浅谈信息安全对审计工作的影响

柳州市城中区审计局　雷薇

【摘要】信息安全已经成为国家战略的重要组成部分，我们国家对于信息安全的重视程度可想而知。因此，审计工作也需要与时俱进，将信息安全作为审计的重要环节来抓。目前，审计机关也在积极落实“金审三期”及信息化建设相关要求，着力提升审计信息化建设和应用水平。但在建设的过程中也发现部分审计机关存在“重建设、轻安全”[1]的现象，给以后的审计过程中信息安全，带来极大的风险和隐患。随着信息技术的迅猛发展，黑客攻击、数据泄露、恶意软件等安全事件频繁发生，在这个背景下，审计机关作为国家经济监督的重要部门，如何加强对数据安全的监管，筑牢国家信息安全屏障，成为了一个亟待解决的问题。

【关键词】信息安全；审计；数据

一、引言

随着互联网、物联网、大数据等技术的不断发展和普及，信息安全问题已经成为了一个日益突出的问题，审计工作面临着越来越复杂的挑战，而审计人员在日常开展审计工作中，应该时刻常鸣“警醒”之声，保护信息安全。本文主要从信息安全的定义及其重要性，以及随之带来的信息安全风险对审计工作带来的影响以及挑战。最后，针对数字化时代的信息安全挑战，提出了相应的解决措施，确保审计工作的有效性和可信度，为推进网络强国建设提供审计支撑。

二、信息安全的定义和重要性

（一）信息安全的定义

信息安全是一个涵盖了多个层面的复杂概念，它主要指的是对信息系统采取的一系列技术和管理措施，以确保这些系统的安全和保护，即包含了物理层面，如计算机硬件、移动存储设备等，也包括了运行层面，如信息数据、数据库等[2]。信息安全包含了可用性、保密性、完整性和不可否认性等[3]，对审计工作的独立、公正开展具有着重要的意义。

（二）信息安全的重要性

数字化时代的信息安全对审计工作具有重要影响，随着网络规模的扩大，不仅产出了海量的数据，而且各种服务器、主机、数据库和信息系统也原来越多[4]，信息系统也愈加复杂这对审计人员的相关的技术知识和技能水平提出来更高的要求。所以，信息安全成为审计工作中不可忽视的重要问题。此外，现如今网络攻击和数据泄露事件频繁发生，要化解各种黑客攻击、网络病毒等网络攻击，给审计工作带

提出了新要求。

三、信息安全风险的来源和分类

信息安全风险管理是一个连续的、动态的过程，它贯穿于整个信息系统的生命的始末。审计是信息安全风险管理的重要组成部分，通过对信息系统的各种风险进行识别、评估、控制和监控，为信息安全风险管理提供支持。

（一）内部风险

信息安全的内部风险，在审计工作中是一个不容忽视的问题。一方面可能存在被审计单位人员、审计人员故意破坏信息系统，窃取敏感信息，或者进行其他形式的非法活动；另一方面可能因为疏忽大意，没有按照规定的操作流程进行操作，从而导致信息泄露或系统故障。例如，可能会忘记关闭电脑，导致敏感信息被他人看到；或者误删除重要的数据，导致系统无法正常运行；系统登录密码采用默认密码、密码口令过于简单等，都会加大被破解的可能性[5]。再者，目前部分审计机关及工作人员对于保密观念的理解和应用仍显落后，没有把信息安全与保密工作放到重要的位置，尤其对新技术条件下的保密工作所面临的严峻形势缺乏足够的重视，导致保密人员不专业、设备不齐全、制度不健全、管理不严格等。

（二）外部风险

信息安全的外部风险，是审计项目控制的重要环节。一般来说，信息安全的外部风险，包括了黑客、病毒、恶意软件等，感染的途径有网页弹窗、电子邮件等方式入侵信息系统，然后对信息系统进行恶意的代码植入，导致相关的信息数据被窃取或者篡改，严重的话还会

导致整个信息系统直接崩坏，相关数据库直接丢失。

（三）物理安全风险

在信息安全领域中，物理安全主要涉及的是计算机设备、网络设施和环境等，它是整个网络信息系统安全的前提。一是存储环境存在安全隐患。数据的分析处理、存放保管等等，都需要相关的物理设备，若是遭受到地震、水灾、火灾等环境事故，则会影响信息数据安全。二是人为因素的隐患威胁。包括外部人员的盗取、损坏、篡改情况以及内部人员的丢失、欺诈等行为，都会影响到审计工作的正常进行。三是其他因素。包括未设置有效的安全措施，相关信息设备及时的维护和更新等。

四、现代审计面临的信息安全挑战

（一）对数据安全提出了挑战

在信息技术日新月异的发展趋势下，数据安全问题已经成为了数字经济发展中亟需关注的重要问题[6]。在审计过程中，在科技强审和信息安全的两个统一结合中，审计人员需要对海量的结构化和非结构化数据进行分析和判断，数据安全风险与日俱增，数据若是被泄露或者篡改、丢失等，则会导致数据分析结果存在偏差，加大审计风险。

（二）对专业技术能力提出了挑战

在数据爆炸的时代，信息安全面临着极大的挑战。审计人员的专业技术能力并不能够仅仅满足于此前传统的审计方法和程序，为了适应大数据、云计算等技术的发展，还需要掌握现代信息技术和信息安全技术。

（三）对法律法规制定、监管提出了挑战

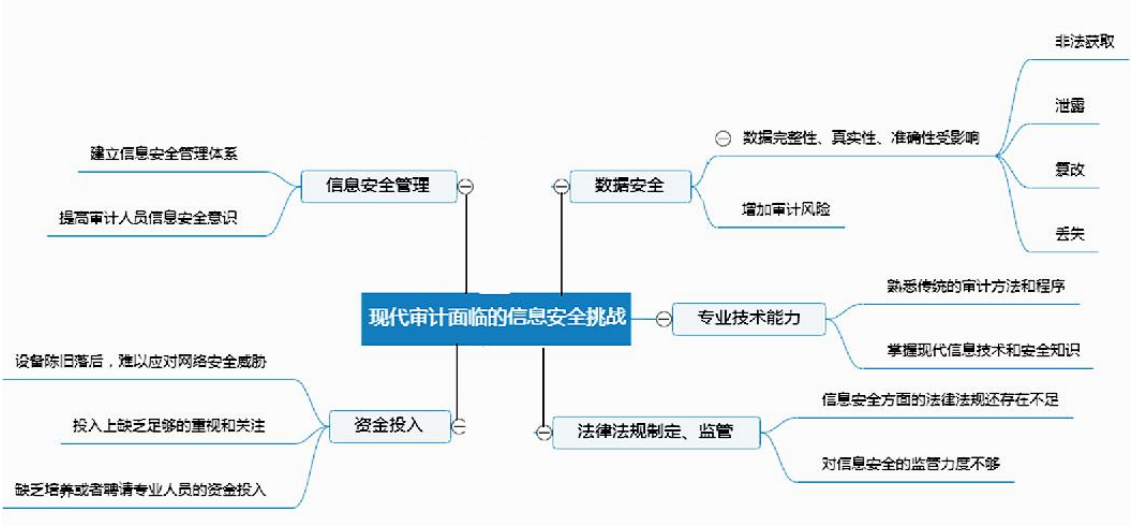
随着信息技术的不断进步和创新，对信息安全治理能力也提出了更高的要求。一方面，我国目前对新形势下的审计工作中的信息安全方面的法律法规还存在不足，对信息安全的基本原则、责任主体和监管要求还未明确到位，在很多信息化管理领域还存在无法可依，或者一些规章制度过于笼统，指导性不强；另一方面，审计机关对信息安全的监管力度不够，尚未形成对重要行业和关键领域的数据安全进行定期检查和评估。

（四）对信息安全管理提出了挑战

信息安全不仅仅是技术问题，更是一个管理问题，信息安全管理贯穿于整个信息传递、存储等方面，是抵御信息安全风险的生命线[7]。在这个信息爆炸的时代，大量的信息被生成、存储和传输，而这些信息往往涉及单位机密、国家安全等多个方面。因此，审计机关在维护国家利益和社会公共利益的过程中，需要建立行之有效的管理模式。

（五）对信息安全资金投入提出了挑战

为了建立信息安全体系，少不了技术设备以及资金的投入。然而，我们也发现目前审计机关对这一方面的投入还是不足。主要表现在：一是资金匮乏，技术设备陈旧落后。由于审计机关受到资金限制，无法更替最新的安全技术和设备，所用设备陈旧落后，运行速度缓慢，根本无法应对日益复杂的网络安全威胁。二是信息安全意识观念不足。部分审计机关对信息安全的重要性认识不足，对安全技术和设备的投入上缺乏足够的重视和关注，即便单位有经费，也会优先用于其他地方。



图一：审计面临的挑战思维导图

五、信息安全风险对审计工作的机遇

信息安全风险对审计工作的影响是复杂而深远的。在当今数字化时代，信息安全问题日益突出，带来巨大挑战的同时，但为审计工作带来了机遇。

（一）提高审计工作效率

信息安全风险的存在可以促使审计人员更加关注被审单位的信息安全状况，能够在信息系统以及管理过程中找到相关的漏洞与风险，从而提高审计的效率。例如，如果审计人员发现被审单位存在严重的信息安全风险，可能会加快审计进度，以便提出更具针对性的审计建议。

（二）提升审计工作质量

随着信息安全意识的提高，被审单位也会越来越重视信息安全管理，并投入大量资源来加强安全防护，这为审计人员提供了更多的数

据和信息，通过对大量数据的分析研判，能够更全面地了解被审单位的风险管理和控制措施，为审计工作提供了更多的可能性。例如，审计人员可以利用数据分析工具来发现异常业务活动和潜在的安全漏洞，从而提升审计质量。

（三）提升审计人员专业能力和知识水平

“互联网+”的背景下，为了应对不断变化的信息安全威胁，审计人员需要不断学习和掌握最新的安全技术和方法，提高安全防护能力。通过持续的学习和培训，了解各种安全漏洞和攻击手段，以及相应的防护措施，提高自身的专业素养。

（四）推动审计方法和技术的创新和发展

信息技术的高速更迭发展，如 5G、云计算、区块链、元宇宙等这些技术，都促进了审计方法和技术的创新与应用，为审计思路提供了更加广阔的遐想空间。自动化、人工智能等技术手段在审计工作上的合力利用，将会给审计成果插上飞翔的“翅膀”，通过不断优化和完善相关审计方法与技术手段，更好的应对在工作过程中可能发生的各种复杂的网络威胁。

表一：信息安全风险对审计工作的机遇表格

机遇	**具体表现**
提高审计工作效率	找到被审单位的信息安全漏洞
提升审计工作质量	被审单位产生了更多的数据和信息，为审计工作提供了更多的可能性。
提升审计人员专业能力和知识水平	促使审计人员不断学习和掌握最新的安全技术和方法
推动审计方法和技术的创新和发展	不断优化和完善，向更高效、更智能的方向发展

六、主要措施

新时代背景下，日益严峻的信息安全问题，给网络安全防护工作带来更多挑战。审计机关要充分发挥自身职能作用，发挥信息化驱动引领作用，保成数据安全和信息安全，为维护国家和社会的信息安全作出贡献。

（一）建立健全法律法规体系，强化信息安全宣传教育

在信息技术不断进步的同时，也不能忽略掉法律法规的建设。审计机关应当及时建立健全的信息安全法律法规体系，这是十分重要和紧迫的[8]。法律法规制定完善后，也需要将其广而告之。就审计机关而言，可以通过开展形式多样的宣传、培训和警示活动，加强审计人员对信息安全法律法规的重视程度，了解并掌握信息安全的基本要求以及信息安全应对监管措施。

（二）加强信息安全审计监督，构建信息安全屏障

审计机关应当加强对信息安全检查，涉及到的机关、个人等需依法接受监督。一是进行定期或不定期的信息安全检查，重点关注在数据处理、存储和传输过程以及检查设备、设施和环境的安全。同时，加强对工作环境的安全管理检查，如安装火灾报警系统、备份电源等。二是对检查过程中发现的数据安全事件进行及时调查和处理，按照“统一领导，逐极负责”的原则，追究相关责任人的责任。四是加强对数据处理和存储的监督管理，加强网络安全防护措施，如使用防火墙、入侵检测系统等；定期更新和升级系统和应用程序，以修复已知的安全漏洞，确保其具备必要的技术和管理能力，能够有效保护信息安全。

（三）强化沟通协作配合，共同维护信息安全

因数据传播途径具有多样性，以此带来的信息安全问题涉及多个领域，若仅仅依靠审计机关的力量便显得有些力不从心。所以为了实现信息安全的有效全面的监管，审计机关应该积极联合相关部门单位，建立协调统一的监管的协作机制，加强统筹协调，形成监管合力，共同为健康有序的数字经济尽一份力。

（四）加强人才培养力度，提升信息安全保护能力

为了应对复杂的信息安全环境，审计人员不仅要具备扎实的专业知识，还要具备一定的信息技术能力。一是审计机关应当定期组织培训，注重现代信息技术手段的培训，以专业信息化技术为根基，信息安全专业知识为主干，提高审计人员的综合素质，进一步加强信息安全专业人才队伍建设，培养一支既懂审计业务，又懂信息安全技术的专业队伍。二是建立健全考核机制，对审计人员的工作进行定期评价，激励他们不断提高业务水平。三是培养审计人员沟通协调能力，能够与各方进行有效沟通，推动数据安全监管工作的落实。

（五）提高技术和资金支持，丰富审计信息安全措施

信息安全技术的提高，除了需要大力发展相关的技术应用，发挥信息化驱动引领作用，如：加大防火墙的建设、入侵检测系统的建立、信息数据的加密等，而且可以依托于“金审三期”的建设，加大审计对网络安全的资金投入，可以采购购买和维护信息安全技术产品的费用，如防火墙、入侵防御系统等[9]，提高防御信息安全的能力。同时，审计机关可以与信息安全领域的专业公司或研究机构合作，分享最新的技术研究成果和经验，提高审计机关的信息安全保护能力。

参考文献：

[1] 马英彬 审计信息安全保密工作不容忽视[J] 中国审计，2010（5）:66-67

[2] 信息安全(Information Security) https://wiki.mbalib.com/wiki/%E4%BF%A1%E6%81%AF%E5%AE%89%E5%85%A8

[3] 中华人民共和国国家质量监督检测检验检疫总局,中国国家标准化管理委员会 信息安全技术信息安全风险管理指南[Z],GB/Z 24364-2009

[4] 刘海蜀 信息安全审计实战[J] Windows IT Pro Magazine 国际中文版，2007（9）:49-51

[5] 刘卫刚 李勇 信息安全管理工作重要性认识初探[Z] 中国管理信息化，（2014）06-0089-02

[6] 东湖大数据 聚焦我国数据安全面临的七大挑战与治理建议[Z]

[7] 康巨瀛 田园 信息安全管理的重要性[Z]，（2006）01-0003-01

[8] 黄春兰 建立健全信息技术的信息安全法律法规[Z]，(2014) 15-0200-01

[9] 周梁 采取四项措施强化审计信息保密工作[J] 审计与理财，2013（9）:42