 DOI: https://doi.org/10.12345/cjygl.v9i3.24915

Information security management strategy in enterprise internal control management

Hai Yan

Guilin Tebang New Materials Co., Ltd., Guilin, Guangxi, 541004, China

Abstract

With the acceleration of economic integration and informatization, there are more and more opportunities and challenges for enterprise development. The wide application of information technology has accelerated the process of enterprise informatization, and information flow has gradually become the "blood" of enterprise operation. However, the continuous changes in the network environment, data leakage, network attacks, internal fraud and other problems are becoming increasingly severe, bringing certain information security threats to enterprises, such as cyber attacks, data leakage, etc., and also bringing serious impact on corporate reputation and customer trust. Therefore, the establishment of a comprehensive and efficient information security management strategy is the key to the internal control management of enterprises. In this context, this paper summarizes the relationship between enterprise internal control and information security management, puts forward enterprise information security management strategies, explores the implementation of information security management in enterprise internal control, and analyzes specific cases.

Keywords

internal control management; informatization; Security management policies

企业内部控制管理中信息化安全管理策略

严海

桂林特邦新材料股份有限公司，中国·广西 桂林 541004

摘　要

随着经济一体化和信息化进程的加快，企业发展的机会和挑战越来越多。信息技术的广泛应用，使得企业信息化进程加快，信息流已逐渐成为企业运作的“血液”。但是，网络环境的不断变化，数据泄露、网络攻击、内部欺诈等问题也日趋严峻，给企业带来一定的信息安全威胁，如网络攻击、数据泄露等，也给企业信誉和客户信任度带来严重的影响。因此，建立全面、高效的信息化安全管理策略，是企业内部控制管理的关键。在此背景下，本文概述了企业内部控制与信息化安全管理的关系，提出了企业信息化安全管理策略，探究了信息化安全管理在企业内部控制中的实施，并对具体案例进行了分析，仅供参考。

关键词

内部控制管理；信息化；安全管理策略

1 引言

在数字经济背景下，企业对信息的安全性提出了更高的要求，而基于信息技术的安全管理策略已经成为必不可少的环节，数据安全直接关系到企业数据的安全性、完整性和可用性，也关系到企业的长期经营和市场竞争能力的提高。通过实施信息化安全管理策略，能够提高企业抵御外来入侵及内部泄露的防护能力，从而降低信息安全事件的发生率。同时，基于信息技术的安全管理策略，采用先进的计算机软件，使内部控制管理的过程更加自动化、智能化，大幅提升管理工作的效率与准确性。通过对企业进行实时监测和数据分析，可以及时发现并纠正存在的内控漏洞，保证企业经营活动的合规性、高效性。因此，采用信息化的安全管理策略，不但可以大幅提高企业的内部控制能力，而且还能有效防范信息安全风险，为企业在不断变化的市场中稳步前进奠定基础。

2 企业内部控制与信息化安全管理的关系

企业内部控制主要是通过构建健全的管理制度，其目标是防范风险，提高管理效率，推动策略目标的达成，保证企业的各种业务活动能够按照规定的方针和政策顺利地开展，并保障资产的安全、完整，财务信息的真实、可靠，从而提高企业的运作效率与效益。信息化安全管理侧重企业在使用信息技术时，有效识别、评估、控制和监控各种类型的信息安全风险，从而保证信息系统的正常运转和数据财产

【作者简介】严海（1978–），男，中国广西全州人，本科，会计师，从事企业财务管理与内部控制研究。

的安全性。在数字经济发展的今天，信息化安全管理的重要性显得越来越突出，因为这不仅是企业声誉和客户信任的关键，也关系到企业的可持续发展。

企业内部控制与信息化安全管理之间有着密切的关系。一方面，信息化安全管理是企业内部控制的重要组成部分，通过强化信息安全管理，可以提高企业内控的准确性和实施效能，从而对由于信息泄露、系统瘫痪等原因造成的内控失败进行有效预防。另一方面，健全的企业内部控制体系，能够为企业信息化安全管理创造良好的支撑与制度环境，保证企业各项信息化安全管理措施的有效实施。因此，二者互为补充，构筑了一道安全的防御体系，确保企业的稳定运行[1]。

3 企业信息化安全管理策略

3.1 风险评估与管理

在企业信息化安全管理策略中，风险评估与管理是一个非常重要的环节。为了保证企业信息化建设的顺利进行，企业需要构建有效的风险评价体系，该体系要求对企业在信息化进程中所面临的各类安全风险进行综合辨识与评价，主要涉及数据泄露、网络攻击、系统故障等。根据风险评价结果，提出有针对性的对策。在企业面临的潜在危害和无法有效管理的情况下，要重视对其进行风险防范，并采取技术改进和工艺优化等方法减少其产生的概率。针对一些不能完全避免的情况，可以通过购买保险或与第三方服务商订立风险分担合同等方式降低其造成的损失。此外，企业还需要针对经过评估后确定可以接受的风险，制定具体的风险接受方案，确定风险监测与对策，保证一旦出现风险，就可以快速做出反应，有效控制风险的影响程度。在这种综合的风险评估和管理体系下，企业可以大幅提高其信息安全性，保障业务的稳健发展。

3.2 技术措施

在企业内部网中配置防火墙，确保企业的内部网不会受到入侵；通过入侵检测系统实时监测网络行为，对可能出现的安全隐患进行探测和应对；使用加密技术，保证资料在传送、储存时的安全，避免信息外泄。实施严格的身份认证机制，保证只允许合法的使用者进入。在授权管理中，对不同用户进行不同的授权，以防止因授权而引起的安全隐患，多因素身份认证更加强了账户的安全，就算密码泄露，也可以使用其他的身份确认方法确保账户的非法登录。定期备份系统中的关键信息，以保证一旦出现数据遗失、损毁等情况，可以及时修复，将造成的经济损失降到最低。在保证备份信息安全的前提下，确保备份信息不被他人获取和篡改。因此，为了保证企业信息财产的安全和稳定性，企业信息化安全管理需要注重技术措施，形成全方位、多层次的安全防护网。

3.3 管理措施

企业信息化安全管理，实施管理措施是重要步骤。首先，必须有一个完整、详尽的信息系统的安全管理体系。包含但不仅局限于清晰的安全性策略，这是一个在企业中为信息安全性行动的基础架构与准则；制定完善的作业程序，保证所有作业的正确实施；并制定完善的应对措施，使企业在面对突发情况时，可以快速反应，并将其控制在可控范围内，减少损失。其次，对职工进行安全教育。员工是企业信息安全的重要屏障，定期组织培训，既可以提高其辨别信息安全风险的技能，又可以提高其责任心和警惕性，保证在工作中能够自觉地遵守相关的规章制度，将人为失误造成的安全隐患降到最低。最后，定期开展安全审计与评估。运用专业化的审计方法，全面核查现行企业信息系统的安全性，评估其实施的有效性和不足，在其基础上持续改进管理制度，确保其高效、可靠。

3.4 合规性管理

为了保证企业信息化活动的合法性，一定要严格遵守国家有关的法律、规定和产业规范，这既关系到企业的信誉和长期发展，也是积极承担社会责任的表现。为了达到这个目标，需要构建一个完整的法规遵循系统。这一制度涵盖企业合规跟踪、合规审核和风险评估等各个环节，以保证企业对不断发展的法规和法规的及时、正确的把握和调整。成立专门的合规小组，密切关注企业的各项法律、政策变化，及时向企业内部汇报，并组织有关人员开展培训与调整，保证企业的各项信息工作都在合规范围之内。此外，强化内部审计与风险评估，定期自查、自纠企业的信息化活动，预警并改正潜在的合规风险，通过不断改进与优化，进一步提高企业的合规管理水平，助力企业的健康发展。合规性是企业信息化安全管理策略中的一个关键环节，应以强烈的责任心和使命感来保证企业的各项业务的合法性、合规性，营造安全、可靠的企业信息化环境[2]。

4 信息化安全管理在企业内部控制中的实施

4.1 明确责任与分工

明确信息化安全管理的主要职责，管理者作为信息安全的第一责任人，有责任制定策略导向，并提供所需的资源；IT 部主要负责相关的技术实现和日常维修工作，以保证安保体系的高效运转；作为企业的一分子，每个工作人员都应该积极主动地按照公司的规定去做，以预防可能发生的风险。保证信息系统的安全性，还需要建立跨部门合作机制。各部门之间要加强交流，及时发现潜在的安全隐患，并制定相应的对策。定期召开安全会议，搭建信息共享平台，加强各部门之间的协作，形成合力。通过这种方式，既可以提高信息系统的安全性，又可以对突发的安全事故做出快速反应，从而降低事故造成的损失。因此，在企业进行信息化安全管理的过程中，应明确责任与分工，并构建跨部门合作机制，共同构建企业信息安全防护的坚实保障。

4.2 整合信息化安全管理与内部控制体系

在企业的内部控制中，实行信息化的安全管理，应整

合信息化安全管理与内部控制体系，保证二者的密切联系和相互配合，这个一体化的进程既需要全面分析与评估企业的信息系统中的潜在风险点，并将其纳入内部控制的范围，形成全面、系统的管理体系。通过对企业的内部控制过程的合理调整，能够有效提高企业的信息安全管理水平。企业需要梳理已有的信息系统的安全管理流程，发现其中的冗余链条和安全隐患，并据此做出有针对性的优化与改善。同时，利用自动化监测、数据分析等现代信息技术，实时监测并迅速反应信息化安全风险，提高管理的准确性与及时性。在信息技术条件下，应加强安全管理和风险防范，将信息安全管理和内部控制系统相结合，优化内控流程，有效保障企业的信息安全。

4.3 持续改进与优化

信息化安全管理在企业内部控制中的实施，需要持续改进与优化，以保证企业信息安全性。要达到这个目的，就必须有一个健全、不断改善的信息化安全管理机制，定期评估已有的管理策略，找出其中的漏洞与不足。在此基础上，企业应根据评估结果，不断地改进现行的信息系统的安全管理战略，提升安全防护的针对性与全面性，确保各项安全措施能够有效应对当前的安全威胁，提升信息化安全管理的效率与质量。随着科技的不断发展，新的安全隐患也随之产生，这些新的威胁又会给企业的信息安全带来直接的影响。在此过程中，企业要密切关注新的科技发展以及可能产生的新威胁，适时地对其进行相应的信息安全管理，调整并更新安全防范手段，保证企业的信息化安全管理紧跟时代步伐 [3]。

4.4 加强信息化安全培训与意识提升

企业要经常对全部人员进行信息安全的教育，包括最近的网络安全法律法规、常见的网络攻击方式和预防策略及个人信息保护方式等，通过模拟黑客攻击、数据泄露等突发情况，让每个职工都做好信息安全的保卫者，提高员工应对突发事件的应变能力。建立健全的企业信息安全管理体系，激励企业积极发现和举报安全隐患，营造“人人关心安全，人人参与安全”的良好企业文化，利用公司内部简报、海报、网上授课等方式，在安全教育中持续传播信息安全知识，提高职工的防范意识与责任心。此外，建立更加严格的重点工作岗位及敏感资料处理人员的安全教育与资格证书制度，以保证其具有较高的安全管理与技术保护技巧，通过建立全方位、多层次的信息技术安全训练系统，可以使企业的总体安全防护能力得到提高，同时也可以进一步提高企业的内部控制水平。

5 案例分析

某集团有限公司（简称某集团），是一家以房地产开发为主，金融、优家为一体的全球大型多元化运营集团。某集团面临日趋复杂的网络环境，以及面临的数据安全性问题，提出了采用先进的信息化安全管理系统。该系统集成防火墙、入侵检测、数据加密及身份验证等多重防护技术。首先，采用先进的防火墙技术，有效隔绝来自外部的安全隐患，保证企业内的信息安全。其次，利用入侵检测技术对整个网络进行动态监测，当出现任何不正常的情况时，可以及时向用户发出警报，使整个安全小组能够迅速响应并处理。对于数据保护，某集团对每一份资料都采取了严格的保密措施，确保从储存到传送的过程，数据都具备一定的机密性与完整性。此外，通过多因素验证，强化员工对企业资源的权限管理，从而减少内部泄露的风险。同时，某集团也会经常举办网络安全训练及演习，让各部门的员工了解并掌握安全威胁和应对策略，以提高员工的安全防范能力，营造良好的安全文化氛围。最终，某集团采用信息化安全管理策略，使企业的整体安全水平得到明显的提高，有效防范各种类型的网络安全风险，为企业数字化转型保驾护航，具有较高的参考价值 [4]。

6 结语

综上所述，基于信息技术的安全管理策略，已成为企业内部控制的核心组成部分，为企业信息安全保驾护航，并助力企业核心竞争力的跃升。通过科学的风险评估、严谨的管理流程、先进的技术手段及严格的合规管理，构建坚实的网络安全防御体系。同时，深度融合信息化安全管理与内部控制体系，明确职责划分，持续优化改进，确保企业在瞬息万变的市场环境中保持竞争优势，实现高质量发展。

参考文献

[1] 庞倩倩.企业会计信息化内部控制中存在的问题及对策探讨[J].中国乡镇企业会计,2024,(13):164-166.

[2] 孟勇.信息化背景下加强企业内部控制的对策[J].中国电子商情,2024,(01):49-51.

[3] 秦晓宇,金・尕迪.国有企业内部网络信息安全访问控制模型设计[J].信息与电脑(理论版),2022,34(14):211-213.

[4] 杨毓,陈园.大数据对企业内部控制信息安全影响研究[J].中外企业家,2020,(06):71.