Advances in Social Sciences 社会科学前沿, 2017, 6(12), 1584-1590
Published Online December 2017 in Hans. http://www.hanspub.org/journal/ass
https://doi.org/10.12677/ass.2017.612224

Hans汉斯

Internal Control Audit of Government Information Security

—The Perspective of Human Behavior

Siyi Liu, Zhanbei Ye

Nanjing Audit University, Nanjing Jiangsu
Email: 455632603@qq.com, yezhanbei@163.com

Received: Dec. 1st, 2017; accepted: Dec. 14th, 2017; published: Dec. 21st, 2017

Abstract

At present, information security audit mostly focuses on information system, but auditing is often lagging behind. Therefore, internal control audit as a preventive mechanism to maintain information security is obviously necessary. To the internal control audit of government information security, we discuss the necessity and feasibility of the internal control audit of government information security from the perspective of human behavior. On this basis, we believe that the implementation of the focal point in the separation of incompatible duties through system, internal supervision, human resources and leadership behavior. To this end, we need to learn from the chief information security executive system to constantly improve the internal control audit of the government's information security in our country.

Keywords

Behavior Oriented, Government Information Security, Internal Control Audit

政府信息安全的内部控制审计

—人的行为的视角

刘思贻，叶战备

南京审计大学，江苏 南京
Email: 455632603@qq.com, yezhanbei@163.com

收稿日期：2017年12月1日；录用日期：2017年12月14日；发布日期：2017年12月21日

摘 要

目前针对信息安全的审计研究多着力于信息系统方面，且审计往往是滞后的，由此把内部控制审计作为

文章引用: 刘思贻, 叶战备. 政府信息安全的内部控制审计[J]. 社会科学前沿, 2017, 6(12): 1584-1590.
DOI: 10.12677/ass.2017.612224

预防机制来维护信息安全显然是必要的。具体到政府信息安全的内部控制审计，我们从人的行为的视角探讨了政府信息安全内部控制审计的必要性和可行性，在此基础上，我们认为实施的着力点在不相容职务的分离、轮岗制度、内部监督、人力资源以及领导人行为等方面。为此，我们需要借鉴首席信息安全执行官制度方面不断完善我国政府信息安全的内部控制审计。

关键词

行为导向，政府信息安全，内部控制审计

1. 引言

不同的信息具有不同的价值，且这些信息传播的空间及使用的渠道是有限制的，因为有些信息一旦被泄露或丢失，它的价值可能就会被扭曲，甚至给国家、社会和个人带来无法挽回的相关损失。特别是在网络空间，信息流在给我们带来各方面便利的同时，其自身的安全也常常面临严重的威胁。这充分说明信息安全问题已经上升到国家战略的高度。具体到政府信息，如果没有适当和严格的安全防范措施的保障，有价值信息的机密性、完整性和可用性都可能会受到影响。考虑到人是任何组织的中心，也是对组织最严重的威胁，而传统的审计方法本质上是技术性的、检查业务的物理、技术和操作程序，却常常忽略人为因素这一信息安全最重要的环节，我们立足于内部控制审计的理论基础，从人的行为的视角来探讨政府信息安全的保障将具有开拓性的价值。

2. 政府信息安全的内涵及其内部控制审计的必要性

2.1. 政府信息安全的内涵

所谓信息安全，指保障国家、机构、个人的信息空间、信息载体和信息资源不受来自内外各种形式的危险、威胁、侵害和误导的外在状态和方式，以及内在主体感受[1]。

信息安全可以分为狭义安全与广义安全两个层次，狭义的安全是建立在以密码论为基础的计算机安全领域，早期中国信息安全专业通常以此为基准，辅以计算机技术、通信网络技术和编程等方面内容；广义的信息安全是一门综合性学科，从传统的计算机安全到信息安全，不但是名义的变更也是对安全发展的延伸，安全不再是单纯的技术问题，而是将管理、技术、法律等问题相结合的产物[2]。

政府部门在考虑信息安全问题时，不能只把信息当作一份文件或数据，而是要当作一份有价值的资产。尽管信息的价值难以评估，也无法表示在财务报表上，但是这并不代表它不具有价值。不同的信息具有不同的价值，保密性不同信息的价值也不尽相同，一旦这些信息泄露或丢失，它的价值就会发生变化，会给国家、社会和人民带来不可挽回的财产损失。因此，信息安全问题应该受到重视，对信息安全的防护也应该提上日程。

2.2. 内部控制审计的必要性

美国审计总署 1999 年的《联邦政府内部控制准则》对内部控制作出定义：“内部控制是管理一个组织的主要成分，包括了用以实现使命和目标的计划、方法和程序，并为管理提供支持[3]。”

内部控制审计是以内部控制制度为前提而建立起的审计模式，但在国内外学术界尚未形成统一定论。美国上市公司会计监管委员会发布的《PCAOB 审计准则第 2 号——内部控制审计原则》(2004 年)、中国注册会计师协会发布的《独立审计具体准则第 9 号——内部控制与审计风险》(1997 年)和中国内部审计协会发布的《内部审计具体准则第 5 号——内部控制审计》(2003 年)中均没有明确对内部控制审计予以定义[4]。

从广义上讲，对内部控制进行审计的作用有二。一方面可以作为一项发现内部控制缺陷的独立审计项目，以促进被审计对象内部控制的不断完善，对问题防患于未然。另一方面也可以作为整体审计程序的一个环节，对被审计单位内部控制的可依赖程度进行评价，以确定是否可以利用被审计单位的内部信息，以提高审计人员的工作效率和质量，确定审计的范围、重点和方法。本文主要从第一个方面阐述了对内部控制进行审计，在防止政府信息泄露方面的作用。

目前，我国对于维护信息安全的审计研究多集中在狭义的信息安全方面，而对于管理方面，防止内部的人为信息泄露的内部控制少有涉及。但是审计往往具有滞后性，即使采用跟踪审计的方法，审计时点也是在既成的事实之后。相对于财务资金而言，信息资产具有可复制性，一旦泄露将不可挽回，如果被审计部门发生人为的重要信息泄露，即使在事后审计中发现问题，也只能对发生的问题进行纠错，产生的损失已经沉没，将造成无法挽回的损失，政府审计的有效性也会大打折扣。内部控制就相当于政府部门的防御系统，弥补了审计监督滞后性的缺陷。内部控制将监督嵌入到行政事业单位的组织构架中，强调了风险预警与即时干预，通过管控措施对风险进行防范和降低，使得监督关口被前置，弥补了政府审计监督的滞后性[4]。

3. 对威胁政府信息安全的人的行为进行内部控制审计的依据

政府每个部门和人员在遵守国家法律法规的同时，还应根据本部门的自身情况，制定适合本部门的防止信息泄露的内部控制制度。然而，由于各地威胁信息安全的问题不同，制定内部控制制度的人的能力和素养也参差不齐，所以虽然具备相应的法律制约和处罚条例，但是由于缺乏必要的预防和监督机制，我国政府工作人员泄露国家机密的事件却屡见不鲜。党的第十九次全国人民代表大会将审计监督作为党和国家监督体系的一部分，为维护国家信息安全，对政府工作人员的行为进行监督和评价是审计的责任和义务。

3.1. 对人的行为进行内部控制的依据

信息安全专家 William Marlik 在其一次来京的访谈中谈到：“任何信息安全都是不完美的，而更重要的是不完美的人使用这些不完美的产品。”员工的行为及其在特殊情况下的反应对部门的信息安全至关重要。为了规范人的行为使其符合组织的目标，保护部门信息的完整性和保密性，组织内部制定了严格和适当的指导方针，详细的说明了员工需要遵守的程序、规则和规章。但是人的行为往往具有主观性，不是按照一套既定的规则来执行的，而是根据个人的个性来进行的。有审计结果表明，尽管经过审核的政策和程序是有效的，但是因为政策没有得到遵守，信息仍然会泄露，这就是人为因素造成的。比如员工离开工作岗位而没有将房间上锁，这时制度对员工的管控失效。密码系统等技术控制也是同样的道理。因此，为了解决这个问题，必须对员工的行为施加内部控制。内部控制的运行控制是关注有关信息安全的员工的行为和行动，以确保员工以及他们的行为在信息安全的产业链中不是薄弱环节。

3.2. 对人的行为进行审计的依据

社会的发展对审计也提出了新的要求。唐大鹏等认为，政府审计关注的内容也不再不仅仅局限于资金管理使用与资产经营，而是涵盖了经济社会的健康运行和发展，以及国家及政权安全等广泛的范围。

政府审计的监督范围已经从财务审计扩大到更广更深的经济业务，甚至未来将把非经济业务纳入审计范围[5]。胡春辉认为，人本审计是与物本审计相对应的一个概念，是指以人及人的行为为中心、为根据的审计，这种意义的审计，重视对人及人行为的审查[6]。房巧玲认为，行为导向审计模式，是将审计活动立足于被审计单位各级受托责任主体的行为动机、行为过程及其后果的审查。对政府信息安全中人的行为进行审计不仅拓宽了审计业务范围，也适应了审计转型的需要[7]。

4. 政府信息安全内部控制审计的着力点

因为政府内部控制与企业内部控制存在很多不同，如控制目标不同、责任机制不同等，所以对政府信息安全内部控制的审计也与传统审计存在差异。但是由于政府内部控制与企业内部控制二者在实质上大体相同，而审计也都是对其设计和运行有效性的评估，所以在构建政府内部控制体系时在许多方面可以合理地借鉴企业内部控制成功的经验。我国政府内部控制研究还未成熟，在信息安全方面尤甚，而企业内部控制已经具备完备的体系，可以为政府内部控制提供理论与方法，但应注意的是，对政府信息安全进行审计时，重要性水平应该更高。

4.1. 不相容职务的分离

一份信息在政府内部或外部流通，需要经过授权审批、信息保管、流通记录和审核监督等环节，为避免职务上的交叉和重叠，应将授权审批与信息保管职务相分离，信息保管与流通记录职务相分离，信息保管与审核监督职务相分离，流通记录与审核监督职务相分离。政府的内部控制制度应该明确不同岗位的职责权限，不相容职务的分离的核心是内部牵制，关键在于执行。审计人员在确定被审计单位是否发布文件制定制度来确定不相容职务以外，还需要注意其是否采取一系列实际措施使制度落地，如对一份信息文件设置多份密钥，不同的密钥由不同的人员控制，形成相互制衡的体系；联机时，要加强员工获取信息的相互依赖性；加强监督检查、实行问责制度等。当然，不相容职务的分离避免信息泄露的效用建立在没有合谋串通的基础之上，当拥有两种或两种以上权力的人相互串通时，不相容职务分离的作用将会失效。

4.2. 轮岗制度

一位员工在一个业务部门工作多年，在积累了经验，对业务得心应手的同时，也最有机会突破信息安全的保护层而导致重要信息的泄露。为提高政府工作人员的素养，防止舞弊和信息泄露等事件的发生，人事部于 1996 年根据《国家公务员暂行条例》制定了《国家公务员职位轮岗暂行办法》。地方政府应根据实际情况，建立轮岗的长效机制，单位内的关键岗位遵循内部性、平级性和有序性的原则，定期进行轮换。审计人员应从是否认真选择轮岗对象，是否做好岗位培训工作等方面，对轮岗的范围、周期和方式进行审查，注意是否有在不相容职务之间进行轮岗。若单位内部设置了专门的轮岗评估机构，审计人员也可以利用其评估考核结果，判断轮岗制度在政府工作人员专业胜任能力等方面是否完善。

4.3. 内部监督

缺乏监督容易导致内部控制形同虚设。良好的内部控制并不是一蹴而就的，而是要在运行过程中针对控制缺陷不断改进，这时内部监督的作用就显现出来了。内部监督可以在日常活动中获得内部控制是否有效执行的证据，并及时报告内部控制存在的缺陷，作为业务执行体系外部的监督，有效的规范了政府工作人员的行为。政府部门的内部监督应该将日常监督与专项监督结合起来，在关注日常业务的同时抓重点，然后根据监督情况自我评价，并根据评价情况出具内部控制自我评价报告。为评价内部监督的

有效性，审计人员需对被审计单位内部监督的监督检查方法进行审查，了解与被审计单位监督活动相关的信息来源是否可靠，以及内部审计的设置和工作情况。内部审计作为内部监督体系的一部分，应具备具有专业胜任能力的执业人员，并定期对其进行适当的培训。审计人员还应对内部审计的独立性进行审查，即是否直接向最高级管理层直接汇报。

4.4. 人力资源

如果一个员工发现了信息泄露行为，那么他应该知道向主管部门汇报且知道向谁汇报。如果他没有这么做，那么部门的安全机制就存在漏洞，这时即使有再功能强大的信息技术系统也无济于事。如果没有对人的行为进行内部控制，任何技术都不能保证信息资源不被泄漏，万无一失。

单位的内部控制归根结底是由人在执行的，所以对人的选拔应该格外的重视，保证政府工作人员的职业道德修养、专业胜任能力和严谨的工作态度是至关重要的。首先，审计人员应重视员工的招聘程序是否规范，以及需求计划是否合理，尤其是关键控制点岗位的人员选拔，审查招聘过程中的审核记录和档案资料，以确定工作人员的身份是否适合担任相应职务。其次，定期的职工培训和继续教育也会增强政府工作人员保护信息安全的意识、问题意识和信息敏感性。尤其对于新招聘的员工，由于责任意识还不是很强，信息泄露的风险也就更大。因此审计人员要评价被审计单位的培训制度是否科学合理，是否根据不同的岗位需要制定不同的培训制度，以引导和规范政府工作人员的行为。最后，对于掌握国家重要机密的重要岗位离任应进行重点审计，确认保密协议的签署并确保其离任限制机制有效，确保其以前接触国家机密的条件已经更换，如密令、钥匙等，以防止其继续接触重要信息，导致信息的泄露。

4.5. 领导人行为

根据行为科学的领导行为论，组织的成败与领导者的行为、素质等密不可分[8]。在政府部门中，党政领导干部在单位内部制度的制定过程中通常起着关键作用，一般来说，“一把手”在决策中能起到决定性作用。因此，对领导者的知识水平、决策能力进行审查是必要的。领导行为理论要求审计人员审查和评价领导者领导方式的可行性，审查和评价权责分层、法律规章制度是否有利于发挥领导者的作用，审查和评价领导者经验、能力、需要、动机、上进心等特征。在电子政务普及的情况下，领导人首先必须了解信息安全的关键控制点，然后才能对整体的内部控制作出决策。但是由于人的能力是有限的，不能完全避免决策错误，所以对于重要信息要避免“一言堂”、“一支笔”，必要时实行联签制。

审计人员获取的单位内部控制信息也大多来自领导者，但是在获取的信息中，单位的外部信息是领导者无法控制的，所以有着比内部信息更强的说服力。在审计过程中，可以开放热线电话，接受群众来信，获得外部群众对政府工作人员服务能力的评价，同时，将内外部信息进行比较能促使二者相互印证，帮助审计人员寻找出价值更高的线索，对领导者的能力和客观性作出更准确的评价。

5. 不断完善我国政府信息安全内部控制审计的建议

在美国的一些大型企业中，为了维护信息的安全，首席信息安全执行官(CISO)应运而生。他的主要通过制定安全策略、评估潜在风险，来防止企业信息受到来自内外部的侵袭。同时也可以监管日常事务，发现安全机制在运行过程中的漏洞，进行及时的修正。在我国政府机关中，尚未建立首席信息安全执行官制度，但是内部控制作为保护政府信息安全的预防机制，应该适应时代发展的要求，做到与时俱进。

5.1. 首席安全执行官应具备的素养

首席安全执行官的工作是监督和提供修正方向，而非决策[9]。所以，首先他应该具有丰富的经验和技能，掌握与业务运营相关的技术，了解部门信息风险的关键控制点，这样才能对政府信息安全施加影

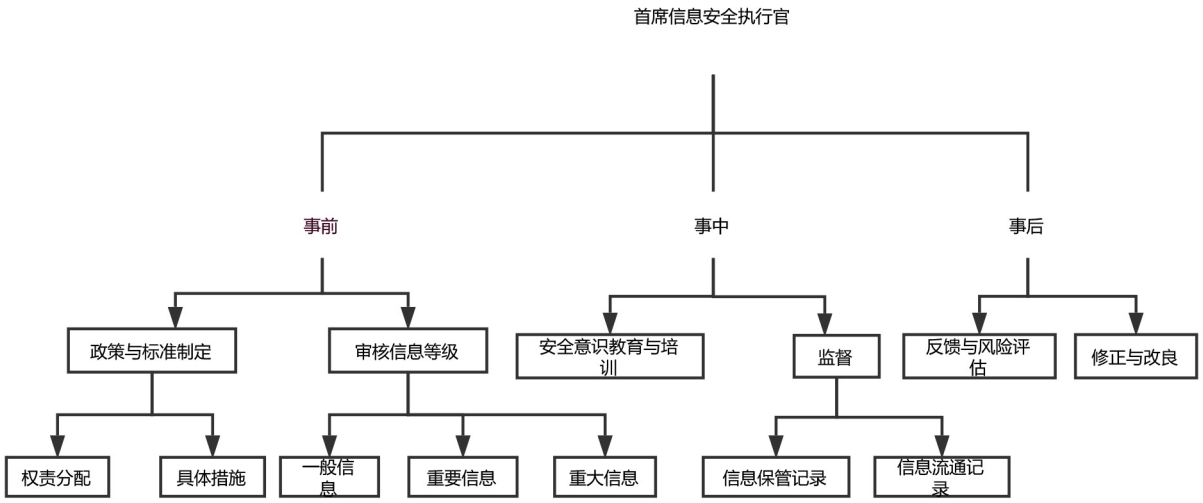

Figure 1. Chief information security executive system
图 1. 首席信息安全执行官制度体系

响。其次必须紧随时代的发展，拥有全新水平的业务才干。首席信息安全执行官可以是注册信息系统安全师出身，也可以是以前从事管理方面的有经验的人员，但是无论如何，面对日益增加的信息安全威胁，都需要不断学习新的技能，各方面武装自己，发展成为多方面的人才，以适应新时期对首席信息安全执行官的需要。再次，良好的沟通能力在团队协作中是必不可少的。沟通能力可以分为表达和倾听两个层次，通过表达，首席信息安全执行官必须让大家都了解控制信息安全的机制，而为了获取这个机制有效性的反馈，执行官还必须学会倾听来自各方的意见，从而做出决断以对控制机制进行修正。最后，作为首席信息安全执行官，领导能力必不可少。首席信息安全执行官脱离首席安全执行官(CSO)独立存在，必须具有领导一个部门的能力。否则不仅对下没有统御能力，更重要的是使整个信息安全部门在政府机构中没有威信力，导致形同虚设。

5.2. 在政府中构建首席信息安全执行官机制的设想

首席信息安全执行官独立在政府部门政务系统之外，但需要参与在信息流通的整个过程中。本文将信息流通过程分为事前、事中和事后三个部分，建立了首席信息安全执行官制度体系(见图 1)，分别对首席信息安全执行官的职责进行了规划和说明。由于政府部门的党政领导人员在当选时多注重行政能力和领导能力，在专业能力方面或多或少都有缺陷。所以在制定内部控制制度时，需要首席信息安全执行官对政策和标准的制定提供意见和建议。并且要对信息进行等级划分，从而确定信息的流通范围和保密程度。在信息流通过程中，要加强对员工信息安全知识的教育与培训，并对信息的保管与流通进行监督，定期和不定期的对信息流通记录和保管记录进行检查。事后，根据了解的情况和发现的问题，对内部控制进行风险评估，并根据控制体系存在的问题进行修正。

致　谢

在论文完成之际，我要特别感谢我的指导老师——叶战备老师的热情关怀和悉心指导。在我撰写论文的过程中，无论是在论文的选题、构思和资料的收集方面，还是在论文的研究方法以及成文定稿方面，我都得到了叶老师悉心细致的教诲和无私的帮助，特别是他广博的学识、深厚的学术素养、严谨的治学精神和一丝不苟的工作作风使我终生受益，在此表示真诚地感谢和深深的谢意。

同时，我也要感谢本论文所引用的各位学者的专著，如果没有这些学者的研究成果的启发和帮助，

我将无法完成本篇论文的最终写作。至此，我也要感谢我的朋友和同学，他们在我写论文的过程中给予我了很多有用的素材，也在论文的排版和撰写过程中提供热情的帮助！

最后，向在百忙中抽出时间对本文进行评审并提出宝贵意见的各位专家表示衷心地感谢！

基金项目

江苏高校优势学科建设工程资助项目现代审计科学江苏高校优势学科建设工程资助项目现代审计科学。

参考文献 (References)

[1] 上海社会科学院信息研究所. 信息安全辞典[M]. 上海: 上海辞书出版社, 2013.

[2] 刘秋明. 基于公共受托责任理论的政府绩效审计研究[D]: [博士学位论文]. 厦门: 厦门大学, 2006.

[3] 钱纪初. 浅论网络信息安全的重要性[J]. 今日湖北(中旬刊), 2015(10): 143-144.

[4] 刘永泽, 况玉书. 我国政府内部控制: 经验借鉴与体系构建[J]. 南京审计学院学报, 2014(4): 3-11.

[5] 唐大鹏, 李怡, 周智朗, 等. 政府审计与行政事业单位内部控制共建国家治理体系[J]. 管理理论, 2015(3): 123-126.

[6] 胡春晖, 王东娣. 人本审计的几个基础问题的探讨[J]. 天津商业大学学报, 2010(5): 49-52.

[7] 房巧玲, 刘长翠, 肖振东. 行为导向审计模式研究_基于国家审计的视角[J]. 当代财经, 2013(4): 119-128.

[8] 王光远. 制度基础审计学[M]. 武汉: 湖北科学技术出版社, 1992: 36-37.

[9] 尹小山. CISO, 何许人也? [J]. IT 经理世界, 1999(9): 46-47.