理、挖掘、分析与可视化等技术提出更高要求。在大数据时代，政务云安全审计实践将在我国广泛开展，其必然需要相关基础理论的广泛支撑。结合彭友的观点[26]，本文认为政务云安全审计应实现的目标具体为：(1)挖掘内部政务云用户的滥用行为与误用行为；(2)定位与发现政务云外部攻击的反复性尝试行为；(3)细致记载政务云访问行为的全面数据，对超越安全机制的威胁行为进行取证，检测与评价安全保护机制的运行效果，并针对安全风险采取相应审计措施；(4)发现政务云系统下软件即服务(SaaS)、平台即服务(PaaS)和基础设施即服务(IaaS)等层面的安全漏洞，若相关要素遭到破坏，即须评估损失并进行系统恢复；(5)审查政务云数据资源的权属划分不清、信息泄露、安全监督缺位、技术处理以及可信度等风险，发现相关审计证据；(6)判断政务云安全控制制度设计的科学性与健全性，评价政务云安全控制制度执行的实时性与有效性。

二、政务云安全风险估计与例证阐释

(一) 政务云安全风险分析

在大数据时代，政务云安全风险具有跨域渗透性、隐蔽关联性、泛在模糊性、交叉复杂性、集群风险性以及整体综合性等特征，对其开展审计管理必须综合各项风险因素。2006 年 2 月，财政部发布《中国注册会计师执业准则》，提出“了解被审计单位及其环境并评估重大错报风险”，这标志着审计模式已由传统的风险导向审计转化为以风险分析为中心的现代风险审计。对于财务审计而言，重大错报风险涵盖控制风险、经营流程风险、会计风险与战略风险。然而，针对政务云安全审计，因目前尚不需要编制安全审计报表，故并不存在重大错报风险这一说法。但是，政务云安全存在误报与漏查等问题，尽管误漏事项并未以报表形式反映，但是它们却以安全报告等其他形式体现在政务云安全控制体系之中。借此，本文将引入财务审计中的重大错报风险，并将其修正为重大误漏风险，基于实施领域风险、技术领域风险、管理领域风险与控制领域风险等层面对政务云风险体系实施评估。

图1列示了政务云安全重大误漏风险(总体风险)的层次结构。在实施领域,政务云战略目标制定、顶层设计以及长远规划是否存在疏漏,政务云内外在环境分析和全流程方案设计是否准确,政务云是否颠覆传统垂直堆叠并进行模式创新,政务云处理与运行过程是否规范科学,政务云各项目分类管理是否严谨精细,上述风险因素将诱发诸多政务云安全事故。在技术领域,虚拟技术是促进政务云资源实现平台化、标准化与共享化的基本工具,技术瑕疵会引发云用户的非法访问与恶意操作;有关云服务商的访问控制技术与身份验证技术存在设计缺陷,则政务云用户的密码与账号将会被其他用户越权访问或恶意修改,进而造成隐私泄露或数据修改[5];加密算法与密钥设计不成熟,将会导致数据的泄露与损毁;政务云安全审计在初始所获取的数据是粗糙的且逻辑关联极弱,必须通过大数据分析技术下的存储、移植、预处理、隔离、挖掘、可视化以及销毁等方法,才能实现大数据价值取证,云服务中弃用的安全数据若因销毁技术漏洞而在销毁后期被恶意恢复,则不严密的接口会将云平台暴露于诸多安全威胁之下,数据移植标准不统一造成云传输障碍,数据切分与隔离机制不完善造成云界限混乱,入侵检测与病毒防御等技术滞后引起外部攻击肆虐等,相关问题都会泄露云数据资源、盗用与滥用云用户信息或促使云服务中断。在管理领域,有关政务云安全的标准和规范尚未成熟健全,云安全管理人员必须具备电子政务、信息科学、计算机科学、数据科学以及管理学等学科领域经验,加之如今我国还没有完备的云服务管理流程与理念可供借鉴,这些都为政务云安全管理实践带来风险与挑战。在控制领域,有关政务云的安全制度设计是否完善以及是否有效执行,业务持续性与灾难恢复等规划是否科学等,相关事项直接影响着政务云的安全控制时效,进而增加政务云安全的控制风险。

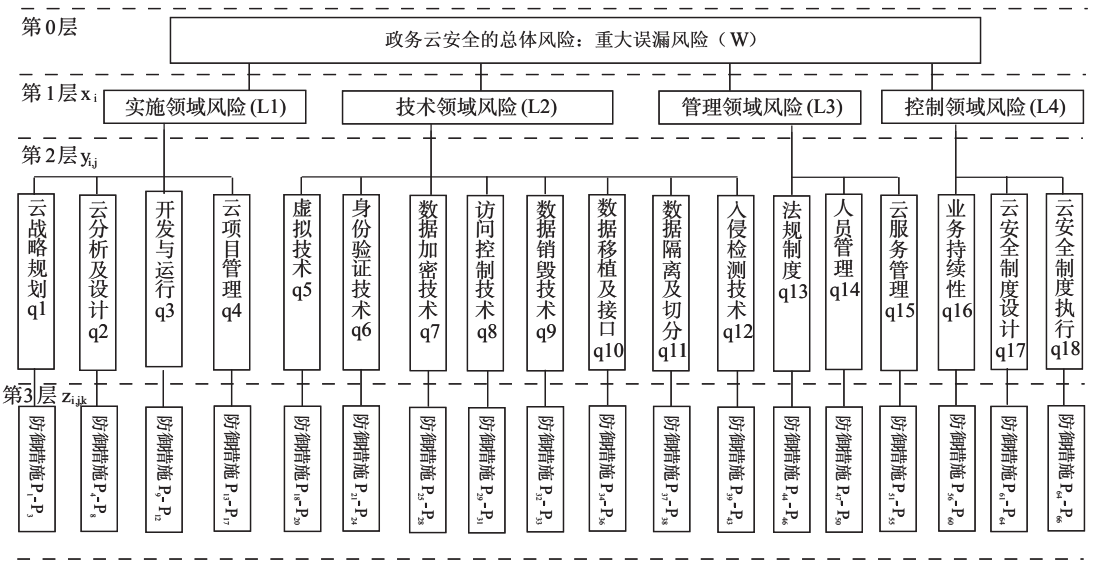

图1　政务云安全总体风险的层次结构图

图1中层级关联的解释如下:第0层表示政务云安全的总体风险;第1层为政务云安全风险的4项管理要素,X_i代表其概率权重;第2层为政务云安全风险的第i个管理要素下所属的具体管控目标,Y_{ij}代表其概率权重;第3层为第i个管理要素下第j个管控目标中的相应风险防御措施,Z_{ijk}代表其概率权重,第3层涵盖若干风险防御措施,并形成政务云安全风险控制的有机体系。图1仅标识66项措施,当然,不同政务云的风控措施项数不尽相同,应视具体情况而定,但该风险防御的终端措施体系将是政务云风险实证估计以及微观管控的根基之所在。

(二)政务云安全风险估计

政务云安全风险估计是指梳理政务云安全威胁,分析有关历史信息,采用数学模型或统计工具,对政务云安全事故的发生概率及其相关损失开展定量推断与预测的过程。在传统时代,政务云安全

风险估计可选用概率分析、因素分析、层次分析、德尔菲与决策树等方法。在大数据时代，安全风险估计将广泛融合人工智能经典模型，熵权理论、机器学习、灰色理论、粒子群优化理论、DS 证据理论、BP 神经网络以及贝叶斯理论等将成为主流方法。丁楠归纳大学生自杀风险的作用机制，对风险因素子序列实施复杂度分析，运用支持向量机方法建立大学生自杀风险估计的预测函数[27]；林云威等构架层次分析与 D－S 证据相融合的工业控制系统安全风险评估方法[28]；薛晔等采纳分布滞后模型分析通货膨胀影响因素的乘数效应，借助决策树算法遴选通货膨胀影响指标，运用 BP 神经网络估计通货膨胀的风险等级[29]；肖奎喜等探索应收账款各个风险变量的逻辑关联，建立应收账款风险估计的贝叶斯网络模型，提出信用交易的特定有向图描述[30]。已有文献横向扩展了相关方法的基础应用，各类风险评估技术的基本原理具有唯一性，关键是如何做好共性和规律的实践运用，政务云安全风险估计也不例外，上述方法对其普遍适用。熵权法是信息安全模糊风险估计的基本方法之一，本文选其为对象对政务云安全风险估计方案进行描述。1865 年，Glausius 提出熵权概念，并用其代表能量在空间中分布的均匀程度。1948 年，Shannon 将“信息熵”界定为“若系统有 n 种不同的状态，即 S_1，S_2，…，S_n，每种状态对应概率分别为 p_1、p_2、…、p_n，则该系统具有不确定信息量 H（熵）可以表示为：$H = -\sum^{n} p_i \ln p_i$。公式中，$p_i$ 满足：$0 \leqslant p_i \leqslant 1 (i = 1, 2, \cdots, n)$，$\sum^{n} p_i = 1$”[31]。本文引入熵权方法，并将政务云安全风险评估步骤具体设计如下[32]。

1. 建立特定政务云下安全风险（重大误漏风险）的层次结构（图 1），结合实际正确设计结构图上第 3 层防御措施的符合度权重范围，正确划分政务云安全风险的标准等级

2. 针对政务云安全风险层次结构，对第 3 层（P 层）防御措施符合度权重 Z_{ijk} 进行赋值

3. 针对政务云安全风险层次结构，计算第 2 层（q 层）诱发因素的熵权系数 Y_{ij} 和风险权向量 U_{ij}

$$Y_{i,j} = -\frac{1}{\ln e}\sum_{k=1}^{e} Z_{i,j,k} \ln Z_{i,j,k} U_{i,j} = (1 - Y_{i,j}) / \left(d - \sum_{j=1}^{d} Y_{i,j}\right), 0 \leqslant U_{i,j} \leqslant 1, \sum_{j=1}^{d} U_{i,j} = 1$$

其中，d 为第 i 个风险要素所属的诱发因素的数量，e 为第 i 个风险要素下第 j 项诱发因素所属防御措施的数量。

4. 针对政务云安全风险层次结构，计算第 1 层（L 层）风险要素的熵权系数 X_i 和风险权向量 U_i

$$X_i = -\frac{1}{\ln d}\sum_{j=1}^{d} Y_{i,j} \ln Y_{i,j}, U_i = (1 - X_i) / \left(g - \sum_{i=1}^{g} X_i\right), 0 \leqslant U_i \leqslant 1, \sum_{i=1}^{g} U_i = 1$$

其中，g 为云政务安全总体风险（重大误漏风险）下风险要素的数量。

5. 针对政务云安全风险层次结构，计算第 0 层（W 层）政务云安全总体风险（重大误漏风险）的熵权系数 S 和风险权向量 U

$$S = -\frac{1}{\ln g}\sum_{i=1}^{g} X_i \ln X_i, U = 1 - S, \text{且 } 0 \leqslant S, U \leqslant 1。$$

6. 分析风险层次结构下各层次相关要项的风险量值，并进行风险评价

在大数据时代，人工智能将广泛应用于政务云安全风险评估领域，其优势是能够避免风险评估方法中的主观判断。熵权法下，Z_{ijk} 赋值依赖于专家自主认知，相关结论不免存在偏差。为此，在政务云风险估计中可将多种方法进行整合，如将机器学习引入熵权法，通过计算机行为模拟逐步替代专家赋值；将熵权与模糊评价相协同，建立风险评判集下的隶属度矩阵，依托各层级熵权风险向量值确定风险等级[33]。在数据信息无序以及亟须量化度量等情形下，强化人工智能多模型的整合应用，将使得政务云安全风险估计更为客观可靠[34]。

（三）熵权估计的例证阐释

本文以江苏省某政府部门的政务云平台安全作为案例分析。首先，结合行业背景，分别界定和描

述政务云安全要项符合度量化范围(表1)和政务云安全风险等级标准(表2);其次,构造该政务云平台安全总体风险(重大误漏风险)的层次结构(图1),并集合15名专家,依托政务云重大误漏风险的属性特征,结合表2,依据自主认知运用德尔菲法对图1中66项防御措施的符合度Z_{ijk}进行赋值,数值见表3;最后,相关计算过程如下。

表1 政务云安全要项符合度的量化及描述

符合度	量化值与范围	符合程度措施
*V*1 不符合	$V=0$	政务云无任何相应的安全控制措施
*V*2 不太符合	$0<V\leqslant 0.25$	政务云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
*V*3 基本符合	$0.25<V\leqslant 0.60$	政务云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
*V*4 较好符合	$0.60<V\leqslant 0.80$	政务云有较好的安全控制措施,但未能起到较好的效果
*V*5 完全符合	$0.80<V<1.00$	政务云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
*V*6 完全符合	$V=1.00$	政务云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 政务云安全风险等级的界定及描述

等级	量化值与范围	影响描述
*U*1 可以忽略	$U=0$	对政务云的危害程度微乎其微,可以不予考虑
*U*2 较小	$0<U\leqslant 0.15$	政务云危害会造成一些很小的影响,只需较小的努力就可以弥补
*U*3 程度中等	$0.15<U\leqslant 0.35$	政务云危害将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
*U*4 较大	$0.35<U\leqslant 0.70$	政务云的危害可导致数据的较大损失,即使付出很大的努力也难于弥补
*U*5 极为关键	$0.70<U<1.00$	政务云的危害可引起灾难性的损失,或直接导致业务的中断或关闭
*U*6 完全风险	$U=1.00$	政务云的危害导致系统安全几乎处于瘫痪状态,业务随时中断与关闭

1. 针对图1,计算q层的熵权系数Y_{ij}和风险权向量U_{ij}

$$Y_{11}=-\frac{1}{\ln e}\sum_{k=1}^{e}Z_{1,l,k}\ln Z_{1,l,k}=-(0.45\times\ln 0.45+0.69\times\ln 0.69+0.71\times\ln 0.71)/\ln 3=0.7815$$

同理:$Y_{12}=0.7234$;$Y_{13}=0.6210$;$Y_{14}=0.6638$;$Y_{21}=0.7209$;$Y_{22}=0.6735$;$Y_{23}=0.7847$;$Y_{24}=0.8125$;$Y_{25}=0.6920$;$Y_{26}=0.7652$;$Y_{27}=0.6110$;$Y_{28}=0.8613$;$Y_{31}=0.6317$;$Y_{32}=0.6577$;$Y_{33}=0.7440$;$Y_{41}=0.8305$;$Y_{42}=0.7166$;$Y_{43}=0.7091$。

$$U_{11}=(1-Y_{1,l})/(d-\sum_{j=1}^{d}Y_{1,l})=(1-0.7815)/[4-(0.7815+0.7234+0.6210+0.6638)]=0.1805$$

同理:$U_{12}=0.2284$;$U_{13}=0.3134$;$U_{14}=0.2777$;$U_{21}=0.1342$;$U_{22}=0.1574$;$U_{23}=0.1035$;$U_{24}=0.0901$;$U_{25}=0.1481$;$U_{26}=0.1129$;$U_{27}=0.1871$;$U_{28}=0.0667$;$U_{31}=0.3810$;$U_{32}=0.3542$;$U_{33}=0.2648$;$U_{41}=0.2278$;$U_{42}=0.3811$;$U_{43}=0.3911$。

2. 针对图1,计算L层的熵权系数X_i和风险权向量U_i

$$X_1=-\frac{1}{\ln d_j}\sum_{j=1}^{e}Y_{l,j}\ln Y_{1,j}=(0.7815\times\ln 0.7815+0.7234\times\ln 0.7234+0.6210\times\ln 0.6210+0.6638\times\ln 0.6638)/\ln 4=0.7175$$

同理:$X_2=0.8416$;$X_3=0.7151$;$X_4=0.5795$。

$$U_1=(1-X_1)/\left(g-\sum_{i-1}^{g}X_i\right)=(1-0.7175)/[4-(0.7175+0.8416+0.7151+0.5795)]=0.2464$$

同理:$U_2=0.1383$;$U_3=0.2485$;$U_4=0.3668$。

3. 针对图1,计算W层的熵权系数S和风险权向量U

$$S=-\frac{1}{\ln g}\sum_{i=1}^{g}X_i\ln X_i=-(0.7175\times\ln 0.7175+0.8416\times\ln 0.8416+0.7151\times\ln 0.7151+0.5795\times\ln 0.5795)/\ln 4=0.6775$$

$$U = (1 - S) = (1 - 0.6775) = 0.3225$$

表 3　江苏省某政府部门政务云安全风险权向量的赋值与计算

基元层（W）	总体风险 $U=0.3225$																	
第 1 层（L）	$U_1=0.2464$				$U_2=0.1383$								$U_3=0.2485$			$U_4=0.3668$		
第 2 层（q）	$U_{1,1}$ 0.1805	$U_{1,2}$ 0.2284	$U_{1,3}$ 0.3134	$U_{1,4}$ 0.2777	$U_{2,1}$ 0.1342	$U_{2,2}$ 0.1574	$U_{2,3}$ 0.1035	$U_{2,4}$ 0.0901	$U_{2,5}$ 0.1481	$U_{2,6}$ 0.1129	$U_{2,7}$ 0.1871	$U_{2,8}$ 0.0667	$U_{3,1}$ 0.3810	$U_{3,2}$ 0.3542	$U_{3,3}$ 0.2648	$U_{4,1}$ 0.2278	$U_{4,2}$ 0.3811	$U_{4,3}$ 0.3911
第 3 层（p）符合度	$Z_{1,1,1}$ 0.45 $Z_{1,1,2}$ 0.69 $Z_{1,1,3}$ 0.71	$Z_{1,2,1}$ 0.53 $Z_{1,2,2}$ 0.85 $Z_{1,2,3}$ 0.82 $Z_{1,2,4}$ 0.75 $Z_{1,2,5}$ 0.59	$Z_{1,3,1}$ 0.71 $Z_{1,3,2}$ 0.79 $Z_{1,3,3}$ 0.75 $Z_{1,3,4}$ 0.75	$Z_{1,4,1}$ 0.69 $Z_{1,4,2}$ 0.72 $Z_{1,4,3}$ 0.85 $Z_{1,4,4}$ 0.77 $Z_{1,4,5}$ 0.72	$Z_{2,1,1}$ 0.69 $Z_{2,1,2}$ 0.65 $Z_{2,1,3}$ 0.69	$Z_{2,2,1}$ 0.76 $Z_{2,2,2}$ 0.72 $Z_{2,2,3}$ 0.76 $Z_{2,2,4}$ 0.65	$Z_{2,3,1}$ 0.54 $Z_{2,3,2}$ 0.70 $Z_{2,3,3}$ 0.71 $Z_{2,3,4}$ 0.68	$Z_{2,4,1}$ 0.64 $Z_{2,4,2}$ 0.58 $Z_{2,4,3}$ 0.63	$Z_{2,5,1}$ 0.71 $Z_{2,5,2}$ 0.72	$Z_{2,6,1}$ 0.55 $Z_{2,6,2}$ 0.68 $Z_{2,6,3}$ 0.70	$Z_{2,7,1}$ 0.73 $Z_{2,7,2}$ 0.78	$Z_{2,8,1}$ 0.69 $Z_{2,8,2}$ 0.72 $Z_{2,8,3}$ 0.50 $Z_{2,8,4}$ 0.63 $Z_{2,8,5}$ 0.69	$Z_{3,1,1}$ 0.71 $Z_{3,1,2}$ 0.77 $Z_{3,1,3}$ 0.70	$Z_{3,2,1}$ 0.80 $Z_{3,2,2}$ 0.62 $Z_{3,2,3}$ 0.71 $Z_{3,2,4}$ 0.78	$Z_{3,3,1}$ 0.54 $Z_{3,3,2}$ 0.66 $Z_{3,3,3}$ 0.79 $Z_{3,3,4}$ 0.83 $Z_{3,3,5}$ 0.70	$Z_{4,1,1}$ 0.71 $Z_{4,1,2}$ 0.61 $Z_{4,1,3}$ 0.74 $Z_{4,1,3}$ 0.54 $Z_{4,1,5}$ 0.72	$Z_{4,2,1}$ 0.68 $Z_{4,2,2}$ 0.52 $Z_{4,2,3}$ 0.83 $Z_{4,2,4}$ 0.72	$Z_{4,3,1}$ 0.82 $Z_{4,3,2}$ 0.55

熵权通过对系统有序程度的衡量，实现了信息的量化度量。表 3 中的 U 值体系隐含如下结论：(1)从第 0 层看，该政府部门政务云安全的总体风险数值为 0.3225，介于表 2 中的 0.15—0.35 之间，风险程度中等，存在较为严重的政务云威胁；(2)从第 1 层看，$U_4 > U_3 > U_1 > U_2$，这说明控制领域风险 *I4* 数值最高，U_4 大于 0.35，属于较大程度风险级别，U_2 小于 0.15，属于较小程度风险级别，U_3 和 U_1 介于 0.15—0.35 之间，属于程度中等风险；(3)从第 2 层看，控制领域风险 *I4* 所对应的管控要项为 *q*16、*q*17 与 *q*18，它们对应的 U 值分别为 0.2278、0.3811 与 0.3911，*q*17 与 *q*18 的 U 值介于 0.35—0.70之间，这说明 *q*17 与 *q*18 所代表的该政府部门政务云的安全控制风险程度较大，影响政务云正常运行，安全制度设计不够科学，安全制度执行不够有效，如果政务云发生安全事故，尽管付出较大努力，政务云资源损失也将难以弥补。

三、政务云安全审计运行框架的理论探索

政务云安全审计是对政务云安全风险的综合治理，审计主体应通过对 Iaas、Paas 与 Saas 层级下实施技术以及管理等领域的固有风险进行职业判断，评价政务云相关层级的控制领域风险，开展实质性测试，优化审计流程，并将政务云安全审计的检查风险降至可接受水平。针对不同审计对象，政务云安全审计内容差异巨大，内在构成分属于不同审计类型。图 2 列示了大数据时代政务云安全审计运行的框架结构，基于审计对象的层面分析具体如下。

（一）政务云提供商

对政务云提供商实施审计意在保障云的安全，所划定的审计内容包括：(1)物理设备安全，主要为基础设施与网络设施等要项的安全审计。审计主体应检查云机房、云主机、虚拟主机、服务器、存储器等基础设施以及路由器与交换机等网络设备的自身安全以及环境安全。(2)虚拟运营安全，主要为虚拟化安全、API 接口与云系统漏洞等要项的安全审计。虚拟化是实现云计算的最关键技术之一，审计主体应评价 AMD－V、VT－x 等虚拟化技术以及 Hyper－V、VMWare 等虚拟化软件的设计与应用是否成熟，是否向政务云租户提供安全性、可拓展性、隔离性以及资源充分利用性的保障，是否基于虚拟服务控制台、数据管理与恢复和网络管理等若干对象实现相关要素之间的逻辑隔离，虚拟机之间的通信机制是否安全可靠，是否建立合理统一的虚拟化安全方针。云 API 暴露于云应用风险之中，审计主体需要运用注入式攻击等策略审查云 API 设计的严谨性，并运用跨站伪造等手段测试 API 运行维护是否成熟。政务云系统漏洞所引发的损失不可估量，且其融合于其他要项的安全审计之中，审计主体需要采用分布式云爬虫或云任务分配机制等方法，对政务云系统开展漏洞测试或渗透测试，检查政

务云系统设计与开发的缺陷、威胁响应措施以及关键系统补丁修复机制。(3)数据安全,在DT时代,云系统中的日志数据、图片数据以及视音频数据将成为安全审计大数据的主导,审计主体应基于SAN、DAS、NAS、弹性拓展等系列适用技术检查云存储设计,基于Hadoop平台、MapReduce框架、Pig流处理以及Avro工具等评价云计算安全,基于维入栈、矢量场以及Protovis等工具测试云系统数据可视化的处理效应。(4)服务与管理。审计主体应关注云服务模式是否成熟,即云系统服务是否专业、准确与合理,关注云服务制度是否完善,即制度设计与执行是否全面有效,关注云网络运行是否快速便捷,问题是否及时反馈,对数据库是否拥有成熟与严格的管理,提升风险估计水平,及时开展相关方面的动态控制测试。

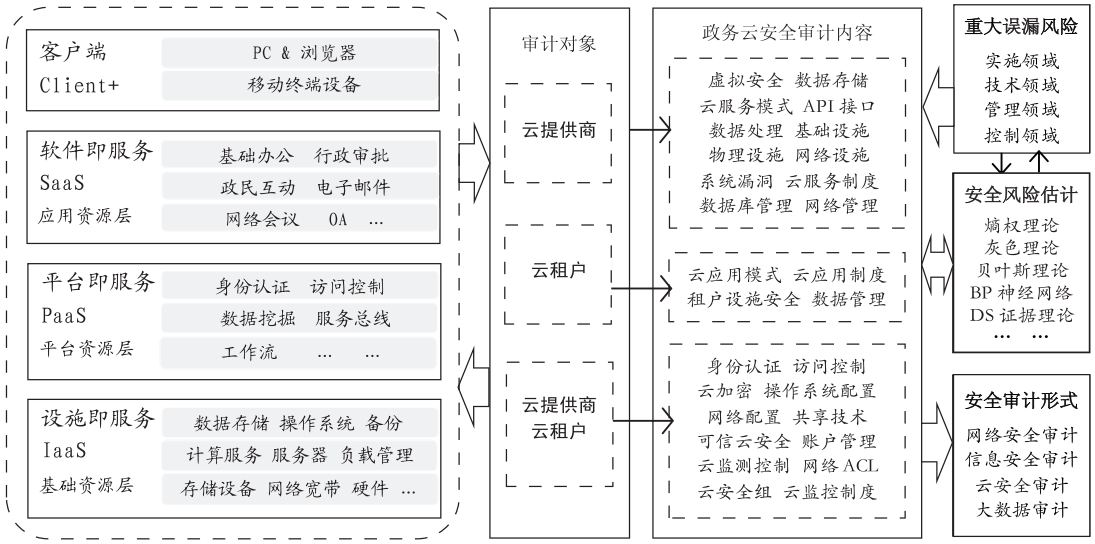

图2 大数据时代政务云安全审计的运行框架设计

(二)政务云租户

对政务云租户开展审计意在保证云中的安全,所确立的审计运行内容涵盖:(1)大数据管理。借鉴王志英等观点[35],政务云租户数据资源面临着诸多风险,具体有云服务器意外宕机或中断,云数据通信被窃听,黑客对云可用性攻击,云提供商查阅、操纵、泄密、遗失以及意外修改用户敏感数据,云系统自身可用性问题而泄露或意外修改用户敏感数据,用户访问政务云数据信息失败以及数据在传输途中被操纵或被意外修改。政务云租户数据安全的基本属性为机密性、真实性、完整性、可用性与可控性。针对云租户,审计主体应检查在购买云服务前是否制定科学的数据擦除方案,是否遴选访问控制严格以及服务水平较高的云提供商,是否安装正确的杀毒软件防御数据篡改并推进软件的实时升级与更新,是否加强云中敏感数据的安全保护,是否回避将机密数据信息放置云系统而移植至特定独立存储器,是否在修改关键数据信息之前运用备份管理备份归档,是否定期对自身的云中数据信息进行一致性检查与维护以及是否及时提示与告知供应商相关问题以减少宕机或服务中断的概率。此外,审计主体还需基于政务部门的特定背景,评价云政务部门数据中心逻辑整合率、部门之间数据共享交换能力、数据共享交换平台接入率以及云政务部门数据中心资源使用提升率等,对政务云数据应用的效率安全与效用安全实施审计取证。(2)制度与应用。审计主体需要监督政务云租户的应用模式、应用制度及其设施安全,审查IaaS层级下物理设备与网络设施、PaaS层级下开发平台与网络程序以及软件平台与技术程序的应用行为是否合理合规,应用过程是否存在人为的误用与滥用,是否拥有资源、能力与经验以及是否推出有关控制策略及时应对此方面威胁,相关内控制度是否健全有效,是否构建政务云应用下切实可行的监测

预警机制，查验政务云租户的物理设备是否安全可靠。

（三）云提供商与云租户

政务云提供商与政务云租户是重要的云安全协作伙伴，诸多安全风险需要双方协同管理。针对两者所联合开展的审计运行工作有：（1）身份认证与访问控制。审计主体应检查云用户身份的提供、认证与注销模式，监测网络 ACL 以及云端访问控制的服务过程。政务云认证模式可以基于服务为中心，也可以基于租户为中心，身份认证方式有数字证书、生物扫描、单次密码、双因子密码、物理密钥与 Kerberos 等类型，审计主体需要研判所划定云用户主体的访问级别，抽检数据使用者是否具备非法的访问权限，验证是否根据授权规则赋予用户访问权利，分析现有访问方式是否适用于云认证安全，判别云端访问管理与云租户 IT 管理之间在云用户的新增与注销等方面是否协调有序，追踪认证失败和盗号事件等事项的异常访问轨迹，推进相关日志取证。（2）隐私保护与动态加密。隐私安全横跨基于大数据的政务云计算全生命周期，动态加密能够有效提升政务云应用安全水平。审计主体应检查政务云加密算法是否存在缺陷，分析对称或非对称加密的密文检索、加密字符串模糊检索、桶划分和分布概率映射思想的保序对称加密以及向量标量积的对称加密等方法究竟哪类更适应被审云加密环境，核验密码设备安全性，查验 PKI 证书签名的准确性，测试密钥管理是否存在安全漏洞。（3）可信云安全。审计主体需要测试政务云租户端附加可信计算模块所属可信链的安全程度，验证被审政务云下以可信密码学为基础的可信云技术的成熟度以及是否能够全面防止通信被截获，监督云用户是否从可信云服务数据中心安装 APP 软件并普遍适用，检查云－端互动的信任根“零知识证明”挑战应答的准确性，评价基于可信模式识别的云终端启动与云接入的完善性以及基于可信融合验证的云－端互信的真实性。（4）病毒防御与安全监控。政务云易于遭受 DoS、音频隐写以及僵尸网络等各类病毒攻击，审计主体应测试云安全组以及云系统病毒防御体系的有效性，安装具有防火墙功能的杀毒软件是否高效并及时修补漏洞，基于挖掘算法开展云环境下的入侵检测取证。针对漏洞威胁，审计主体需要评价被审政务云的安全监控机制，审阅云虚拟化的监控行为与制度，查看有关软件内部安全以及云共享技术安全的事前设计、事中控制与事后响应。（5）其他事项。审计主体需要充分掌握政务云提供商与政务云租户之间的协同情况，在操作系统配置和网络配置等方面，判定云提供商是否满足云租户差异化、个性化、多样化与自主化的决策需求，是否基于无缝对接进而避免政务云缺陷。此外，审计主体还需关注双方的云安全恢复机制，是否采纳自动解析与语义跟踪重放等方法设计政务云安全的整体恢复模式以及是否运用 RX 或 Flashback 等技术建立政务云安全的局部恢复策略。

四、政务云安全审计运行的保障分析

政务云安全审计体系的孕育是知识创新的过程。审计部门是创新的主体，是推动创新创造的生力军。未来大数据与云计算将与审计运行深度融合，针对日趋复杂的科技风险，传统审计思想已无法适应政务云安全审计的多层次需求，审计主体必须全面推进运行保障的理念创新，积极顺应新时代审计体制改革的时代趋势，寻求全新的智慧，确保云政务安全审计的动态化发展之路。

（一）审计组织与管理

组织是将散乱要素加以集聚，管理是将资源要素有机整合，两者是政务云安全审计目标得以实现的基本前提。审计主体在优化自身组织与管理中应关注如下策略：（1）通盘筹划。审计主体应高度重视大数据时代的政务云安全审计建设，并做好顶层设计与统筹协调。首先，云安全审计正经历着传统审计的理念变革，传统审计以财政财务审计、财经法纪审计与经济效益审计为重心，侧重于事后经济监督，而现代政务云安全审计横跨审计科学、大数据科学、云计算、信息科学、网络科学、计算机科学、安全科学以及电子政务等若干学科领域，承载着以估计、识别、测试、评价、揭露、自稳、抵御、监测、预警为主导的一体化任务体系。其次，事前对政务云安全审计开展全局设计与科学筹划极为关键，审

计主体需要全局考量政务云各安全要素与各安全层次,统揽全局、追根溯源,统筹考虑风险评估、过程分析、证据可视化、监测预警、云数据跟踪、云漏洞防御等各项环节,基于全局视角求证政务云安全问题的审计之道。(2)队伍建设。2018 年 5 月 28 日,习近平总书记在两院院士大会中提出“功以才成,业由才广。创新之道,唯在得人”。审计机构有必要引入多学科专业人才,合理设置审计队伍的年龄结构与学历层次,定期聘请业界专家开展广泛交流,制定切实可行的人才培养计划,设计正确的审计人才评价制度,孕育完善的人才使用机制、人才激励机制与人才竞争机制。这是因为政务云安全审计的属性要求审计人员必须胜任被审云系统下各方面的运作,熟悉政务云的产业环境、租户信赖度、业态成熟度、法律环境、监管环境以及国际安全环境等,培植以学科融合为导向的“审计通才”是队伍建设的宗旨,而优秀的策略、计划、制度与机制是保障。(3)协同文化。在智能科技时代,政务云安全审计融合诸多学科知识,审计与云安全的理念冲突、审计方法与云计算技术差异、审计专家与云计算专才的认同危机以及审计参与者的话语权等都将削弱审计团队文化。审计机构应积极塑造优秀的团队协同文化,基于质量管理推进有关于政务云安全审计的专业整合、经验互补、信息互换、成果共用、方法共建与优势共享的协同建设[36],平等互助、责权利分明、契约互信、尊重差异,培育协作创新的审计文化愿景,强化新时代审计体制创新的内在驱动力。

(二) 审计技术与方法

近年来,新一轮技术变革推进了国家政务的机制重塑。然而,与政务云发展相比,其审计技术与方法并未与时俱进。未来审计主体针对政务云安全审计方法应做的努力主要涵盖如下方面:(1)信息安全审计。审计主体应熟悉信息安全学科体系,基于各个层面深化政务云审计技术;针对信息内容安全审计范域,需要掌握信息获取、分析、识别、管理与控制等技术;针对信息系统安全审计范域,需要精通系统的软硬件安全、安全测评认证、访问控制以及安全等级保护等技术;针对密码学审计范域,需要通晓量子保密、生物密码、密码协议、公钥密码、对称密码以及密码应用等技术;针对信息对抗审计范域,需要了解电子对抗、光电对抗以及计算机软硬件对抗等。有关于政务云信息的秘密性、完整性与可用性等属性审计及其设备安全、数据安全、内容安全和行为安全等内涵审计,均需上述方法作为全方位支撑。(2)网络安全审计。网络安全集中于区域边界、网络通信、VPN 系统、入侵检测和防火墙等层面,审计主体应基于上述要项获取各类政务云网络安全审计技术;对于 web 流量安全,采用网络级、传输级与应用级等技术;对于网络边界防御,采用网闸、多重网关和数据交换网等技术;对于区域通信安全,采用数据加密、数字签名、通信认证和通信对抗等技术;对于 VPN 系统安全,采用 IPsec VPN 与 SSL VPN 等技术;对于入侵检测,采用阈值检测、轮廓检测、异常检测和渗透鉴别等技术;对于防火墙安全,采用状态检测、NAT、包过滤、NAT 与代理等技术;对于网页内容检测,主要采用 DFI 与 DPI 两类审计方法。(3)云安全审计。可信云安全审计主要表现为云服务的保密性审计与完整性审计[37]。针对可信数据存储外包,主要采用基于时间、基于策略或基于云存储的文件确定删除、数据可恢复证明、云可信访问控制以及云密文检索等审计方法;针对可信计算外包,主要采用基于全同态加密证明、交互式证明、数学验证与变换以及基于多副本的完整性保护等审计方法;针对可信虚拟机外包,主要采用基于可信计算的验证执行、VM 安全监控与完整性度量等技术。此外,面对政务云虚拟化安全问题,审计主体需要具备宿主机安全、虚拟机隔离、Hypervisor 安全以及虚拟机的监控、防护与检测等审计技能。(4)大数据审计。面对海量政务云安全数据,审计主体应熟练运用并进行计算、采用 Oracel、数据挖掘、SQL、机器学习、预测性分析和 R 语言等大数据审计技术,充分利用审计大数据采集、存储、预处理、挖掘、分析与可视化平台,大幅提升政务云安全审计取证的效率与效应。

(三) 审计标准与规范

2017 年 7 月,发改委印发的《“十三五”国家政务信息化工程建设规划》指出,按照“数、云、网、端”融合创新趋势,建成统一的国家电子政务网络,提升其承载服务和安全保障能力。然而,有关政

务云安全审计的法规与制度在我国尚缺,亟待一系列相对成熟的标准及规范对安全审计实践予以指导。针对此现状,审计主体需要借鉴:(1)国内政府云计算安全指南。2014 年 2 月,《基于云计算的电子政务公共平台顶层设计指南》发布,为政务公共平台建设提供安全制度支持。2015 年 5 月,网信办分别发布国家标准《信息安全技术:云计算服务安全指南》与《信息安全技术:云计算服务安全能力要求》,提出云服务安全管理基本要求以及 10 类云服务安全能力规定。2016 年 1 月,《基于云计算的电子政务公共平台 9 项标准》发布,提出系统架构、功能和性能要求、安全规范、信息资源安全要求、数据管理技术规范、系统和数据接口技术规范、服务质量评估规范以及服务测试规范。(2)国外政府云计算安全标准。在美国,NIST 机构发布信息安全控制指南、云计算安全参考体系架构、公有云安全与隐私指南以及 FedRAMP 云项目,云安全联盟(GSA)发布的 STAR certification 计划。在欧盟,ENISA 机构发布云安全保障框架、云合同安全服务水平监测指南和政府云安全框架。在澳大利亚,AGIMO 机构发布云服务指南、政府机构的隐私及云计算、云管理盘点、云档案管理以及云计算政策。(3)其他网络信息安全控制规范。ISACA 发布《信息系统审计准则》,阐释了信息系统审计的基本准则、审计指南与作业程序。COBIT 框架提供了信息技术控制目标的基本标准。SC27 信息安全国际标准提出信息安全管理度量方法以及 ISMS 控制指南。BS7799 标准推出信息安全管理的 10 个要项、36 个总体目标、127 项控制目标以及 500 余项控制要点。此外,基于国家层面,政府机构有必要全方位制定有关政务云安全的审计标准与规范。政务云安全涉及 IaaS、PaaS 与 SaaS 层级的各个方面,因此,对于系列审计标准的制定,政府应予强化统筹规划,融合云应用开发商、云系统构建商、云设备提供商、云服务销售商、云服务部署交付商、云服务运营商以及政务云租户等各利益主体的权责分工,评价实施、技术、管理与控制等领域风险,汲取国内外先进理论经验,通盘设计政务云安全审计的执业标准、质量尺度、技术要求与作业指南,力求通过制度与规范保障政务云安全审计标准化工作的顺利实施。

参考文献:

[1]刘国城. 基于过程的电子政务云安全审计模式研究[J]. 新疆大学学报:哲学·人文社会科学版,2016(1):28-35.

[2]Kandias M, Virvilis N, Gritzalis D. The insider threat in cloud computing[J]. Springer Berlin Heidelberg, 2013, 83(10): 93-103.

[3]姜茸,马自飞,李彤,等. 云计算安全风险因素挖掘及应对策略[J]. 现代情报,2015(1):85-90.

[4]王国峰,刘川意,潘鹤中,等. 云计算模式内部威胁综述[J]. 计算机学报,2017(2):296-316.

[5]Wang P, Lin W H, Kuo P T, et al. Threat risk analysis for cloud security based on attack-defense trees[J]. International Conference on Computing Technology, 2012, 1(2): 106-111.

[6]张银燕,李弼程,崔家玮. 基于云贝叶斯网络的目标威胁评估方法[J]. 计算机科学,2013(10): 127-131.

[7]高杨,李东生,雍爱霞. 结合网络层次分析法的云推理威胁评估模型[J]. 计算机应用研究,2016 (11):3430-3434.

[8]Lee C, Kim S, Yeo Y, et al. Proposal of security requirements based on layers and roles for the srandardization of cloud computing security technology[J]. Journal of Security Engineering, 2013, 10(4): 473-488.

[9]张晓娟,郭娟. 国外政府云计算安全标准建设及启示[J]. 电子政务,2016(4):83-90.

[10]林果园,贺珊,黄皓,等. 基于行为的云计算访问控制安全模型[J]. 通信学报,2012(3): 59-66.

[11]王于丁,杨家海,徐聪,等. 云计算访问控制技术研究综述[J]. 软件学报,2015(5): 1129-1150.

[12]Kim C S, Jang B I, Jung H K. A study on the security technology for introduction the secure cloud computing service[J]. Journal of Security Engineering, 2013, 10(5): 567-580.

[13]冯朝胜,秦志光,袁丁. 云数据安全存储技术[J]. 计算机学报,2015(1):150-163.

[14]马友忠,孟小峰. 云数据管理索引技术研究[J]. 软件学报,2015(1):145-166.

[15]Gilbert P, Chun B G, Cox L P, et al. Vision: automated security validation of mobile apps at app markets[A]. The second international Workshop on Mobile Cloud Computing and Services[C]. ACM, 2011.

[16]闫莉,石润华,仲红,等. 移动云计算环境中基于身份代理签名的完整性检测协议[J]. 通信学报,2015(10):278-286.

[17]Oberheide J, Veeraraghavan K, Cooke E, et al. Virtualized in-cloud security services for mobiledevices[C]. New York, USA: ACM, 2008.

[18]张伟,王汝传,李鹏. 基于云安全环境的蠕虫传播模型[J]. 通信学报,2012(4):17-24.

[19]Chow R, Jakobsson M, Masuoka R, et al. Authentication in the clouds: a framework and its application to mobile users[C]. New York,

USA:ACM,2010.
[20]王中华,韩臻,刘吉强,等. 云环境下基于 PTPM 和无证书公钥的身份认证方案[J]. 软件学报,2016(6):1523-1537.
[21]姜茸,张秋瑾,李彤,等. 电子政务云安全风险分析[J]. 现代情报,2014(12):12-16.
[22]程桂枝,于秀娟. 新技术环境下政务系统应用安全研究[J]. 科技管理研究,2014(12):165-169.
[23]章谦骅,章坚武. 基于云安全技术的智慧政务云解决方案[J]. 电信科学,2017(3):107-111.
[24]胡俊,张熠,黄传河. 基于云平台的政务信息系统的访问控制设计[J]. 华中科技大学学报:自然科学版,2013(12):147-151.
[25]李卫东,徐晓林. 云政务信息资源共享的国家安全隐患及安全保障机制研究[J]. 华中科技大学学报:社会科学版,2017(6):90-97.
[26]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(2):112-116.
[27]丁楠. 基于机器学习的大学生自杀风险预测与分析[J]. 现代电子技术,2017(21):91-97.
[28]林云威,陆冬青,彭勇. 基于 D-S 证据理论的电厂工业控制系统信息安全风险评估[J]. 华东理工大学学报:自然科学版,2014(8):500-505.
[29]薛晔,蔺琦珠,任耀. 我国通货膨胀风险的预测模型——基于决策树与 BP 神经网络[J]. 经济问题,2016(1):82-89.
[30]肖奎喜,王满四,倪海鹏. 供应链模式下的应收账款风险研究——基于贝叶斯网络模型的分析[J]. 会计研究,2011(11):65-71.
[31]Shannon C E. A Mathematical theory of communication[J]. The Bell System Technical Journal,1948,27(3):378-656.
[32]刘国城,王会金. 基于 AHP 和熵权的信息系统审计风险评估研究与实证分析[J]. 审计研究,2016(1):53-59.
[33]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.
[34]刘国城. 基于大数据过程挖掘的互联网安全审计过程建模研究[J]. 兰州学刊,2018(3):95-106.
[35]王志英,葛世伦,苏翔. 云用户数据安全风险感知乐观偏差及其影响实证[J]. 管理评论,2016(9):121-133.
[36]王会金. 政府审计协同治理的研究态势、理论基础与模式构建[J]. 审计与经济研究,2016(6):3-11.
[37]丁滟,王怀民,史佩昌,等. 可信云服务[J]. 计算机学报,2015(1):133-149.

[责任编辑:刘　茜]

Risk Assessment and Audit Run of E-Government Cloud Security in Big Data Age

WANG Huijin, LIU Guocheng
(Nanjing Audit University, Nanjing 211815, China)

Abstract: The cloud computing practice has promoted the construction of government cloud with the government's cloud technology as the support and integration with multi-sources big data. However, the government cloud is faced with some serious security issues. Many risk factors such as big data leakage, internal abuse, external invasion, and technological loopholes, restrict the effective operation of the government cloud. It is imperative to carry out government cloud security audit based on the risk-oriented model. Through the monitoring of threat behavior and mining security incidents for audit forensics, the cloud model is widely used in the field of e-government. Based on the theoretical review, this paper analyzes the cloud security risk assessment methods under big data and exemplifies the validity of them. It establishes a government cloud security audit framework through the division of responsibilities between cloud providers and cloud tenants, and uses the three dimensions of management, technology, and standards to provide the operational protection of the government's cloud security audit with an aim to find constructive ideas for government cloud security management practices in the era of big data.

Key Words: big data; cloud computing; e-government; government cloud audit; security audit; cloud risk; entropy estimate