分类号：　　单位代码：10335

密　级：　　学　　号：21860805

浙江大学

硕士专业学位论文

中文论文题目： CZ银行小微贷款系统的信息安全风险评估研究

英文论文题目： **Research on Information Security Risk Assessment of Small and Micro Loan Business System in CZ Bank**

申请人姓名：张　斌

指导教师：王义中

合作导师：

专业学位类别：工程管理（专业学位）

专业学位领域：工程管理

所在学院：工程师学院

论文提交日期　2022年9月30日

CZ 银行小微贷款系统的信息安全风险评估研究

论文作者签名:_____

指导教师签名:_____

论文评阅人 1：_____

评阅人 2：_____

评阅人 3：_____

评阅人 4：_____

评阅人 5：_____

答辩委员会主席：_____

委员 1：_____

委员 2：_____

委员 3：_____

委员 4：_____

委员 5：_____

答辩日期：_____

Research on Information Security Risk Assessment

of Small and Micro Loan Business System in CZ Bank

Author's signature:_____

Supervisor' s signature:_____

External Reviewers: _____

_____

_____

_____

_____

Examining Committee Chairperson:

_____

Examining Committee Members:

_____

_____

_____

_____

_____

Date of oral defence: _____

浙江大学研究生学位论文独创性声明

本人声明所呈交的学位论文是本人在导师指导下进行的研究工作及取得的研究成果。除了文中特别加以标注和致谢的地方外，论文中不包含其他人已经发表或撰写过的研究成果，也不包含为获得浙江大学或其他教育机构的学位或证书而使用过的材料。与我一同工作的同志对本研究所做的任何贡献均已在论文中作了明确的说明并表示谢意。

学位论文作者签名：张强　　签字日期：2022年9月27日

学位论文版权使用授权书

本学位论文作者完全了解浙江大学有权保留并向国家有关部门或机构送交本论文的复印件和磁盘，允许论文被查阅和借阅。本人授权浙江大学可以将学位论文的全部或部分内容编入有关数据库进行检索和传播，可以采用影印、缩印或扫描等复制手段保存、汇编学位论文。

（保密的学位论文在解密后适用本授权书）

学位论文作者签名：张强　　导师签名：[illegible]

签字日期：2022年9月28日　　签字日期：2022年9月28日

致谢

时光荏苒，行色匆匆，经历了丰富的课程学习，让我更感持续学习之重要。行文至此，发觉我的学习阶段已渐尾声，学习期间感触良多，感谢的人和事不胜枚举。

首先，本论文是在我的导师王义中教授指导下完成的。王义中教授渊博的专业知识，严谨的治学精神对我的成长产生了深远影响。在论文撰写期间正是王老师百忙之中不辞辛劳的指导，才让本人对论文编写思路更加清晰，才使本文顺利完稿，在此本人向导师王义中教授表示深深的谢意！

其次，感谢浙江大学工程师学院提供优秀的学习平台和师资力量，让我在此开阔了视野，深入理解了“求是”精神，感谢一起陪伴学习成长的老师和同学们。

最后，感谢家人对我学习的默默支持，正是你们的理解与支持，才使得我的学业顺利完成。

摘要

信息技术的不断深入，加速了金融科技的高效发展，给商业银行业务智能化的带来了新的发展契机。银行业务过程中有大量资金流转和用户敏感数据共享，这些都给信息安全风险管理工作带来了前所未有的挑战，一旦发生严重安全事件将直接危害用户财产或个人敏感隐私数据，甚至影响民计民生。近年来，银行业关键信息系统网络安全事件频率呈上升趋势，针对商业银行信息系统的信息安全风险评估的研究具有实践意义。

本文以CZ银行小微贷款系统的信息安全风险为研究对象，构建了基于层次分析法与模糊综合评价法结合的模型，结合德尔菲法建立了该系统的信息安全风险评价体系，并对CZ银行小微贷款的信息安全风险进行风险评估。

本文建立了CZ银行信息系统的信息安全风险因素递阶层次体系，即准则层为物理安全、数据安全、运行安全、管理安全 4 项，方案层为机房环境安全、设备安全、通信线路安全、存储介质安全、认证与鉴权、访问控制、数据加密、抗抵赖与审计、系统容灾备份、恶意软件防护、网络攻击防护、人力资源管理、信息安全制度、信息安全培训等14项。该指标体系经文献检索与专家判断结合方式获得，科学性与合理性较强。

本文证明了层次分析法结合模糊综合评价法模型在对CZ银行小微贷款系统的信息安全风险评估场景中具有适用性。通过层次分析法对风险评估指标体系进行构建与权重计算，同时采用模糊综合评价法对被评估对象进行综合评价，解决了小微贷款系统风险评价过程中模糊性定性结果到科学性量化结果的转化。实践证明，该模型可以应用在CZ银行小微贷款的评价过程中，因此可以推广到其他同类信息安全风险评估场景中。

本文通过对CZ银行小微贷款系统的信息安全风险评估的研究，实证了层次分析法结合模糊综合评价法模型的可行性与普适性，可为商业银行同类信息系统的信息安全风险管理以经验和参考。

关键字：金融科技；信息安全；风险评估；模糊综合评价法；层次分析法

Abstract

The continuous deepening of information technology has accelerated the efficient development of financial technology and brought new development opportunities to the intelligentization of commercial banking business. In the process of banking business, there are a large number of capital flows and users' sensitive data sharing, which have brought unprecedented challenges to information security risk management. Once a serious security incident occurs, it will directly endanger users' property or personal sensitive privacy data, and even affect people's livelihood and people's livelihood. In recent years, the frequency of network security incidents of key information systems in the banking industry has been on the rise, and the research on information security risk assessment of commercial bank information systems has practical significance.

This paper takes the information security risk of CZ Bank's small and micro loan system as the research object, constructs a model based on the combination of analytic hierarchy process and fuzzy comprehensive evaluation method, and combines the Delphi method and the questionnaire method to establish the information security risk evaluation system of the system. , and conduct risk assessment on the information security risks of CZ Bank's small and micro loans.

This paper establishes a hierarchical system of information security risk factors of CZ Bank information system, that is, the criterion layer is physical security, data security, operation security, and management security, and the scheme layer is computer room environment security, equipment security, communication line security, and storage. Media security, authentication and authentication, access control, data encryption, non-repudiation and auditing, system disaster recovery backup, malware protection, network attack protection, human resource management, information security system, information security training, etc. 14 items. The index system is obtained through the combination of literature retrieval and expert judgment, and it is scientific and reasonable.

This paper proves that the analytic hierarchy process combined with the fuzzy comprehensive evaluation method model has applicability in the information security risk assessment scenario of CZ Bank's small and micro loan system. The risk assessment index system

is constructed and weighted by the analytic hierarchy process, and the assessed object is comprehensively assessed by the fuzzy comprehensive assessment method, which solves the transformation from the fuzzy qualitative results to the scientific quantitative results in the risk assessment process of the small and micro loan system. . Practice has proved that this model can be applied in the evaluation process of CZ Bank's small and micro loans, so it can be extended to other similar information security risk assessment scenarios.

Through the research on the information security risk management of CZ Bank's small and micro loan system, this paper demonstrates the feasibility and universality of the analytic hierarchy process combined with the fuzzy comprehensive evaluation method model, which can provide experience for the information security risk management of similar information systems in commercial banks. and reference.

Keywords: Fintech; Information Security; Risk Assessment; Fuzzy Comprehensive Evaluation; Analytic Hierarchy Process

目录

插图清单

附表清单

1 绪论

1.1 研究背景

近年来，随着信息技术的飞速发展，信息技术与商业银行业务的融合极大地推动了金融科技的高速发展[1]。但金融科技在推动并加速我国商业银行信息化变革进程的同时，由于信息安全技术与金融科技发展的不对称，信息安全风险评估不到位，造成各种信息安全问题不能及时有效发掘出来，导致安全漏洞持续暴露，造成诸多网络与信息安全事件，引发诸如病毒木马、信息泄露、资金失窃、非法控制、数据篡改等严重事故，给银行金融信息化业务带来了极大的信息安全挑战与危害[2]。

商业银行数字化的快速迭代，各种网络安全威胁成为制约金融活动持续有效运行的“瓶颈”。信息系统的信息安全，是在业务活动中，由于技术漏洞和管理缺陷产生的影响信息与网络的可用性、完整性、机密性等信息安全方面风险[3]。经过多年的建设发展，商业银行金融业务信息系统基于传统信息安全防御理论建立的信息安全体系初步建立，信息安全基础架构基本形成，信息安全设备及系统基本完备，基本可以满足当前实际需要；而随着数字化业务的不断更迭，商业银行金融活动信息系统信息安全防护体系存在的不足变的越来越明显，普遍面临着严重的信息安全风险[4]，严重制约金融业务的持续发展，亟待一套行之有效的风险评估方法有效地挖掘信息安全风险，提升安全防护水平，保障业务的持续稳定增长[5]。近年来商业银行持续开展大规模科技创新信息系统构建，但由于疏于信息安全风险管理导致的安全事件屡见不鲜，且呈现持续上升趋势，事件类型影响巨大，造成了严重的直接和间接损失。近五年商业银行信息系统重大网络安全事件比比皆是，国内外大中商业银行均受到不同程度影响。

(1) 2016 年 5 月，孟加拉国 Bangladesh 银行跨行结算交易 SWIFT 协议存在安全漏洞，导致黑客利用该漏洞进行资金盗窃，最终导致该银行损失 8100 万美元[6]。

(2) 2016 年 10 月印度国家银行（SBI）、印度工业信贷投资银行 ICICI、YeCZ 银行、AxiCZ 银行以及 HDFC 在内的多家银行信息系统遭受严重恶意软件攻击，造成数据库中 320 万用户的借记卡信息泄漏，严重威胁了相关用户个人信息数据的隐私性[7]。

(3) 2017 年 6 月，黑客组织 Anonymous 与 Armada Collective 对全球多家金融机构实施了一系列网络攻击行动，使多家线上银行服务干扰，导致严重的业务中断银行，造成严重的业务损失[8]。

(4) 2019 年 1 月国内某银行某技术处长利用职务之便，在银行核心系统内植入计算机恶意程序，为自己个人账户持续“转账”，共支取 700 多万据为己有，造成了严重的信息技术风险与资金损失[9]。

(5) 2020 年 9 月，智利 BancoEstado 银行遭到黑客大规模黑客攻击，导致重要业务文件被恶意加密并勒索巨额赎金，造成相关分行被迫关闭，严重影响正常金融业务[10]。

(6) 2021 年 5 月，据国外网络安全研究机构统计，针对去中心化借贷协议 DeFi 的黑客攻击持续上升，造成近 2 亿美元损失[11]。大量的网络安全事件造成了严重的业务影响，给全球商业银行业务造成了严重的损失。

这些典型的信息安全事件给商业银行信息系统带来了前所未有的警示。商业银行信息系统的逐步发展，需要信息安全管理水平提升的支撑，以缩小信息资产的风险暴露面，促进信息安全风险防控效果[12]。虽然我们已经意识到信息安全风险管理对商业银行新系统的重要性，但我国商业银行针对信息系统的信息安全风险评估工作仍有一定欠缺，并未形成系统、科学的综合评估方法。因此，需针对当前商业银行信息系统现状，提出可行、系统、科学的评估方法。

1.2 研究意义

大数据、物联网、机器学习、人工智能等新兴信息技术为商业银行创新金融业务开展提供了非常好的技术架构，也更好地促进了商业银行金融互联网化、信息化、智能化、体系化[13]，这些由科技引发的创新，能对金融活动产生实质的促进作用，被业界称为金融科技[14]。然而金融科技发展的同时，随之而来的是严峻的信息安全风险挑战。大规模商业银行信息系统的数据泄漏、关键在线银行业务中断、电子银行资金失窃等安全事件频发，给商业银行金融业务信息安全风险管理带来了新的挑战[15]。在此背景下，商业银行金融数字化工程中急需针对信息系统构建完整信息安全风险管理体系，提升网络安全管理水平。

截至 2021 年 12 月 31 日，中国大陆有开发性金融机构 1 家、国有大型商业银行 6 家、政策性银行 2 家、股份制商业银行 12 家、城市商业银行 128 家、农村商业银行 1596 家，不论数量还是资金体量都是世界前列的[16]。银行业务和数字化逐步深化的同时，我国商业银行的信息安全风险也逐步成为制约发展的关键因素。我国商业银行当前信息系统仍存在诸多信息安全风险，主要包括系统漏洞等技术风险与制度体系等管理风险，针对这

些风险管理有全面的管理体系规范[17]，包括《商业银行信息科技风险管理指引》、《ISO/IEC27001 信息安全风险管理标准》、《GB/T 20984 2007 信息安全技术信息安全风险评估规范》等诸多安全管理指南，但针对商业银行系统的风险管理需要从银行业务属性出发，明确金融资产价值与风险影响性，从业务属性角度开展科学风险评估，以提升风险管理水平[18]。本文以商业银行信息系统的信息安全风险入手，对其存在的信息安全风险进行识别、评估，并提出风险控制方案，以提升风险应对能力。本文的主要研究目的为：一是在前人研究信息安全风险评估的基础上，深入剖析 CZ 银行小微贷款系统存在的信息安全风险，借鉴技术与管理风险控制思路，系统地降低该系统的信息安全风险。二是运用标准信息安全风险管理体系规范，结合德尔菲法，对 CZ 银行小微贷款系统进行充分的信息安全风险指标识别。三是运用层次分析法与模糊综合评价法，对 CZ 银行小微贷款系统信息安全风险进行评估，明确高风险项，提出相应风险的解决方案。本文研究的理论与实践意义归纳起来有如下几点:

(1) 为 CZ 银行小微贷款系统信息安全风险评估提供依据：对于商业银行信息安全风险评估越来越多，研究方法业层出不穷。本文通过采用层次分析法与模糊评价法结合，弥补了传统层次分析法一致性校验不足的劣势，通过定性与定量结合思路，构建了评估 CZ 银行小微贷款系统的信息安全风险模型，这既是对以前学者研究成果的总结，也是对后来学者新评估思路的借鉴。

(2) 作为商业银行信息安全风险自检工具，降低安全事件发生与损失：科学系统的信息安全风险评估方法，可以有效地发掘商业银行信息系统的安全风险，为控制风险输入了关键的风险弱点，提升了风险控制效果。针对信息系统的信息安全风险，人们往往只关注技术风险，而忽略了深层次的管理风险，这使得风险的根源不能得到进一步挖掘。因此本文通过层次分析法与模糊综合评价法对小微贷款进行系统风险评估的研究，提供了一种科学系统的评估方法，提升了风险评估效果，可以有效降低信息安全事件发生概率以及事件发生的损失。

(3) 为商业银行信息化规划提供参考：商业银行业务持续发展，促进了银行科技的新业务、新技术落地，而信息安全是商业银行信息系统稳定运行的基础，因此信息安全的管理水平直接关乎商业银行信息规划。本文通过对 CZ 银行小微贷款系统风险评估的研究，提出了结合层次分析法与模糊综合评价的信息安全风险评估思路，可以科学有效地发掘

商业银行信息系统潜在的信息安全风险因素，对信息安全事件进行有效的预判，进而采取合理的规划，从规划阶段减少信息安全事件的发生。

(4) 为我们信息安全保险业提供评估依据：随着信息技术的发展，多家保险架构针对信息系统开拓了信息安全保险业务，但对于保险定价、标的评估过程没有统一、科学的方法来高效开展保险业务。保险机构是风险管理的重要环节，也是风险事件损失的“接力棒”，他们承担信息系统的信息安全保险时，需要具备科学有效的风险评估办法对承保系统进行全面的信息安全风险评估，明确风险因素与风险级别，以便更好地评估保费与保险策略。本文研究成果可以科学有效地建立信息系统的信息安全风险评估方法，对于保险行业的保费评估起到了借鉴作用。

1.3 国内外研究现状

1.3.1 信息安全风险评估研究

(1) 国外研究综述

20 世纪 80 年代，信息技术从军方逐步扩展到民方，通信与信息技术发展给社会、经济发展带来了新的机遇，与此同时信息安全问题也表现出了多样化趋势。1993 年，美国发布了通用准则，即 CC 标准；1995 年英国发布了 BS7799 标准，成为最早的体系化信息安全风险管理规范[19]。CC 标准侧重于信息安全风险评估，对信息系统各流程环节进行审查约定，并明确了相关技术规范要求，技术性较强[20]；BS7799 则是针对组织的信息安全风险管理标准，侧重点为通过对组织、资产、战略等风险的管控，提升整体风险管理水平，该标准中侧重持续化优化与保持，重点提到了 PDCA 循环思想在信息安全风险管理中的实践应用[21]。这两套标准后来分别演变成了 ISO 15408 和 ISO/IEC 27001 标准，同时也推出了 ISO/IEC 27005 信息安全风险评估规范，并逐步推广成为全球认可度较高的信息安全风险管理体系性规范[22]。

COBIT（信息和相关技术控制目标）是当下国内外公认的信息系统审查规范，自二十世纪九十年代发布以来，已经持续更新到了 COBIT2019 版本[23]。该规范在商业风险、控制目标和技术风险三方面进行了关联性约束，并在企业战略、成本、风险、技术、人员等多角度进行了规范明确，提出了有效性、完整性、机密性、复合性等控制目标[24]。进入 21 世纪后，美国相继发布了 NIST-SP800-30 信息安全风险评估规范和 NIST-SP800-37 信息安全风险管理规范[25]，开发了一种针对信息资产、自身弱点、外部攻击与风险的关

联办法，分别从业务连续性、完整性、秘密性角度进行风险评测[26]，形成了较为完备的风险评估思路。

二十世纪八十年代巴塞尔银行委员会颁布了《巴塞尔资本协议》，明确了银行风险管理要求、银行资本的构成、信用资产的容量等内容。为适应新时代银行的风险管理，2013 年重新修订后发布了 Base III[27]。新的巴塞尔资本协议适用国际化银行风险监管，对市场活动风险、业务风险、信任风险进行标准化约束，并通过资金充足率、监督核查、数据披露三方面进行安全评估，实现通过监管约束实现风险控制水平的提升[28]。2002 年美国议会颁发了《2002 年公众公司会计改革和投资者保护法案》[29]，该法案由 Paul Sarbanes 和 Mike Oxley 共同提出，即“SOX 法案”。“SOX 法案”对美国上市公司提出了全面的内部控制和风险管理合规要求，同时针对 IT 风险管理也提出了全面的监管细则，使得在美上市的公司必须遵照该法案进行全面的数字风险治理[30]。

在国际上，NIST SP800 系列和 ISO/IEC 27001 系列信息安全风险管理标准通过实践证明都是通用性管理规范，在金融类特定行业需要加强基于自身行业特性的信息安全风险管理体系的挖掘与建立。2004 年美国 COSO 委员会在其前期颁布的《内部控制—综合框架》内容上，结合了“SOX 法案”相关内容，颁布了《企业风险管理—整合框架》，为国际化企业提供统一的内部管理框架和规范，并在 2017 年进行修订重新颁布《企业风险管理框架——与战略和绩效的整合》[31]，简称 COSO 2017。其提出了企业内部管理过程由评估、监测、控制、沟通等主要内容构成[32]。新加坡金融局 2013 年发布了《技术风险管理指引》，从金融技术风险管理上明确金融机构在信息技术风险管理的相关要求，同时提出了安全治理、安全组织的约束，并兼顾了巴塞尔协议的相关思路[33]。

(3) 国内研究综述

20 世纪 90 年代，《计算机信息系统安全保护条例》颁布并执行，提出了等级保护的管理要求，并在国内逐步开展等级保护评估方法、安全产品的评估、系统安全级别划分规范等研究。2019 年 12 月，我国正式开始执行新的等级保护制度，明确了云计算安全、物联网安全、工业互联网安全的等级保护管理要求[34]，同时提出了安全管理中心架构，进一步提高了安全管理要求。

国内信息安全风险管理标准也借鉴了 ISO15408（即 CC 标准）、ISO/IEC 27001、ISO/IEC 27005，分别形成了 GB/T 18336、GB/T 22080 和 GB/T 20984[35]，阐释了信息安

全的基本原则，明确了风险评估由信息资产、自身弱点、外部攻击等过程组成，并为信息安全风险管理的提出指导，为国内信息安全风险管理提供了有效的参考。2009 年中国银行业监督管理委员会为加强商业银行信息科技风险的管理要求，发布了《商业银行信息科技风险管理指引》。该指引是国内重要的商业银行信息科技风险管理规范，其明确了在信息科技在业务活动可能引发的操作风险、信息安全风险、安全管理风险等，进一步规范了相关风险的约束与管控[36]。目前该规范是国内商业银行业务信息系统安全风险管理重要参照标准之一[37]。

国内商业银行业在信息安全风险管理方面投入了非常多的精力，相关过程形成了如下风险管理状态：一是信息安全风险管理合规体系基本形成，参照国家等级保护要求、行业信息科技风险管理、国际 ISO/IEC 27001 等体系规范逐步形成了合规体系化管理的模式，已经初步形成了信息安全风险管理规范化、标准化[38]，形成普适性合规管理模式；二是商业银行金融科技的持续迭代需要科技的革新，也需要信息安全技术的创新。在信息安全风险管理过程中运用新兴信息技术可以提升管理效率[39]。三是监管科技发展推动了行业信息安全风险管理的发展，特别是近年国家对信息安全、隐私保护的高度重视，更是推动了我国信息安全风险监管科技的发展[40]。

1.3.2 信息安全风险评估的 AHP-FCE 应用研究

(1) 国外研究综述

1971 美国著名数学家 Satty 教授于二十世纪 70 年代提出层次分析法（Analytical Hierarchy Process，以下简称 AHP），是一个可以处理多指标、多层次复杂问题的分析方法[41]，并在 1990 年对 AHP 方法应用在决策方面的实践进行了说明[42]。1965 年美国专家 Zadeh 教授提出了模糊集理论（Fuzzy Sets）的概念，用来表示事物的不确定性[43]，后根据模糊集合和隶属度的数学方法，实现了解决现实中定性问题的科学分析。AHP 和 FCE 在处理决策分析、方案比选方面具有非常良好的互补性，应用广泛，2004 年 Han L 将 AHP 方法与 FCE 方法结合应用与评估分析研究中[44]。Liem 等采用 AHP 与 FCE 结合方法对综合生态指标进行分析，创造了综合评估生态环境的新思路[45]。ZW Feng 将 AHP 与 FCE 方法应用于煤气风险识别与评价，建立了煤气风险指标体系，并对结果进行了充分评估[46]。Ling X 采用 AHP-FCE 方法应用于卫星移动通信决策评估领域[47]。

AHP-FCE 模型在国外应用广泛，很快被应用到了信息安全风险评估领域。Sha F 采用

AHP-FCE 对信息安全风险进行评估，构建了完整的信息安全风险指标模型，并对信息安全的风险评估给出了应用思路[48]。L Xiao 等通过多级模糊评价结合 AHP 方法建立了对信息系统风险评估的思路[49]。Peng X 等结合 AHP 与 FCE 对信息安全风险进行研究，通过实例研究了 AHP 与 FCE 方法结合的应用场景[50]。

(2) 国内研究综述

AHP-FCE 评估模型在国内应用广泛。马永刚采用 AHP-FCE 方法对港口物流竞争力进行了研究，并通过上海港与釜山港实例对比应用该方法可行性[51]。赵伏军等采用该方法对矿井通风系统进行评估，并给出优化建议[52]。赵彬等采用该模型对综合实战系统的指挥效能进行分析，实现了不便于量化的信息量化评价，识别了应用重要的因素。而在信息安全风险评估领域，AHP-FCE 在国内有较成熟的应用研究[53]。肖龙等将 AHP-FCE 应用到信息安全风险评估领域，并给出了实例应用，提升了 AHP-FCE 在国内信息安全领域的应用[54]。韩霞等将 AHP-FCE 应用于电力信息系统领域，对电力行业相关系统进行了信息安全风险评估，提升了电力系统风险评估新思路[55]。

1.4 研究内容与研究方法

1.4.1 研究内容

安全是动态的，风险是不确定的，金融科技的持续发展更需要信息安全风险评估方法支撑[56]。对于商业银行来说，信息安全风险管理远不止安全防护技术的堆砌，而更应像 Bruce Schneider 所说的——“安全应该是一套管理流程”[57]。商业银行在面对信息安全风险管理过程中，需要一套科学、系统的风险识别、评估方法，以便准确地发现信息系统安全风险，提出针对性解决方案，提升信息安全风险管理水平。

本文研究内容为 CZ 银行小微贷款系统的信息安全风险评估，通过德尔菲法的结合开展风险识别与评估指标确认，构建层次分析法与模糊综合评价法结合的评价模型，对信息安全风险进行定性与定量分析，提高评估科学性与实用性，不仅验证了评估模型的科学性与普适性，也具有一定的实践意义。

1.4.2 研究方法

本文通过定性与定量结合方法提升风险评估的系统性与科学性，主要采用模糊综合评估法和层次分析法开展研究；辅助方法有文献研究法和德尔菲法，以提升风险识别过

程可操作性和科学性。相关方法说明如下：

(1) 文献研究法：通过信息安全风险相关文献进行深入统计、分析、调研，借鉴前期学者相关经验和知识，识别相关信息系统面临的风险因素与指标。该方法简便易用，具备一定的科学依据，说服力强，应用广泛。

(2) 德尔菲法：德尔菲法通过邀请专家进行多轮匿名问答、统计分析、反馈机制，直到达成一致意见，该方法对相关问题进行全面剖析，并通过多名专家、多轮匿名问答方式提升了评判结果的科学性、准确性。信息安全风险识别过程中，采用德尔菲法对关键信息安全风险指标进行识别，并对指标进行递阶层次构建，提升指标建立效果。

(3) 层次分析法：层次分析法可以处理复杂因素指标问题的量化分析方法。该方法建立在对系统充分分析的基础上，将复杂的因素联系分解为由局部简单关系构成的递阶层次关系，通过构造关系矩阵、权重向量和评级矩阵进行模糊综合评估的分析方法。信息安全风险评估中，通过调研得到的信息安全风险指标体系，通过建立层次分析数学模型进行量化计算分析[58]，获得影响CZ银行小微贷款系统信息安全风险指标权重，提升风险评估的科学性、系统性。

(4) 模糊综合评价法：模糊综合评价法是根据模糊数据的隶属度理论将定性的评价结果转化为定量结果的方法。针对CZ银行小微贷款系统风险评估过程中，采用模糊数学的隶属度思路将定性结果定量化，获得被评估对象各指标分值信息，提升评价的数据性、合理性。

1.5 技术路线与论文结构

1.5.1 技术路线

本文技术路线主要从研究方法、研究内容、研究思路三个方面进行介绍。研究方法方面，本文采用文献分析法、德尔菲法、模糊综合评价法、层次分析法等方法，对CZ银行小微贷款系统的信息安全风险进行识别、评价，以明确信息安全风险因素、指标权重，挖掘信息安全风险要素。研究内容方面针对CZ银行小微贷款系统开展信息安全风险识别与评估，给出信息安全风险对策，以提升风险应对效果。研究思路方面分别从问题的提出、分析、解决角度进行研究，对应研究内容中的绪论、风险识别与评估、风险对策。本文研究技术路线如下图所示。

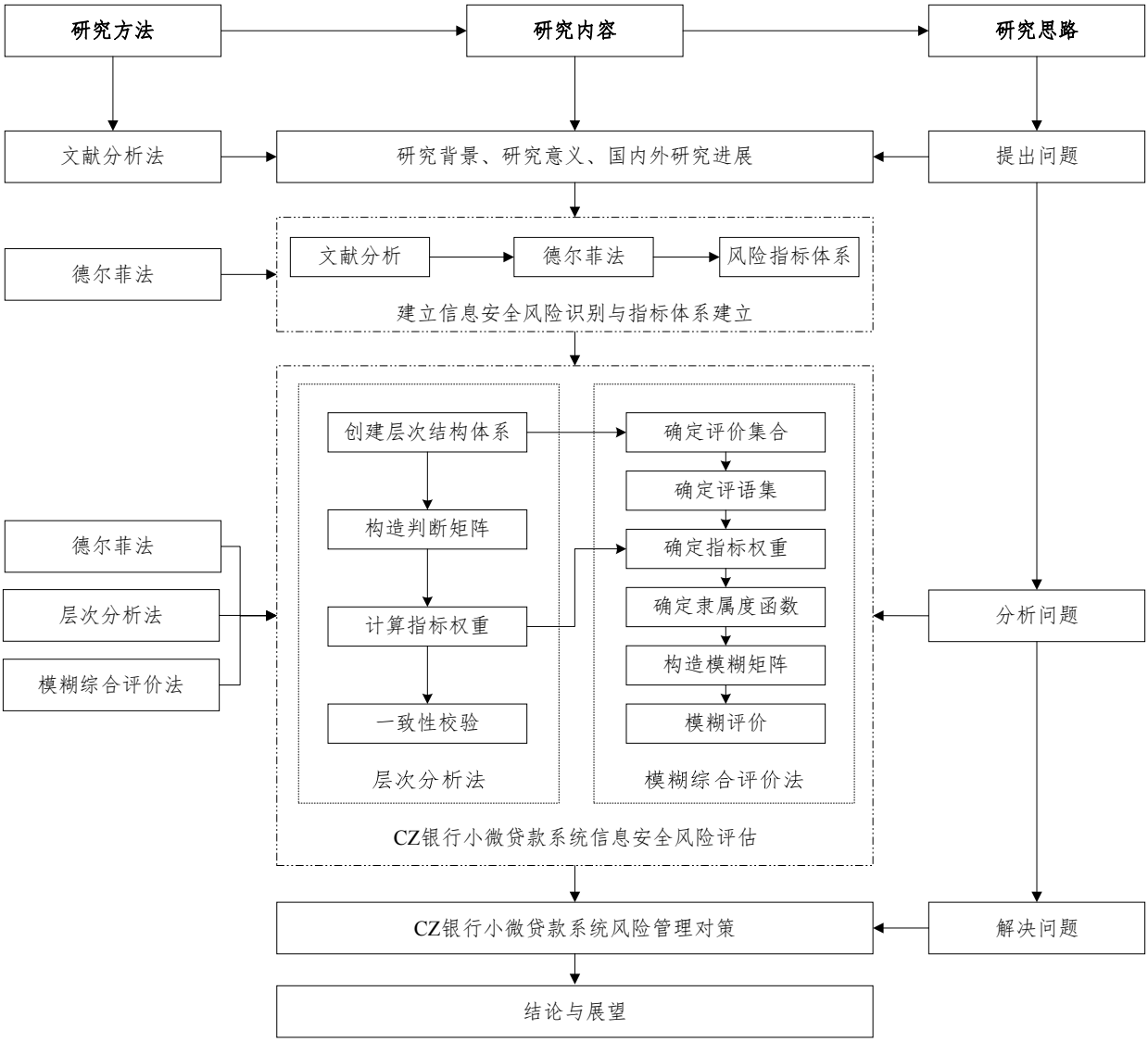

图 1-1 本文研究技术路线图

1.5.2 论文结构

第 1 章绪论，介绍本文研究背景、意义、内容及研究路线。

第 2 章 CZ 银行小微贷款系统信息安全风险识别与指标体系确定，本章节通过对 CZ 银行小微贷款系统现状进行分析，识别管理问题，并通过德尔菲法确认安全风险指标。

第 3 章结合 CZ 小微贷款风险现状，通过对比风险评估方法，建立基于 AHP-FCE 的信息安全风险评估思路。

第 4 章通过层次分析法与模糊综合评价法，对 CZ 银行小微贷款系统进行风险评估，明确当前风险状态，识别主要风险问题。

第 5 章针对风险评估结果，提出信息安全风险控制对策，提升风险应对能力。

第 6 章结论与展望，总结本文研究的成果，并说明未来的改进和研究目标。

2 CZ银行小微贷款系统信息安全风险识别

2.1 CZ银行小微贷款系统概况

CZ银行成立于二十世纪末，是经中国银行业监督管理委员会批准成立的商业银行。成立以来，CZ银行确立了“科技创新、业务合规”的经营文化，充分利用新兴信息技术为客户提供智能化的金融服务。CZ银行积极拥抱金融科技，紧跟银行业信息化进程，加快推进数字化转型。2016年CZ银行在区域银行业中率先开展云计算网络体系构建，并经过5年时间充分融入金融业务；2019年，引入区块链技术，对存单、存证等票据管理上进行了初步的应用，取得了较好的效果。

2016年，国务院印发《推进普惠金融发展规划（2016-2020）》，首次提高了普惠金融在国家金融政策层面的地位[59]，国家十四五规划再次将有效推进普惠金融标准建设列为重要工作目标，而小微企业贷款作为关键普惠金融内容已成为商业银行贷款业务的重要组成[60]。CZ银行自2015年起逐步开始针对小微企业开展贷款业务，“十四五”规划初期，为更好地服务区域小微企业，并于2016年中上线小微贷款系统，一方面强化内部贷款管理，另一方面提升客户体验，为小微企业提供便捷的线上贷款业务。

(1) 信息科技团队组织架构

CZ银行信息安全管理部属于信息科技部的下级部门，负责全行信息安全管理与技术综合管理工作。信息科技部共有在编115人，信息安全管理部有在编12人，其相关组织架构如下表所示：

表2-1 CZ银行信息科技部组织与职责明细表

序号	部门	部门职责
1	综合管理部	负责信息科技部门相关综合办公、行政管理、党群建设； 负责协调其他部门信息技术管理工作；
2	系统运维部	负责信息系统硬软件的部署、调试和运维工作； 负责信息系统网络的部署、调试和运维工作； 负责信息系统应用和数据库部署、调试和运维工作； 负责网络安全设备的安装部署工作；
3	应用开发部	负责信息系统需求、规划、设计、编码、测试、维护工作； 负责规范应用系统、中间件、数据库编码和管理规范； 负责对接业务部门开展信息系统建设规划设计；
4	终端运维部	负责营业厅信息系统资产运维部署、调试、运维工作； 负责ATM机部署、调试、运维工作； 负责信息主机端部署、调试、运维工作；

续表 2-1

序号	部门	部门职责
5	科技创新部	负责大数据、云计算、物联网等新技术研究与落地场景研究 负责区块链技术研究与落地工作
6	信息安全管理部	负责信息安全设备部署、调试、运维工作； 负责日常安全管理监测、预警、响应与恢复工作； 负责信息安全风险评估、风险处置、风险优化等管理工作； 负责信息安全管理策略制定、规划、实施工作； 负责信息安全政策、标准合规管理工作；

(2) 小微贷款系统网络架构

CZ银行信息科技经历了10余年的快速发展，参考了当下政策、标准、规范，借鉴了行业领先单位的信息技术优势，形成了适合自己业务发展的“两地三中心”云计算网络体系架构，形成异地“双活”、多层次网络安全防御体系，网络架构示意图如下所示：

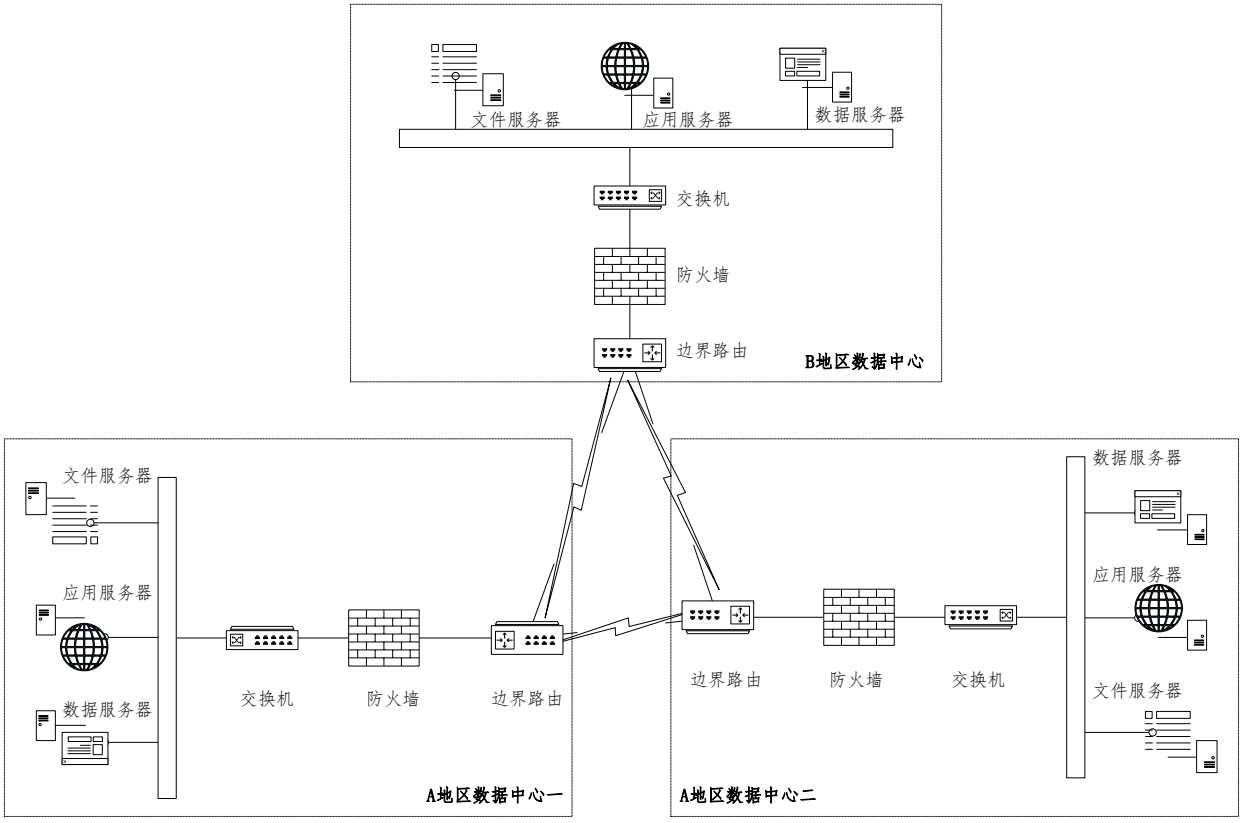

图 2-1 CZ 银行网络架构示意图

CZ 银行网络安全架构示意图如上所示，网络安全架构共分为网络安全接入防护层、应用安全防护区、数据安全与安全审计管理区，相应功能如下：

① 网络接入安全防护层：该层是网络架构最外层，是最先遭受网络攻击的主要层面，所以此层次担负着整个体系架构的主要网络安全防护与容灾管理工作。该层次中通过路由器策略管理实现“两地三中心”的双活灾难管理模式，通过抗 DDoS 安全网关、网络

防火墙、入侵防御系统、APT攻击预警平台实现对网络攻击的防御、监测、预警能力；

② 应用安全防护层：该层是针对应用系统、服务进行攻击过滤、防护的核心层次。CZ银行整体信息系统有超过230个，所以应用安全是非常重要的安全管理工作。该层次部署应用安全防护管理系统，对所有应用安全攻击进行防护、审计、预警。

③ 数据安全防护层：该层次是针对数据安全进行防护的层次。数据安全是银行信息系统重要保障目标，所以该层也是CZ银行重点关注的层次。该层次通过部署数据库防火墙、数据库审计、运维风险管理系统等对数据进行集中审计，提升攻击防御、预警能力。

CZ银行云计算数据中心集群可以为线上应用系统提供全方位稳定、防护体系，以提升整体安全防护水平。小微贷款系统部署于该云数据中心，通过共享现有网络安全架构体系，提升系统的安全性及资源弹性拓展。

④ 小微贷款系统功能架构

小微贷款系统总体包含前端业务和后台业务两部分组成，前端业务即面向公众用户，主要受众为申请小微贷款的客户群体，表现形式为网站、安卓应用、IOS应用；后台业务为银行内部进行业务管理的后台侧流程，表现形式为网站。其功能架构示意图如下图所示：

图2-2 CZ银行小微贷款系统功能架构示意图

综上图所示，小微贷款前台业务涵盖用户管理、贷款管理、还款管理等六个功能模块组成，后台业务由贷款管理、客户管理、报表管理、系统设置等六个功能模块组成。该系统部署于CZ银行云计算平台，开发语言为JAVA，关系型数据库管理系统为MySQL，同时该系统通过Hadoop云集群对用户信息、贷款信息进行大数据分析统计，形成贷款风险数据。

2.2 小微贷款系统信息安全风险管理问题

CZ银行信息安全管理经历了10余年积淀，已经实现了从信息安全事件频发到偶发、被动接受信息安全审计到主动建立安全合规体系的跨越，信息安全风险管理效果显著。但小微贷款系统作为新兴金融科技业务系统，将面临复杂的信息安全挑战，且信息安全风险具有不确定性，管理工作仍存在如下问题亟待解决：

(1) 信息安全风险管理水平与银行业务发展规模不匹配

CZ 银行通过十余年持续发展，已经在金融体量、业务种类、行业影响力方面有了长足的发展，且发展趋势向好。2020 年财报显示，银行全年总营收 477.03 亿元，总资产 2.05 万亿元，同比商业银行处于中等偏上水平。信息安全风险管理是一个系统性工作，具有战略性的，需要全局考虑。CZ 银行在信息安全风险管理工作中着眼于技术工作落地，但未将相关规划落实于组织战略管理与规划中，未实现信息安全整体规划，依旧遵循着“头痛医头，脚痛医脚”的落后模式，在 2020 年全年通过外部网络安全审计团队发现小微贷款系统的高风险网络安全漏洞 12 个，管理体系和水平亟待提升以匹配业务的快速发展。

(2) 信息安全风险管理与金融科技投入不匹配

随着金融技术的持续发展，CZ 银行已经提出拥抱 Bank4.0 金融科技，持续在金融技术方面加大投入。根据公开信息，CZ银行2020年科技投入将达到全行营收的3.17%，达到在同行业中处于中等偏上水平，小微贷款系统也是在该预算下同比例投入。同时，CZ银行信息安全风险管理的投入占金融科技总投入的2.31%，在同行业中处于较低水平，远低于全球平均水平的 3.74%。对比来看，美国白宫发布的 2021 年政府预算显示，网络安全投入占IT预算20.4%，这个数字是CZ银行当前安全投入的8.8倍。当前针对信息安全风险管理相关的投入存在明显的不足，主要表现在信息安全人员不足、风险管理专项资金不到位等问题，导致信息安全风险方面投入不到位、新的风险管理技术引入不足等问

题。

表2-2 2020年主要上市银行披露的信息科技投入情况

序号	银行名称	信息科技投入金额	信息科技投入占总营收比
1	工商银行	238.19亿元	2.70%
2	建设银行	221.09亿元	2.93%
3	农业银行	183.00亿元	2.78%
4	中国银行	167.07亿元	2.49%
5	招商银行	119.12亿元	4.45%
6	中信银行	69.26亿元	3.56%
7	浦发银行	57.15亿元	2.91%
8	光大银行	51.5亿元	3.61%
9	CZ银行	15.22亿元	3.17%

(3) 信息安全风险管理制度与发展趋势不匹配

根据自身发展及合规需求，CZ银行信息安全管理部建立了大量信息安全管理制度，但没有形成体系性的信息安全管理。当前的管理制度文档可以快速应用到日常安全管理工作中，但是应对安全战略、安全纲领性工作时存在明显短板。在2020年外部网络安全审计中发现高风险管理缺陷14个，其中涉及管理制度9条，占比64%，亟待提升管理制度体系。

综上CZ银行小微贷款系统信息安全风险管理问题，已经对其日常的安全管理工作造成了如下偶发性安全问题，对CZ银行造成了一定的直接和间接损失：

(1) 恶意程序感染，造成系统负载加剧，业务停摆；

(2) 安全设备巡检不及时，安全防护策略更新不及时，防病毒软件过期；

(3) 运维账号共享使用，不能对安全运维管理过程进行充分审计；

(4) 应用系统安全测试不及时，整改修复工作迟滞。

2.3 信息安全风险评估指标识别原则

信息安全风险评估指标体系的建立是CZ银行小微贷款系统信息安全风险评估的关键环节，直接影响风险评估的要素与结果，因此指标体系的建立需要符合如下原则：

(1) 系统性原则

信息安全风险具有不确定性、随机性，且随着信息技术的高速发展，信息安全风险越发复杂多样，因此针对小微贷款系统的风险评估指标建立，需要从整体网络、信息、管理角度入手，全面开展风险指标确立。对风险指标的挖掘需明确按层次结构进行，梳

理清晰相互关联关系，突出核心要素与次要要素，均衡考虑各指标的内在联系，以保证评价的全面性与准确性。

(2) 科学性原则

信息安全风险是复合型学科的综合，不仅包含信息安全技术，同时涵盖了管理学、心理学等，因此对商业银行信息系统的信息安全风险评估需以完善的科学理论为基础，结合信息安全专家实践经验，对风险指标进行科学概括与量化分析。在指标建立过程中，需采用科学的评估方法，结合定性与定量结合分析法，对信息安全风险进行识别与量化评估，以保证指标的准确性与可信度。

(3) 独立性原则

信息安全风险指标在挖掘与比较打分过程中，为保证判断矩阵数据的科学性，在专家评估过程需符合独立性原则，以提升判断结果的准确度。专家判断环节中相互不产生干扰，以最终结果平均值方式对相关结果进行整理，通过独立性评判，获得各指标的科学性结果，以提升指标评价体系的准确性。

(4) 可实践性原则

信息安全风险指标的建立，需要具备可实践性原则，结果简明扼要，针对性强，能够在商业银行信息系统信息安全风险评价中具备良好的操作性，可以普遍适用于大部分评估场景，具备实践意义和广泛应用性。

2.4 信息安全风险识别与指标体系建立

信息安全风险评估指标的确立是评价指标体系建立的第一步，指标体系的质量直接影响权重乃至风险评估结果。本文通过根据信息安全风险管理相关标准、规范、规定，参考多份商业银行信息系统与信息安全风险相关文件，结合CZ银行小微贷款系统风险管理现状，形成如下影响CZ银行小微贷款系统的主要指标因素：

(1) 机房环境安全：机房温度、湿度、电力等物理环境为 CZ 银行小微贷款系统的稳定运行提供基础的物理环境保障，其稳定性直接从物理层面影响系统的安全稳定运行。同时物理环境具备的门禁、楼宇控制、地理位置等均不同程度影响信息系统的安全指标，对风险管理有一定的影响。

(2) 设备安全：小微贷款系统的稳定运行离不开物理设备的稳定运行支撑，包括网络设备、安全设备、电力设备、容灾设备、加解密设备等，相关设备为商业银行信息系统

提供稳定的运算、运行、存储、网络等基础支撑，是系统运行的关键基础设备，直接影响信息系统的稳定运行。

(3) 通信线路安全：CZ银行小微贷款系统需要网络数据交换，因此通信线路的安全性直接影响着信息系统的安全性。一旦通信线路被破坏、窃听、干扰，直接影响着通信数据的可用性、机密性和完整性，对信息系统的信息安全造成严重的安全威胁。

(4) 认证与鉴权：小微贷款系统的用户认证与权限管理是应用安全管理的重要环节，关乎系统数据与业务逻辑的安全性。一旦信息系统的认证与鉴权不完整，直接导致信息系统被非授权访问，造成严重的数据与业务甚至资金损失。

(5) 访问控制：访问控制能力是评价一个信息系统安全能力完整性的重要指标。一旦访问控制不严格，很容易造成信息系统机密性受到侵害，造成非授权数据、功能泄露，甚至数据与资金损失。

(6) 抗抵赖：CZ银行小微贷款系统面向储户、供应链、监管机构、内部柜台、管理层等多方，相关方面都需要对数据进行一定的数据、业务操作权限，因此数据的操作抗抵赖与审计能力是小微贷款系统的重要安全指标。一旦抗抵赖能力失效，极易造成银行业务与数据操作记录混乱，甚至造成银行业务系统的未授权交易，具有严重的信息与业务风险。

(7) 系统容灾备份：金融系统数据需要具备严密的容灾机制，以防止未预期的事件对数据、业务影响。容灾备份的结果直接影响小微贷款系统的数据保全与业务可用性，在不完备的容灾备份机制下，商业银行信息系统在遭受网络攻击、电力中断、极端自然灾害等情况下极易造成严重的数据与业务损失。

(8) 恶意软件防护：恶意软件是指病毒、木马等恶意程序，其是小微贷款的操作系统和应用软件的主要危害来源。当下恶意蠕虫病毒、挖矿木马、勒索病毒、僵尸网络、远程控制木马等恶意程序对小微贷款系统造成了严重的威胁，一旦感染这些恶意程序，极易对商业银行信息系统造成严重的信息、资金影响。

(9) 网络攻击防护：网络层面的攻击直接影响小微系统的业务稳定性与业务安全。当下 DDoS 分布式拒绝服务攻击、高级持续性攻击、数据窃取攻击事件层出不穷，这些都直指商业银行内部的用户敏感数据信息与资金，一旦攻击成功，可能造成严重的用户敏感数据泄露，甚至资金损失。

(10) 人力资源管理：对小微贷款系统的管理离不开人员管理，包括管理层人员、技术人员、外包人员、供应商人员等管理都对信息系统安全产生至关重要的影响。一旦人力资源管理缺失，极易造成严重的职权滥用、泄密、舞弊等人力管理方面问题，直接造成系统中运行的业务系统产生严重的数据与业务影响。

(11) 信息系统安全制度：小微贷款系统的稳定运行离不开人力的支撑，同时也离不开安全管理流程与制度的控制。信息安全保障体系中素有“三分技术，七分管理”之说，因此在商业银行信息系统的管理过程中，信息安全的制度与流程是信息安全的重要保障措施。如果流程管理不健全，极易造成误操作、管理控制缺失等信息安全隐患。

为保证信息安全风险评估指标的系统性、科学性和可实践性，笔者通过德尔菲法方式，参照附录一 CZ 银行小微贷款系统信息安全风险指标因素调查提纲，对 12 位信息安全方面专家就小微贷款系统的信息安全风险评估指标准则层与指标层的确定进行了讨论分析。这12名专家包含信息安全行业专家、CZ银行信息系统安全管理专家、银行业信息安全研究员组成，其中正高职称4名、副高职称6名、中级职称2名，所有专家均为本科及以上学历。专家清单如表2-3所示。

表 2-3 CZ 银行小微贷款系统风险指标评价专家清单

序号	姓名	年龄	工作年限	职称	最高学历	工作领域
1	卓华	38	17	副高	硕士	信息安全
2	韩文俊	53	29	正高	本科	信息安全
3	王允	45	22	正高	硕士	信息安全
4	林伟民	36	14	副高	硕士	网络安全
5	周敏慧	41	18	副高	本科	信息安全
6	简波	43	19	正高	硕士	信息安全
7	吴明	29	6	中级	硕士	信息安全
8	贾兰娟	35	13	正高	硕士	信息安全
9	李亮	34	12	副高	硕士	信息安全
10	申佳	30	7	中级	硕士	数据安全
11	贾鹏飞	33	11	副高	硕士	信息安全
12	戴伟	37	13	副高	硕士	信息安全

各位专家参照附录一问题清单结合理论积淀与实践经验，在深入了解CZ银行小微贷款信息系统信息安全风险特性基础上，对如上获得信息安全风险评估指标进行了分析与评判，结果共确认8条风险指标优化意见，其中包括增加风险指标4项，整合分类4项，形成CZ银行信息安全风险指标层次结构，建立了风险评估的指标基础。信息安全风险指

标调整与优化结果如下表2-4所示：

表2-4 专家判断信息安全风险指标反馈表

序号	专家意见	意见说明	指标调整
1	“抗抵赖”指标增加“安全审计”要求	“抗抵赖”具备完整的防护功能力，但CZ银行小微贷款较其他系统需要具备完备的审计能力，对抵赖行为发生过程的成功和失败行为进行必要的审计措施，提升信息系统应对审计的能力	对“抗抵赖”调整为“抗抵赖与审计”
2	增加“数据加密”指标	商业银行数据关乎民计民生，因此数据的机密性要求相较其他行业更高。CZ银行小微贷款系统中的储户信息、信用信息、资金信息、行业数据等均具备高敏感性要求，需要高强度数据加密要求。如果敏感数据未经加密直接泄露极易造成明文数据泄露风险，对商业银行非常大。	增加“数据加密”指标
3	增加“存储介质安全”指标	商业银行的数据交换离不开数据的存储，数据落地的存储介质的安全性对信息安全有着至关重要的影响。存储介质一旦存在不稳定、抗干扰能力弱，会导致严重的数据丢失、数据泄露等风险，对系统的数据安全造成严重的危害。	增加“存储介质安全”指标
4	增加“信息安全培训”指标	信息安全培训是对信息系统技术人员、使用人员的安全技术、安全意识培训，普及安全开发、安全运维、网络安全、数据安全、防病毒木马等安全技能培训，提升商业银行相关工作人员安全水平和意识，提升风险应对能力。	增加“信息安全培训”指标
5	增加“物理安全”准则	将“机房环境安全”、“设备安全”、“通信线路安全”、“存储介质安全”归类为“物理安全”准则	增加“物理安全”准则，并归并相关方案指标
6	增加“数据安全”准则	将“认证与鉴权”、“访问控制”、“抗抵赖与审计”、“数据加密”归类为“数据安全”准则	增加“数据安全”准则，并归并相关方案指标
7	增加“运行安全”准则	将“系统容灾备份”、“恶意软件防护”、“网络攻击防护”、“安全监测”归类为“运行安全”准则	增加“运行安全”准则，并归并相关方案指标
8	增加“安全管理”准则	将“人力资源管理”、“系统开发管理”、“信息安全培训”归类为“安全管理”准则	增加“安全管理”准则，并归并相关方案指标

在充分考虑专家意见后，经过整理、汇总，初步获得CZ银行小微贷款系统信息安全风险评估指标体系。CZ银行小微贷款的信息安全风险评估主要可以分为物理安全（A1）、数据安全（A2）、运行安全（A3）、管理安全（A4），其中物理安全（A1）包含机房环境安全（B1）、设备安全（B2）、通信线路安全（B3）、存储介质安全（B4），数据安全（A2）包含认证与鉴权（B5）、访问控制（B6）、数据加密（B7）、抗抵赖与审计（B8），运行安全（A3）包含系统容灾备份（B9）、恶意软件防护（B10）、网络攻击防护（B11），管理安全（A4）包含人力资源管理（B12）、信息安全制度（B13）、信息安全培训（B14）。通过对相关指标进行编号，形成CZ银行小微贷款系统信息安全风险评估指标体系，结果

如下表2-5所示

表2-5 CZ银行小微贷款系统的信息安全风险评价指标体系模型

目标层	准则层	方案层
CZ银行小微贷款系统信息安全（Z）	物理安全（A1）	机房环境安全（B1）
		设备安全（B2）
		通信线路安全（B3）
		存储介质安全（B4）
	数据安全（A2）	认证与鉴权（B5）
		访问控制（B6）
		数据加密（B7）
		抗抵赖与审计（B8）
	运行安全（A3）	系统容灾备份（B9）
		恶意软件防护（B10）
		网络攻击防护（B11）
	管理安全（A4）	人力资源管理（B12）
		信息安全制度（B13）
		信息安全培训（B14）

2.5 本章小结

本章对CZ银行小微贷款系统进行了介绍，并对其信息科技现状进行了描述，介绍了CZ银行信息小微贷款信息系统的科技团队组织架构、信息系统网络架构以及核心信息系统情况，最后对当前CZ银行小微贷款系统当前存在的信息安全风险管理问题进行梳理，识别了管理理念落后、管理人员不足、管理体系化不到位的问题，同时采用文献分析与德尔菲法对小微贷款系统的信息安全风险指标进行了识别，建立了针对性信息安全指标体系，为进一步风险评估提供了基本要素。

3 信息安全风险评估方法选择

3.1 CZ 银行小微贷款系统信息安全风险特性

CZ 银行信息系统众多，涉及多个业务层次，由多个不同子系统组成，各子系统可以独立运转，也可进行系统间业务交互，因此小微贷款系统的信息安全风险因素、风险影响、触发条件等均复杂关联，因此其信息安全风险特性具有因素众多、动态性、事件危害大等。

(1)信息安全风险因素众多。CZ 银行业务是高度信息化的，相关业务系统均实现了高度的信息化、数字化、智能化。小微贷款系统建设的逐步深入，其复杂度也越来越高，且近年来随着 ICT 的迅速发展，诸多金融业务逐步与新兴信息技术深度融合，给信息系统的信息安全带来了更多、更复杂的风险因素。这些风险因素包括相关技术自身以及不同技术的契合过程，这都给 CZ 银行小微贷款系统的信息安全风险带来了极大的挑战。

(2) 信息安全风险具有动态性。CZ银行信息安全风险主要来源于技术与管理风险，而技术持续革新过程中会不断引入新的技术风险，管理过程中也会由于人为因素引发风险，这些风险导致了 CZ 银行信息小微贷款系统的安全风险具有动态性。信息安全技术在持续发展过程中也会发现新的风险，例如微软操作系统的漏洞会不断被挖掘出来，而不是一蹴而就可以完全发现。另一方面，CZ 银行信息安全建设方面起步相对较晚，在新技术、新业务探索上趋于前列，相关风险的动态性较明显。

(3) 信息安全风险一旦触发危害巨大。CZ银行是区域国计民生的重要支柱行业，其信息系统更是支撑金融业务的重要途径，一旦发生信息安全事件，直接影响系统的稳定运行，乃至银行业务的顺利开展。而信息安全事件的后果往往比较严重，轻则影响民众隐私信息保全，重则影响储户或银行的资金安全。近几年商业银行网络安全事件频发，对民众生活的影响也愈发明显。

综上，在选择对 CZ 银行小微贷款系统信息安全风险评估的方法时，需要有效识别其信息安全风险因素，充分考虑风险的动态性与不确定性，结合风险可能影响，建立一套科学、有效、具备实践性的评价体系。

3.2 CZ 银行小微贷款系统信息安全风险评估方法选择

3.2.1 典型信息安全风险评估方法

(1) 层次分析法（AHP）

层次分析法，是一种可以处理复杂问题的量化分析方法[61]。该方法建立在对系统充分分析的基础上，将复杂的因素联系分解为由局部简单关系构成的递阶关系，通过构造关系矩阵、权重向量和评级矩阵进行模糊综合评估的分析方法。该方法化繁为简，将定性分析结果进行量化，以便更好呈现各评估指标，便于风险控制决策。

层次分析法一般步骤如下:

首先，构建递阶层次指标结构。AHP 法的首要步骤就是识别影响评估目标的因素，并通过层次结构构建指标体系，以便于对层次结构进行量化权重分析。识别影响因素一般采用头脑风暴、德尔菲法等方法;

其次，建立两两比较矩阵。两两比较矩阵是量化计算的基础，通过对两个同级指标进行两两比较，评判影响级别并用 1、3、5、7、9 及其倒数方式表示相对重要程度，以此建立两两比较矩阵。

再次，层次单排序与一致性校验。计算当前层次两两判断矩阵的特征向量与最大特征值，并对一致性进行校验。

最后，层次总排序与一致性校验。计算所有层次的最大特征值与特征向量，并对一致性进行校验。

利用层次分析法可以自顶向下构建层次结构指标体系，并通过计算识别各指标对评估目标的影响因素比重，直观获得指标结果权重，以提升对风险指标的定性与定量评价。

(2) 模糊综合评价法（FCE）

模糊综合评价法是根据模糊数据的隶属度理论把定性的评价结果转化为定量结果的方法。通过构造风险指标集合和评价指标集，通过专家评判各风险指标的水平等级，定义隶属函数来建立权重矩阵和关联模糊矩阵，并把权重矩阵和关联模糊矩阵的积作为评价结果[62]。该方法可以量化不确定性风险指标，能够很好地解决不确定性指标的量化问题。

(3) 基于贝叶斯网络

该方法以贝叶斯网络为模型，对影响指标的各要素通过专家评判的概率方式进行描

述，并形成评价结果[63]。该方法适用不确定性信息的评价问题，高度依赖专家水平，复杂网络中使用会计算过程复杂。

(4) 故障树法（FTA）

故障树分析法（FTA）是通过逻辑因果关系形成倒立的树形分析方法，下层是上层的“因”，上层是下层的“果”，以此形成不同事件的因果逻辑关系。该方法逻辑性强，可以快速形成不同事件间的因果逻辑，也可以快速针对某一特定的事件进行原因分析[64]。但是在信息安全风险识别过程中采用故障树法由于受因素规模和专家水平，较容易造成风险因素遗落。

(5) 风险矩阵法

风险矩阵法是通过将风险发生的可能性与风险引发危害通过二维坐标矩阵表示，形成行、列交叉的风险矩阵，根据风险评价结果直接对照风险矩阵即可获得相应的风险评价结果。该方法简便易用，应用广泛。

3.2.2 信息安全风险评估方法选择

本文对典型的信息安全风险评价方法进行了简要对比分析，明确相关方法的适用情况、优点、缺点，以便选择适合商业银行信息安全风险评价的方法，不同风险评价方法对比详见表 3-1。

表 3-1 信息安全风险评价方法对比表

风险识别方法	适用情况	优点	缺点
风险矩阵法	适用于评价结果匹配，与其他方法配合使用	同时考虑风险发生可能性与风险危害双重指标	依赖专家经验，误差较大
层次分析法	适用于处理风险指标层次清晰，量不大	可以将复杂的结果量化为层次性结果	评价者经验水平要求较高
模糊综合评价法	适用于处理难以量化的风险指标	模糊化量化不便确定指标	复杂度高
基于贝叶斯网络	适用于轻量级风险指标评估，评估不确定因素	可以处理不确定性因素，总体和局部要素均可评估	复杂度高，高度需求专家水平
故障树法	适用于风险因素较少，项目体量小、专家经验丰富的项目	快速分析相关事件逻辑关系，明确风险点	复杂项目容易遗落风险点

由上表可知，贝叶斯网络法可以处理不确定性因素，可以全局评估信息安全风险因素，但实施复杂度高，需要操作人员非常高专业水平；风险矩阵法同时考虑风险发生可能性与危害，可以更好地识别风险指标，但实施结果误差大；故障树法适用于风险指标少的目标，且各指标间逻辑清晰，复杂项目由于逻辑关系错综复杂且技能要求水平高，

不适合作为信息安全风险评估过程中使用。层次分析法逻辑清晰，可以将复杂的指标层次化，逻辑性强，适用性广，计算结果相对误差小，可以方便在信息安全风险评估过程中对各风险指标进行量化分析。模糊综合评价法适用于处理难以量化的风险指标场景中，并对模糊指标进行量化评估，虽然实施复杂度高，但评价结果准确，可信度高。

商业银行信息系统的信息安全风险指标数量不确定，如果采用贝叶斯网络评价方法一旦风险指标量太大直接导致计算过程非常复杂。而其风险指标层次结构清晰，使用层次分析法可以快速实现相互关联风险指标的量化分析，将众多风险因素进行逻辑分层，确定各风险指标的权重。风险评价模型建立过程中一方面权衡专家水平与复杂度，选择模糊综合评价法对各风险指标进行风险评价，评判风险等级，提升不确定性风险评价效果，有效解决模糊性和不确定性问题。层次分析法和模糊综合评价法都可以独立作为商业银行信息安全风险评估方法，但在独立使用中都具有一定的缺陷，不能更科学获得评估结果。层次分析法实现了风险指标的层次逻辑，能够获得各指标的权重，但无法针对相关指标进行深入分析。模糊综合分析法可以针对各风险指标要素进行深入分析，但无法获得指标权重。因此只有两者结合充分发挥各自优势，弥补不足，提升信息安全风险评估的科学性与准确性。

综上所述，本文通过采用 AHP-FCE 方法来对 CZ 银行小微贷款系统信息安全风险评估，通过构建商业银行信息系统信息安全风险指标体系，得出各指标权重，并采用模糊综合评价法对主要风险因素进行模糊量化评价分析，以明确风险控制针对性措施，提升风险管理效果。

3.3 基于 AHP-FCE 的信息安全风险评估模型构建

通过前文对信息安全风险评估方法的选取，本文采用层次分析法 AHP 与模糊综合评价法结合的方式构建商业银行信息系统的信息安全风险评估模型。步骤主要为构建 AHP 模型，形成风险指标权重，并结合模糊综合评价，对风险要素进行风险比重计算，形成风险结果评价。模型示意图如下图 3-1 所示：

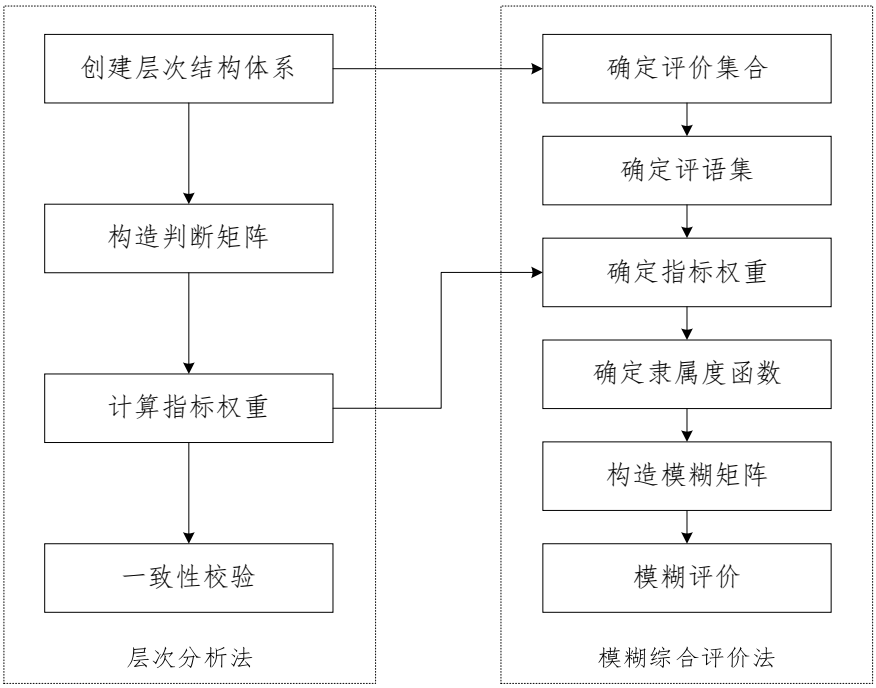

图 3-1 基于 AHP-FCE 信息安全风险评估模型示意图

3.3.1 层次分析法（AHP）

层次分析法（Analytical Hierarchy Process），是一种可以处理复杂问题的量化分析方法。该方法建立在对系统充分分析的基础上，将复杂的因素联系分解为由局部简单关系构成的递阶层次关系，通过构造关系矩阵、权重向量和评级矩阵进行模糊综合评估的分析方法。在商业银行信息系统的信息安全风险评估中，通过 AHP 方法结合专家判断，可以快速获得各风险指标的权重，将复杂的因素关系层次化，并对定性结果进行定量计算，提升风险评估指标的客观性。AHP 方法主要有四个过程：构造递阶层次结构、建立两两比较矩阵、单排序与校验、层次总排序与校验。

(1) 构造递阶层次结构

AHP 方法开展前，需要对信息安全风险评估目标进行分解，构建递阶层次关系，一般最上层是我们要解决问题的目标，即目标层，中间层为一级分类层，即准则层，最底层为方案层，层与层之间有关联关系，形成层次、递阶结构模型，如图 3-2 所示。

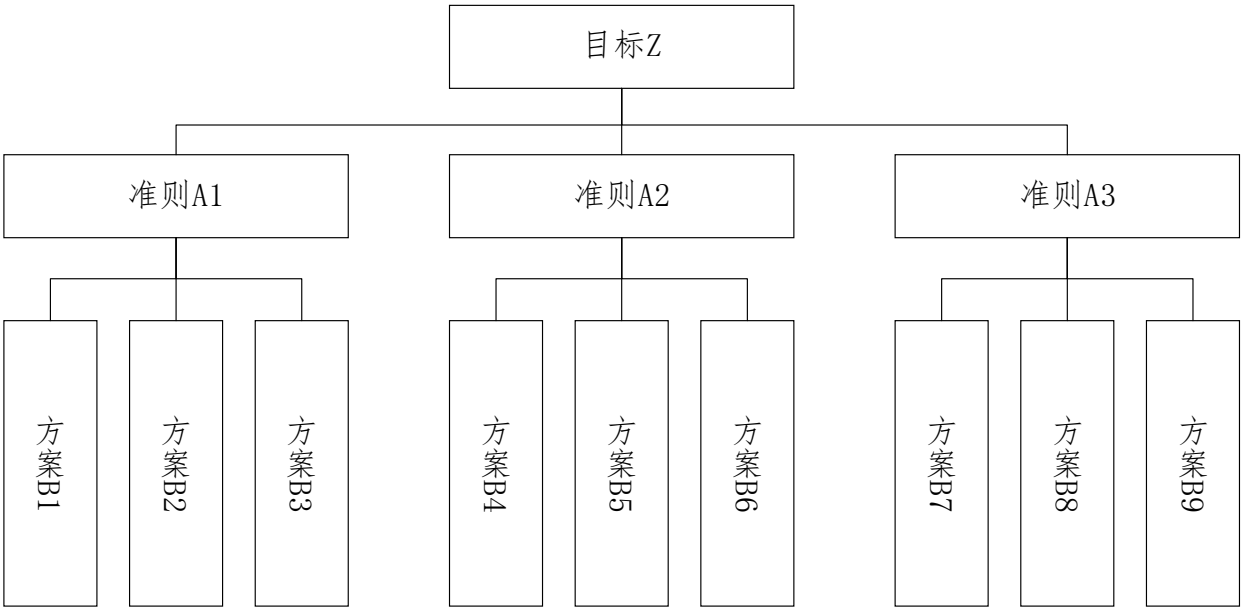

图 3-2 AHP 层次递阶结构模型示意图

(2) 建立两两比较矩阵

判断矩阵表示当前层各要素对上层的影响程度的相对关系，例如方案层$B_1, B_2, B_3, .., B_n$与对应的上层准则层A_m有层次关系，对方案进行两两比较，明确相对重要性，建立该方案的判断矩阵 A 如下：

$$A_m = (b_{ij})_{n\times n} = \begin{bmatrix} b_{11} & b_{12} & \cdots & b_{1n} \\ b_{21} & b_{22} & \cdots & b_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ b_{n1} & b_{n2} & \cdots & b_{nn} \end{bmatrix} (m = 1,2,\ldots,n) \qquad (3-1)$$

式中a_{ij}表示第i个指标相对第j个指标的相对重要程度。

一般针对单一准则来说，2 个方案进行两两比较，总能识别出相对重要性关系。层次分析法采用 1~9 标度法，对不同方案进行数量化标度，形成量化判断矩阵，标度说明如下表所示。

表 3-2 AHP 判断矩阵标度基准表

标度值	标度定义	标度说明
1	重要性相同	B_i与B_j同等重要，$b_{ij}=1$，$b_{ji}=1$
3	稍微重要	B_i比B_j稍微重要，$b_{ij}=3$，$b_{ji}=1/3$
5	明显重要	B_i比B_j明显重要，$b_{ij}=5$，$b_{ji}=1/5$
7	非常重要	B_i比B_j非常重要，$b_{ij}=7$，$b_{ji}=1/7$
9	绝对重要	B_i比B_j绝对重要，$b_{ij}=9$，$b_{ji}=1/9$

以上判断矩阵标度基准表中，如在两两指标评判中遇到中间状态取值，可以取值为 2、4、6、8，相应的对方取值为 1/2、1/4、1/6、1/8。

(3) 单排序与一致性校验

根据以上获得的判断矩阵，对矩阵相关风险因素进行权重计算。主要过程如下：

①对矩阵进行归一化：

$$\bar{A}_{ij} = \frac{b_{ij}}{\sum_{k=1}^{n} b_{kj}} \ (i, j, \dots, n) \tag{3-2}$$

式中n为判断矩阵阶数。

②判断矩阵A求和：

$$\bar{W}_i = \sum_{j=1}^{n} \bar{A}_{ij} \ (i = 1,2, \dots, n) \tag{3-3}$$

③$\bar{W}_i$归一化处理：

$$W_i = \frac{\bar{W}_i}{\sum_{i=1}^{n} \bar{W}_i} \ (i = 1,2, \dots, n) \tag{3-4}$$

④最大特征值计算：

$$\lambda_{max} = \sum_{i=1}^{n} \frac{(AW)_i}{nW_i} \ (i = 1,2, \dots, n) \tag{3-5}$$

式中$W = (W_1, W_2, \dots, W_n)^T$，又称判断矩阵的特征向量，$\lambda_{max}$是表示判断矩阵的最大特征根。

⑤计算一致性指标：

$$CI = \frac{\lambda_{max} - n}{n - 1} \tag{3-6}$$

⑥对照RI，计算CR一致性比率：

$$CR = \frac{CI}{RI} \tag{3-7}$$

Saaty 在 AHP 评估方法过程中引入随机一致性指标RI，解决多阶判断矩阵偏离问题，根据判断矩阵阶数n，参照下表获取RI的值。

表 3-3 随机一致性指标基准表

$\boldsymbol{n}$	1	2	3	4	5	6	7	8	9	10
$\boldsymbol{RI}$	0	0	0.58	0.90	1.12	1.24	1.32	1.41	1.45	1.49

⑦一致性校验判断：

根据上式获得的一致性比率CR，根据如下原则进行判断：

$CR < 0.10$：判断矩阵具有一致性；

$CR \geq 0.10$：判断矩阵不具备一致性，偏离较大需要修正；

(4) 层次总排序与一致性校验

根据如上计算已经获得某一层次单排序的结果，利用同一层次所有排序结果就可以计算出当前层所有因素的权重结果，这个过程就是层次总排序。层次总排序的计算过程要从上向下地将单排序结果进行计算得出。假设 A 层为 B 的上一层，A 的m个因素层次总排序为$a_1, a_2, \dots, a_m$，B 层中相对于A_k的层次单排序为$b_{1k}, b_{2k}, \dots, b_{nk}$（当$B_i$与$A_k$无关系时，$b_{ik} = 0$）包含主要计算过程如下:

①第 B 层的各因素相对总目标排序向量：

$$b_i = \sum_{k=1}^{m} b_{ik} a_k \ (i = 1,2, \dots, n) \tag{3-8}$$

②计算层次总排序的一致性比率并判断：

$$CR = \frac{\sum_{k=1}^{m} CI_k a_k}{\sum_{k=1}^{m} RI_k a_k} \tag{3-9}$$

式中RI_k表示 B 层中与A_k相关因素单排序平均随机一致性指标，CI_k表示相应的单排序一致性指标。对总排序的一致性校验同样通过CR与 0.1 的比较获得，$CR < 0.1$认为一致性校验通过，结果可接受。

综上，通过以上计算过程，可以获得商业银行信息系统信息安全风险要素指标权重，并通过一致性校验可以判断评估过程一致性，提升评估科学性。

3.3.2 模糊综合评价法（FCE）

通过前序章节采用层次分析法 AHP 已经获得影响商业银行信息系统的信息安全风险指标与相关权重，需要进一步对相关指标因素进行量化评价，而 FCE 法在处理模糊定性信息时效果非常具有优势。模糊综合评价是根据模糊数据的隶属度理论把定性的评价结果转化为定量结果的方法，通过构造风险指标集合和评价指标集，结合专家评判各风险指标的水平等级，定义隶属函数来建立权重模糊矩阵和关系模糊矩阵，并把权重模糊矩阵和关联模糊矩阵的积作为评价结果。该方法可以量化不确定性风险指标，能够很好地解决模糊指标的量化问题。模糊综合评价法基本步骤如下：

(1) 确定评价因素集与权重集

模糊综合评价的第一步是确定评价因素集，即明确评价目标的组成集合。此处评价集合由层次分析法过程中的指标因素组成，记为集合U，相应的权值记为集合A，如下式：

$$U = \{u_1, u_2, \dots, u_n\} \tag{3-10}$$

$$A = \{a_1, a_2, \dots, a_n\} \tag{3-11}$$

式中n为指标因素个数。

(2) 建立评价因素的评语集

根据评价因素集的实际情况，将评价区分为若干级别，方便对相关因素进行模糊化评价，例如信息安全风险因素评价级别可以定义为“非常安全”、“安全”，“一般”，“危险”，“非常危险”，记作集合V，如下式：

$$V = \{v_1, v_2, \dots, v_p\} \tag{3-12}$$

式中p为评语集个数。

(3) 建立综合评价矩阵

评价过程需要对定性结果进行模糊评价，一般采用专家打分方式对相关指标进行评价，并对结果进行整理形成隶属度向量$r_i = \{r_{i1}, r_{i2}, \dots, r_{ip}\}$，其中$r_{ip} = V_{ip}/k$，$k$为实际评价结果总人数。则因素集$U_i$的隶属度矩阵如下：

$$R_i = \begin{bmatrix} r_{i1} \\ r_{i2} \\ \vdots \\ r_{ij} \end{bmatrix} = \begin{bmatrix} r_{i11} & r_{i12} & \dots & r_{i1p} \\ r_{i21} & r_{i22} & \dots & r_{i2p} \\ \vdots & \vdots & \ddots & \vdots \\ r_{ij1} & r_{ij2} & \dots & r_{ijp} \end{bmatrix} (i = 1,2, \dots, n) \tag{3-13}$$

式中，j为子集因素个数，p为评语集个数。

(4) 进行模糊综合评价

一级模糊综合评价：

$$\begin{aligned} B_i = A_i \circ R_i &= (a_{i1}, a_{i2}, \dots, a_{ij}) \circ \begin{bmatrix} r_{i11} & r_{i12} & \dots & r_{i1p} \\ r_{i21} & r_{i22} & \dots & r_{i2p} \\ \vdots & \vdots & \ddots & \vdots \\ r_{ij1} & r_{ij2} & \dots & r_{ijp} \end{bmatrix} \\ &= (b_{i1}, b_{i2}, \dots, b_{ij}) \end{aligned} \tag{3-14}$$

模糊综合评价计算过程一般有主因素决定型$\Delta = (\wedge, \vee)$，主因素突出型$\Delta = (\cdot, \vee)$，加权平均$\Delta = (\cdot, +)$，广义加权平均$\Delta = (\cdot, \oplus)$，考虑商业银行信息系统信息安全风险之间有一定的关联性，需要对相互程度进行兼顾，因此本文采用广义加权平均方法。

二级模糊综合评价：

$$B = A \circ R = A \circ \begin{bmatrix} B_1 \\ B_2 \\ \vdots \\ B_n \end{bmatrix} = (b_1, b_2, \ldots, b_n) \qquad (3-15)$$

3.4 信息安全风险评估模型可行性分析

CZ 银行小微贷款系统的信息安全风险具有不确定性、动态性，且指标因素众多，需要对相关指标采用科学的方法对因素进行识别，并通过科学有效的计算方法对定性结果进行定量权重计算。而层次分析法正式应对复杂且有逻辑层次关系的指标进行层次递阶排布，并通过专家打分方式对定性结果量化，进一步对结果进行计算后获得各层次相关指标的单权重和综合权重，具有科学性、可操作性。而模糊综合评估法在应对模糊、定性的风险级别有非常好的适用性，可以对原本难以量化的指标进行量化评价，提升综合评价的科学性。

层次分析法 AHP 与模糊综合评价 FCE 结合，可以充分利用层次分析法影响商业银行信息系统信息安全的要素进行全面量化分析，构建层次模型，同时生成权重结果以供模糊综合评价方法使用。而模糊综合评价法综合了多个专家意见，对模糊数据定量化评价，两者结合使用有效地解决了评价过程的模糊性和不确定性，为评估结果的科学性和合理性奠定了基础。

笔者通过查阅相关文献，AHP-FCE 模型应用于管理决策、方案比选、规划预测等领域均有成熟的应用，在相关领域均很好地实现对因素指标的识别、权重的判断、结果评估，因此两者结合方式势必可以应用与商业银行信息系统的信息安全风险评估领域，且具备良好的科学意义。

3.5 本章小结

本章通过对层次分析法、模糊综合评价法、基于贝叶斯网络、风险矩阵法、故障树法等评估方法的比选，结合 CZ 银行小微贷款系统信息安全风险的特性，确定了层次分析法（AHP）与模糊综合评价法（FCE）结合的风险评估方法。层次分析法（AHP）可以构建商业银行信息系统的信息安全风险指标层次结构，并对各指标权重进行确定，同时利用模糊综合评价法（FCE）对评估系统的指标进行定量化评价，有效解决了模糊性指标的定量化评估。最后对两者结合的可行性进行了分析说明，给出了合理的解释。

4 CZ银行小微贷款系统信息安全风险评估

4.1 信息安全风险评估指标权重确定

4.1.1 构造评估指标递阶层次结构

根据上述阐述，通过文献分析与专家判断确定了CZ银行小微贷款系统的信息安全风险指标体系模型，其中包括1个一级指标：CZ银行小微贷款系统信息安全（Z），4个二级指标：物理安全（A1）、数据安全（A2）、运行安全（A3）、管理安全（A4），14个三级指标：机房环境安全（B1）、设备安全（B2）、通信线路安全（B3）、存储介质安全（B4）、认证与鉴权（B5）、访问控制（B6）、数据加密（B7）、抗抵赖与审计（B8）、系统容灾备份（B9）、恶意软件防护（B10）、网络攻击防护（B11）、人力资源管理（B12）、信息安全制度（B13）、信息安全培训（B14），相关风险指标说明详见2.4章节。通过专家判断明确的递阶关系，形成如下层次体系图，如图4-1所示：

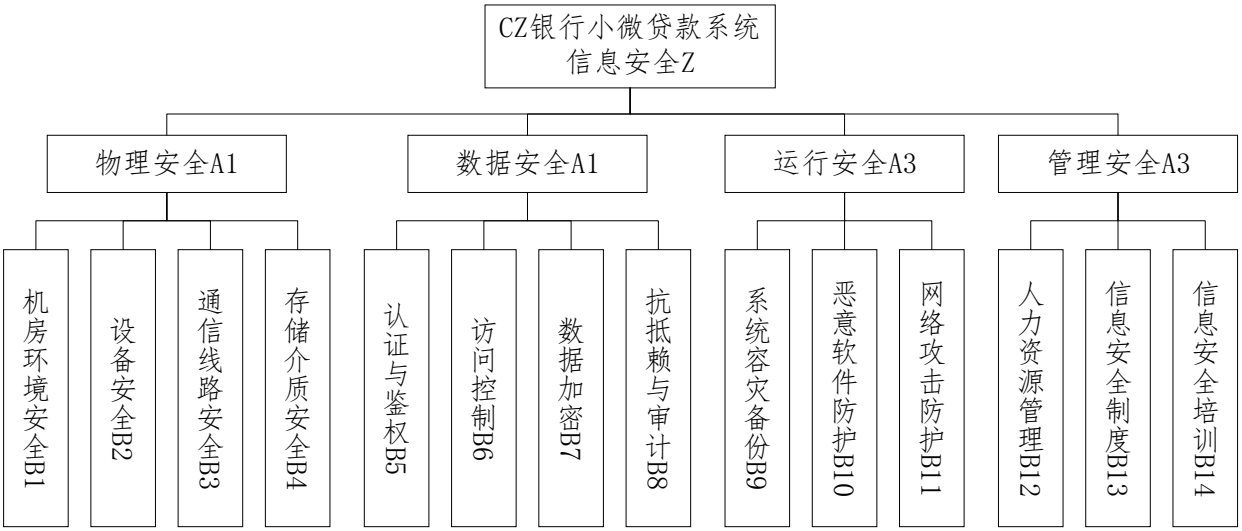

图4-1 CZ银行小微贷款系统信息安全风险评估指标层次体系图

4.1.2 构造两两比较矩阵及单排序与一致性校验

鉴于信息安全风险的动态性、复杂性、不可确定性，构造两两比较矩阵过程中，采取专家判断打分方式开展，以提升结果可信度。为保证信息安全风险评估指标的系统性、科学性和可实践性，同时兼顾节约时间与操作便捷性，笔者通过德尔菲法方式组织12位信息安全方面专家就两两矩阵打分进行现场讨论确定，打分表格提纲参见附录二CZ银行小微贷款系统信息安全风险指标权重调查表。专家信息简介如表2-3所示。

通过他们的理论积淀与实践经验对如上获得信息安全风险指标评价进行两两比较，遵从1、3、5、7、9不同的级别数字表示相对更危险，通过相应的倒数1、1/3、1/5、1/7、1/9表示相对更安全的原则，输出两两判断矩阵，并通过权重计算，分别得到如下表4-1、表4-2、表4-3、表4-4、表4-5。

表4-1 准测层判断矩阵与权重计算结果

信息安全（Z）	物理安全	数据安全	运行安全	管理安全	单层权重	组合权重
物理安全（A1）	1	1/4	1/3	1/7	0.0635	0.26
数据安全（A2）	4	1	2	1/3	0.2552	1.05
运行安全（A3）	3	1/2	1	1/2	0.1864	0.75
管理安全（A4）	7	3	2	1	0.4948	2.08

表4-2 方案层相对于A1的判断矩阵与权重计算结果

物理安全（A1）	机房环境安全	设备安全	通信线路安全	存储介质安全	单层权重	组合权重
机房环境安全（B1）	1	1/2	1/2	1/3	0.1209	0.4910
设备安全（B2）	2	1	1/2	1/2	0.1928	0.7778
通信线路安全（B3）	2	2	1	1/2	0.2695	1.1053
存储介质安全（B4）	3	2	2	1	0.4168	1.7041

表4-3 方案层相对于A2的判断矩阵与权重计算结果

数据安全（A2）	认证与鉴权	访问控制	数据加密	抗抵赖与审计	单层权重	组合权重
认证与鉴权（B5）	1	1/2	1/2	2	0.1981	0.8086
访问控制（B6）	2	1	1/2	2	0.2748	1.1442
数据加密（B7）	2	2	1	2	0.3873	1.6127
抗抵赖与审计（B8）	1/2	1/2	1/2	1	0.1397	0.5698

表4-4 方案层相对于A3的判断矩阵与权重计算结果

运行安全（A3）	系统容灾备份	恶意软件防护	网络攻击防护	单层权重	组合权重
系统容灾备份（B9）	1	7	5	0.7380	2.2370
恶意软件防护（B10）	1/7	1	1/2	0.0944	0.2837
网络攻击防护（B11）	1/5	2	1	0.1676	0.5041

表4-5 方案层相对于A4的判断矩阵与权重计算结果

管理安全（A4）	人力资源管理	信息安全制度	信息安全培训	单层权重	组合权重
人力资源管理（B12）	1	1/2	1/3	0.1593	0.4815
信息安全制度（B13）	2	1	1/3	0.2519	0.7667
信息安全培训（B14）	3	3	1	0.5889	1.8222

根据如上两两比较矩阵及权重结果，对各矩阵进行一致性比例计算，对单排序一致性结果进行校验，如下表4-6所示，以上5个两两比较矩阵$CR < 0.1$，一致性校验通过，结果有效。

表4-6 准测层判断矩阵与权重计算结果

判断矩阵	λ_{max}	CI	RI	CR	一致性校验结果
信息安全（Z）	4.1079	0.0360	0.90	0.0400	CR<0.1，通过一致性校验
物理安全（A1）	4.0712	0.0237	0.90	0.0264	CR<0.1，通过一致性校验
数据安全（A2）	4.1217	0.0406	0.90	0.0451	CR<0.1，通过一致性校验
运行安全（A3）	3.0142	0.0071	0.58	0.0122	CR<0.1，通过一致性校验
管理安全（A4）	3.0539	0.0270	0.58	0.0465	CR<0.1，通过一致性校验

4.1.3 层次总排序及一致性校验

根据如上单排序结果，通过对准则层与方案层权重整合计算，形成如下表4-7层次总排序权重汇总表，其中权重越高的风险因素指标相较权重低的对商业银行信息安全结果影响更大，而权重低说明其对风险危害等级影响更大。

表4-7 层次总排序汇总表

目标层	准则层	准则层权重	方案层	权重	综合权重	总排序
CZ银行小微贷款系统信息安全（Z）	物理安全（A1）	0.0635	机房环境安全（B1）	0.1209	0.0077	14
			设备安全（B2）	0.1928	0.0122	13
			通信线路安全（B3）	0.2695	0.0171	12
			存储介质安全（B4）	0.4168	0.0265	10
	数据安全（A2）	0.2552	认证与鉴权（B5）	0.1981	0.0506	7
			访问控制（B6）	0.2748	0.0701	6
			数据加密（B7）	0.3873	0.0989	4
			抗抵赖与审计（B8）	0.1397	0.0357	8
	运行安全（A3）	0.1864	系统容灾备份（B9）	0.7380	0.1376	2
			恶意软件防护（B10）	0.0944	0.0176	11
			网络攻击防护（B11）	0.1676	0.0312	9
	管理安全（A4）	0.4948	人力资源管理（B12）	0.1593	0.0788	5
			信息安全制度（B13）	0.2519	0.1246	3
			信息安全培训（B14）	0.5889	0.2914	1

通过公式(3-8)对层次总排序一致性比例进行计算，结果如下：

$$CR = \frac{\sum_{k=1}^{4} CI_k a_k}{\sum_{k=1}^{4} RI_k a_k} = 0.0389 \qquad (4-1)$$

从计算结果可以得出，$CR < 0.1$，一致性校验通过，结果有效。

4.1.4 信息安全风险指标与权重结果分析

根据以上风险指标的建立与权重分析，我们明确了对CZ银行小微贷款系统的信息安全风险主要影响因素有机房环境安全、设备安全、通信线路安全、存储介质安全、认证与鉴权、访问控制、数据加密、抗抵赖与审计、系统容灾备份、恶意软件防护、网络攻击防护、人力资源管理、信息安全制度、信息安全培训等，可以分别从物理、数据、运行、管理安全维度进行影响性判断，构建了层次体系模型。结合专家判断，利用层次分析法 AHP 对影响 CZ 银行小微贷款系统的信息安全风险因素进行分析，准则层相关风险因素对信息安全风险影响排序优先级依次为管理安全、数据安全、运行安全、物理安全，如下图 4-2 所示，相关顶点越靠近边缘说明安全风险越高，因此影响 CZ 银行小微贷款系统信息安全的相对主要因素为管理安全。商业银行的基础设施建设方面相对健全，对信息安全影响相对较弱，而管理体系、流程、制度与应用数据安全对信息安全的影响更明显，包括对误操作、人员管控、社会工程学攻击、容灾备份管理等相关内容。

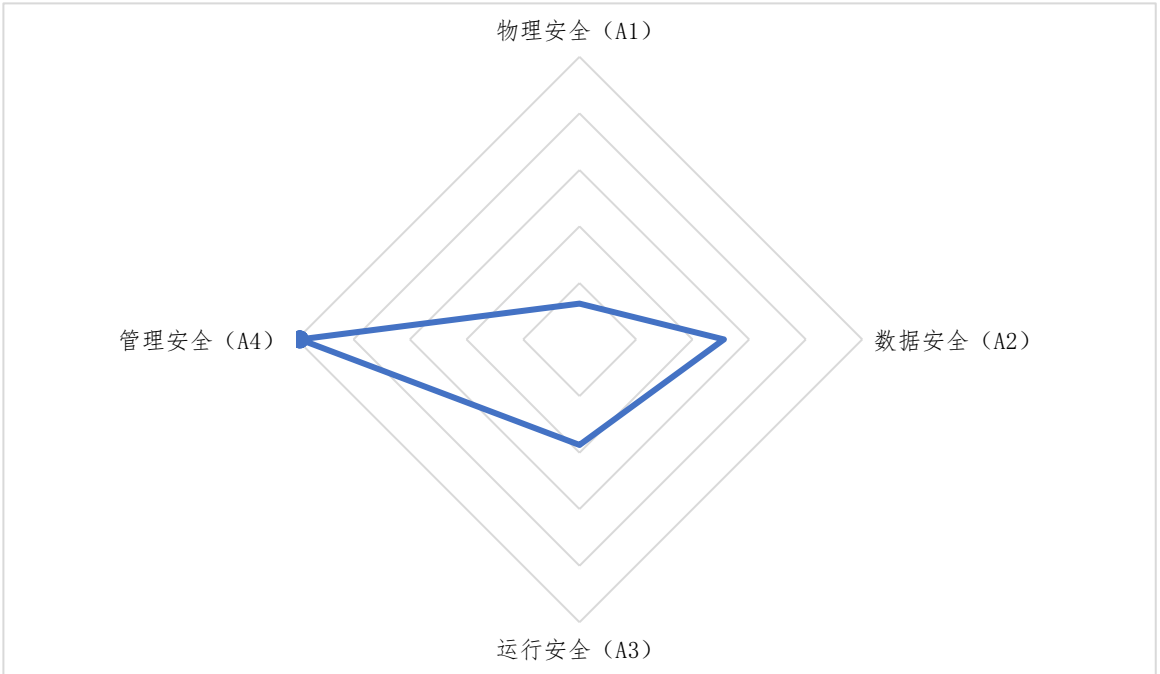

图 4-2 CZ银行小微贷款系统信息安全风险评估准则层指标权重分布图

信息安全风险评估指标体系构建过程中，方案层因素较多，因此采用中位数方式进

行筛选。通过计算，影响权重中位数为 0.0431，进一步排序，确定排在中位数以上的有信息安全培训、系统容灾备份、信息安全制度、数据加密、人力资源管理、访问控制、认证与鉴权，相关指标对信息安全风险影响权重较高；中位数以下依次为抗抵赖与审计、网络攻击防护、存储介质安全、恶意软件防护、通信线路安全、设备安全、机房环境安全，这些指标对信息安全风险影响权重较低，参见图 4-3。因此，初步分析 CZ 银行小微贷款系统的信息安全风险主要来源管理体系、数据与应用安全防护，需建立完善的信息安全风险管理体系，完善数据与应用安全访问控制策略，提升整体安全防护水平。

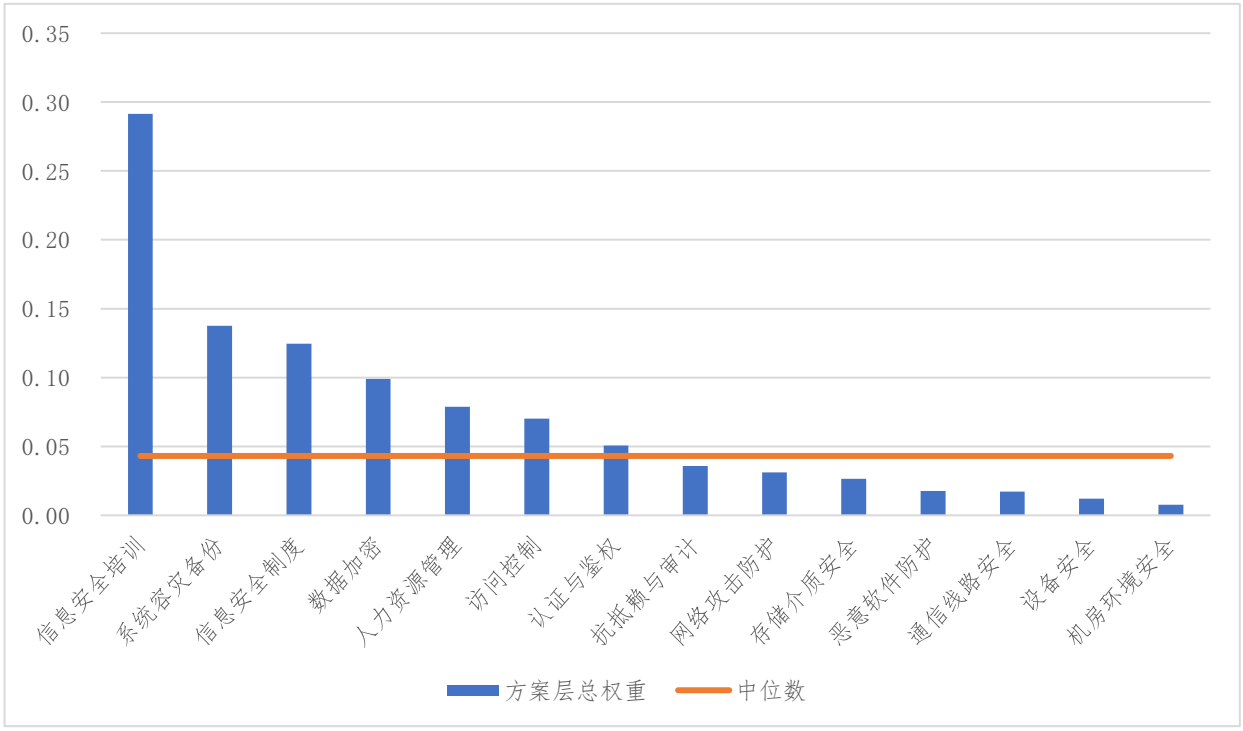

图 4-3 CZ 银行小微贷款系统信息安全风险评估指标权重分布图

4.2 信息安全风险的综合模糊评价

(1) 确定信息安全风险评估指标与权重

由前文内容，建立了 CZ 银行小微贷款系统信息安全风险评估指标体系，并对相关因素采用层次分析法进行计算，通过一致性校验，相关结果可信度较高，作为本实例中风险因素集与权重集，详见表 5-9。

(2) 确定评价集与隶属度矩阵

针对本案例中的小微贷款信息系统的信息安全风险评估过程，采用评语集如下：

$$V = \{非常安全, 安全, 一般, 危险, 非常危险\} \quad (4-1)$$

本案例中对指标进行评价过程中，采用专家背靠背打分方式，对方案层指标进行专家评判打分，调研表详见附录三。参与评判的专家与前期指标确认、权重确认一致，详见表 2-3。根据结果进行汇总整理，并对相应指标比例进行分析，明确如下表 4-8 专家评判汇总表。

表 4-8 CZ 银行小微贷款系统信息安全风险专家评判汇总表

风险因素指标	非常安全	安全	一般	危险	非常危险
机房环境安全（B1）	0.6	0.4	0	0	0
设备安全（B2）	0.7	0.3	0	0	0
通信线路安全（B3）	0.6	0.4	0	0	0
存储介质安全（B4）	0.4	0.6	0	0	0
认证与鉴权（B5）	0.6	0.3	0.1	0	0
访问控制（B6）	0.5	0.4	0.1	0	0
数据加密（B7）	0.6	0.4	0	0	0
抗抵赖与审计（B8）	0.5	0.5	0	0	0
系统容灾备份（B9）	0.7	0.3	0	0	0
恶意软件防护（B10）	0.6	0.3	0.1	0	0
网络攻击防护（B11）	0.5	0.4	0.1	0	0
人力资源管理（B12）	0.2	0.3	0.3	0.1	0.1
信息安全制度（B13）	0.3	0.3	0.2	0.2	0
信息安全培训（B14）	0.2	0.4	0.3	0.1	0

由以上表格可以得出物理安全（A1）的隶属度矩阵：

$$R_1 = \begin{bmatrix} 0.6 & 0.4 & 0 & 0 & 0 \\ 0.7 & 0.3 & 0 & 0 & 0 \\ 0.6 & 0.4 & 0 & 0 & 0 \\ 0.4 & 0.6 & 0 & 0 & 0 \end{bmatrix} \quad (4-2)$$

数据安全（A2）的隶属度矩阵：

$$R_2 = \begin{bmatrix} 0.6 & 0.3 & 0.1 & 0 & 0 \\ 0.5 & 0.4 & 0.1 & 0 & 0 \\ 0.6 & 0.4 & 0 & 0 & 0 \\ 0.5 & 0.5 & 0 & 0 & 0 \end{bmatrix} \quad (4-3)$$

运行安全（A3）的隶属度矩阵：

$$R_3 = \begin{bmatrix} 0.7 & 0.3 & 0 & 0 & 0 \\ 0.6 & 0.3 & 0.1 & 0 & 0 \\ 0.5 & 0.4 & 0.1 & 0 & 0 \end{bmatrix} \quad (4-4)$$

管理安全（A4）的隶属度矩阵：

$$R_4 = \begin{bmatrix} 0.2 & 0.2 & 0.3 & 0.3 & 0 \\ 0.3 & 0.3 & 0.2 & 0.2 & 0 \\ 0.2 & 0.4 & 0.3 & 0.1 & 0 \end{bmatrix} \quad (4-5)$$

(3) 根据公式$B = A \circ R$确定评判向量

根据A_1和R_1运算获得物理安全 A1 相关指标的风险隶属度向量B_1：

$$\begin{aligned} B_1 &= A_1 \circ R_1 \\ &= (0.1209, 0.1928, 0.2695, 0.4168) \circ \begin{bmatrix} 0.6 & 0.4 & 0 & 0 & 0 \\ 0.7 & 0.3 & 0 & 0 & 0 \\ 0.6 & 0.4 & 0 & 0 & 0 \\ 0.4 & 0.6 & 0 & 0 & 0 \end{bmatrix} \\ &= (0.5359, 0.4641, 0, 0, 0) \end{aligned} \quad (4-6)$$

同理可以得出其他准则层相关指标的风险隶属度向量B_2、B_3、B_4：

$$B_2 = (0.5585, 0.3942, 0.0473, 0, 0) \quad (4-7)$$

$$B_3 = (0.6570, 0.3168, 0.0262, 0, 0) \quad (4-8)$$

$$B_4 = (0.2252, 0.3430, 0.2748, 0.1570, 0) \quad (4-9)$$

针对目标层，整体风险评估指标隶属度向量B按照如下方式计算：

$$\begin{aligned} B &= A \circ R = A \circ (B_1, B_2, B_3, B_4)^T \\ &= (0.0635, 0.2552, 0.1864, 0.4948) \circ \begin{bmatrix} 0.5359 & 0.4641 & 0 & 0 & 0 \\ 0.5585 & 0.3942 & 0.0473 & 0 & 0 \\ 0.6570 & 0.3168 & 0.0262 & 0 & 0 \\ 0.2252 & 0.3430 & 0.2748 & 0.1570 & 0 \end{bmatrix} \\ &= (0.4105, 0.3588, 0.1529, 0.0777, 0) \end{aligned} \quad (4-10)$$

根据专家判断，相应评语集安全风险分数取值集合如下，其中分值越高说明风险越大：

$$V = \{20, 40, 60, 80, 100\} \quad (4-11)$$

对 CZ 银行小微贷款系统的整体信息安全分数进行计算

$$Y = B \circ V^T = 37.96 \quad (4-12)$$

参照业界专家经验确认风险分值与风险等级的对应关系如下表 4-9 所示，因此 CZ 银行小微贷款系统得分 37.96 分说明整体风险级别处于四级，低风险水平，个别风险指标需要加以控制。现对各二级、三级风险指标进行信息安全分数和加权分数计算、排序，汇总结果如下表 4-10 所示。

表4-9信息安全风险等级对照表

风险分值	[0,20]	(20,40]	(40,60]	(60,80]	(80,100]
风险等级	五级	四级	三级	二级	一级
风险描述	风险很低，安全事件发生可能性很小	风险低，安全事件发生可能性较小	风险中，安全事件发生可能性较大	风险高，安全事件发生可能性较大	风险很高，安全事件发生可能性非常大

表4-10 CZ银行小微贷款系统信息安全风险评估结果汇总表

目标层	准则层	得分	综合得分	方案层	得分	综合得分	综合排序
CZ银行小微贷款系统信息安全（Z）	物理安全（A1）	29.28	1.86	机房环境安全（B1）	28	0.22	14
				设备安全（B2）	26	0.32	13
				通信线路安全（B3）	28	0.48	12
				存储介质安全（B4）	32	0.85	10
	数据安全（A2）	29.78	7.60	认证与鉴权（B5）	30	1.52	7
				访问控制（B6）	32	2.24	6
				数据加密（B7）	28	2.77	5
				抗抵赖与审计（B8）	30	1.07	8
	运行安全（A3）	27.38	5.11	系统容灾备份（B9）	26	3.58	4
				恶意软件防护（B10）	30	0.53	11
				网络攻击防护（B11）	32	1.00	9
	管理安全（A4）	47.27	23.39	人力资源管理（B12）	54	4.26	3
				信息安全制度（B13）	46	5.73	2
				信息安全培训（B14）	46	13.40	1

4.3 风险评估结果分析

通过如上信息安全风险综合模糊评价及计算结果，CZ银行小微贷款系统的整体安全评分为37.96分，符合“低风险”等级水平。根据准则层与方案层加权数据整合，形成CZ银行小微贷款系统信息安全二级、三级加权分值分布图，如图4-4所示，图中面积越多说明对信息安全风险越大。结合隶属度原则，我们可以获得如下信息：

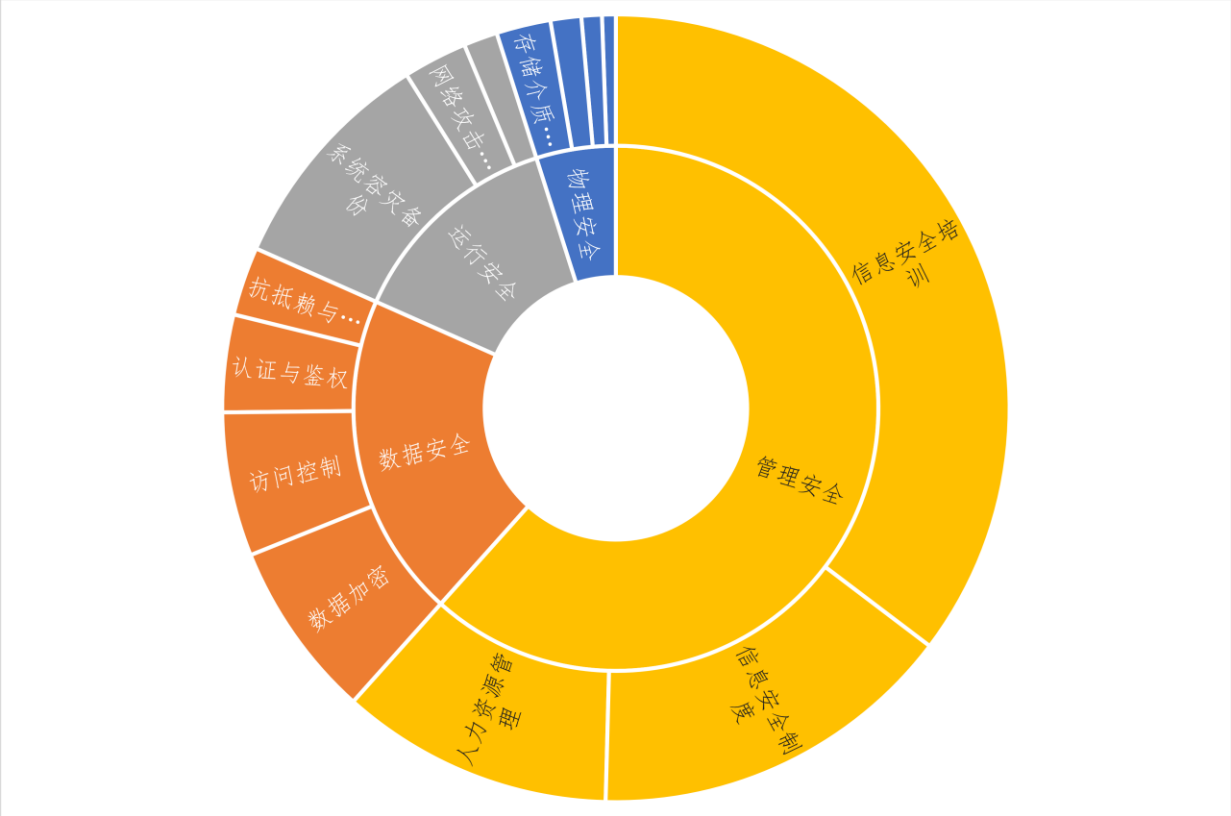

图 4-4 CZ银行信息安全风险指标加权分值比重分布图

物理安全方面，$B_1 = (0.5359, 0.4641, 0, 0, 0)$，第一级的隶属度最大，第三、四、五级为 0，信息安全风险分值为 29.28 分，达到“低风险”水平等级，说明 CZ 银行小微贷款系统物理安全相关指标是良好的。通过对三级指标测算，机房环境安全（B1）、设备安全（B2）、通信线路安全（B3）、存储介质安全（B4）分项得分均低于分，达到“低风险”水平等级，相关安全水平较高。物理安全加权分值为 1.86，未见对安全风险影响较大的因素。物理安全得益于 CZ 银行小微贷款系统建设对基础设施建设的高标准，而潜在风险主要包括不可抗性自然灾害、通信电力等不可预期情况，相关风险触发条件高且概率极低，对信息安全影响较低。

数据安全方面，$B_2 = (0.5585, 0.3942, 0.0473, 0, 0)$，第一级隶属度最大，超过半数，其他级别依次递减，第四、五级为 0，信息安全风险分值为 29.78，达到“低风险”水平等级，说明数据安全相关指标是良好的。通过对三级指标测算，认证与鉴权（B5）、访问控制（B6）、数据加密（B7）、抗抵赖与审计（B8）分项得分均介于 20~40 分之间，达到“低风险”水平等级。数据安全加权分值为 7.6，三级指标中访问控制（B6）、数据加密（B7）风险分值相对其他指标影响较大，分析原因为CZ银行针对小微贷款系统数据安全定期开展内、外部交替审计，并及时针对风险点进行优化处置，提升了整体数据安全水

平，而访问控制和数据加密受技术、流程、人员等多方面因素影响，风险面广且危害大，查阅以往审计记录，有多项访问控制与数据加密相关风险未整改，有一定的安全隐患。

运行安全方面，$B_3 = (0.6570, 0.3168, 0.0262, 0, 0)$，第一级隶属度最大，其他级别依次递减，第四、五级为 0，信息安全风险分值为 27.38，达到“低风险”水平等级，说明运行安全相关指标是良好的。通过对三级指标测算，系统容灾备份（B9）、恶意软件防护（B10）、网络攻击防护（B11）分项得分均介于20~40分之间，达到“低风险”水平等级。CZ 银行在小微贷款系统运行安全防护上投入大量人力、物力和资金，建立了体系信息安全运营保障体系，构建了网络层、系统层、应用层、数据层全方位防护体系，保障了运行安全性，而小微贷款系统由于为近几年上线业务，未对系统采取“双活”灾备模式，一旦发生不可预期事件，有一定的可用性风险。

管理安全方面，$B_4 = (0.2252, 0.3430, 0.2748, 0.1570, 0)$，第二级隶属度最大，第五级为 0，信息安全风险分值为 47.27，达到“中风险”安全水平等级，说明管理安全指标存在一定的风险，需要加以控制。通过对三级指标测算人力资源管理（B12）、信息安全制度（B13）、信息安全培训（B14）分值均介于40~60分之间，为“中风险”水平等级，需要进行进一步整改优化。管理安全加权分值为 23.39，占 60%以上，对 CZ 银行小微贷款系统的整体安全风险影响较大。分析主要原因，CZ 银行在小微贷款系统的信息安全基础设施建设、技术等方面投入较大，但对于专业技术人力资源管理、外包管理、制度建设与落实、专业技术培训等方面有待提升，偶发外包人员信息泄露、违规操作等现象。

综上所述，CZ 银行小微贷款系统的主要信息安全风险为信息安全培训（B14）、信息安全制度（B13）、人力资源管理（B12），该三种风险值排名前三，且权重综合超过 50%，相关风险指标对信息安全水平影响相对较大，均达到中风险水平，形成了整体安全水平的“短板”，需要开展进一步安全优化，提升信息安全水平。

4.4 本章小结

本章通过定性与定量分析方法对CZ银行小微贷款系统信息安全风险进行了评估。首先对信息安全风险指标进行确认与权重计算，采用文献分析与专家评判方式对指标进行确定与层次结构梳理，权重确认过程应用了层次分析法（AHP）对相关权重进行计算，并通过一致性校验，相关结果有效。通过风险评估指标体系建立，明确主要风险因素包含信息安全培训、系统容灾备份、信息安全制度、数据加密、人力资源管理、访问控制、

认证与鉴权，相关指标均排在CZ银行小微贷款系统信息安全风险权重中位数以上，为进一步优化商业银行信息安全管理，提升风险水平打下了基础。最后采用模糊综合评价法（FCE）对CZ银行小微贷款系统进行整体安全风险评价，笔者评估该信息系统的整体安全评分为26.02分，处于“低风险”水平等级，人力资源管理（B12）、信息安全制度（B13）、信息安全培训（B14）三项指标风险比重较大，需进一步对相应风险进行控制。

5 CZ银行小微贷款系统信息安全风险管理策略

5.1 信息安全培训风险优化对策

CZ 银行小微系统的平稳运行离不开相关人员的专业职业素质，不但要求具备专业的业务能力，也需要具备良好的信息安全意识。当前CZ银行小微贷款系统相关人员在安全意识淡薄、安全机能水平偏弱，主要表现在账号口令共享、钓鱼邮件事件频发、安全监控能力不具备等，因此需要开展信息安全技能培训与继续教育工作能迅速提升员工技能水平，以提高信息安全风险管理水平。

笔者建议CZ银行分层次、分阶段、循序渐进地对银行全员、科技部技术人员、信息安全部人员进行不同维度的信息安全技能培训，并在培训结束后进行技能考核，提升培训受众的信息安全风险管理意识和技能水平，提高 CZ 银行风险应对能力。CZ 银行根据风险评估结果，特制定如下培训计划如下表5-1所示。

表5-1 CZ银行信息安全培训课程清单

序号	课程内容	培训受众	培训频率
1	信息安全风险意识专项培训	CZ银行全员	每年2次
2	信息安全攻防演练	CZ银行全员	每年2次
3	办公环境信息安全风险防护	CZ银行全员	每年2次
4	信息安全风险管理文件培训	CZ银行全员	每年2次
5	个人信息安全防护	CZ银行全员	每年2次
6	网络安全运维管理培训	科技部全员	每年2次
7	信息安全测试培训	科技部全员	每年3次
8	Windows操作系统安全管理培训	科技部全员	每年3次
9	Linux操作系统安全管理培训	科技部全员	每年3次
10	信息安全风险评估培训	科技部全员	每年3次
11	等级保护合规培训	信息安全部全员	每年4次
12	网络安全设备运维管理培训	信息安全部全员	每年4次
13	安全开发管理培训	信息安全部全员	每年4次
14	SDL软件安全开发管理培训	信息安全部全员	每年4次

5.2 信息安全制度风险优化对策

信息安全管理制度是信息安全管理的重要组成部分，一方面需要制定完备的信息安全管理制度和流程，另一方面在执行与考核方面进行深入落地。CZ 银行小微贷款系统制定了基本的信息安全管理制度，但管理制度体系性不足，因此笔者建议 CZ 银行参照ISO/IEC 27001:2018标准健全信息安全风险管理制度，建立四级信息安全风险管理体系，

提升信息安全管理体系落实效果。四级体系如下图5-1所示，相关级别说明如下：

一级政策方针：CZ银行全组织范围内信息安全方针，明确信息安全目标、体制、职责等纲领性内容，如信息安全方针、适用性声明等,；

二级管理程序：各类管理制度程序文件，明确人、物理、技术方面信息安全、风险管理、法律法规遵守、教育、监视评审等，如信息安全风险管理程序、设备管理程序、审核程序等；

三级操作规范：具体的作业规范指导文件，明确运行程序、信息系统的措施以及流程规范和指南等，如信息安全风险评估指南；

四级记录表单：信息安全风险管理过程的记录文件表单，包括记录、管理台账、检查表等，如机房进入登记表等。

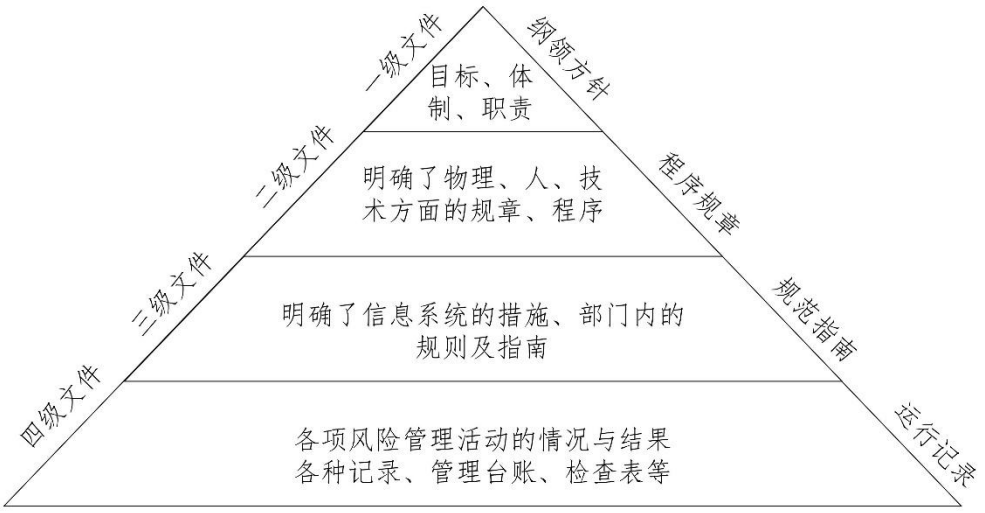

图5-1 四级信息安全管理文档体系示意图

根据信息安全风险评估结果与四级信息安全风险管理文件体系，需要对现有管理体系进行了完善，健全了信息安全风险管理体系中方针、程序、规范、记录等制度体系，形成如下管理体系清单如下表5-2所示：

表5-2 CZ银行四级信息安全风险管理体系表

序号	文件类别	文件名称	版本
1	方针文件	CZ银行信息安全方针	修订
2	程序文件	CZ银行业务持续性程序	修订
3	程序文件	CZ银行事故、薄弱点与故障程序	修订
4	程序文件	CZ银行企业商业技术秘密管理程序	修订
5	程序文件	CZ银行信息安全人员考察与保密管理程序	修订
6	程序文件	CZ银行信息安全奖励、惩戒管理规定	修订

续表 5-2

序号	文件类别	文件名称	版本
7	程序文件	CZ银行信息安全风险评估程序	新增
8	程序文件	CZ银行内部审核程序	修订
9	程序文件	CZ银行恶意软件控制程序	修订
10	程序文件	CZ银行更改控制程序	修订
11	程序文件	CZ银行物理访问程序	新增
12	程序文件	CZ银行系统开发与维护控制程序	修订
13	程序文件	CZ银行系统访问与使用监控管理程序	修订
14	程序文件	CZ银行重要信息备份管理程序	修订
15	操作规范	CZ银行介质销毁办法	修订
16	操作规范	CZ银行保障业务管理规定	新增
17	操作规范	CZ银行信息中心主机房管理制度	修订
18	操作规范	CZ银行信息中心密码管理规定	修订
19	操作规范	CZ银行数据加密管理规定	修订
20	操作规范	CZ银行文件审批表	修订
21	操作规范	CZ银行机房安全管理规定	修订
22	操作规范	CZ银行经营部信息事故处理规定	新增
23	操作规范	CZ银行经营部信息安全岗位职责规定	修订
24	操作规范	CZ银行经营部计算机机房管理规定	修订
25	操作规范	CZ银行网络中间设备安全配置管理规定	新增
26	操作规范	CZ银行计算机硬件管理维护规定	修订
27	记录文件	CZ银行事故调查分析及处理报告	新增
28	记录文件	CZ银行用户设备使用申请单	新增
29	记录文件	CZ银行信息发布审查表	修订
30	记录文件	CZ银行信息处理设施使用情况检查表	修订
31	记录文件	CZ银行信息安全外部专家名单	修订
32	记录文件	CZ银行信息安全故障处理记录	新增
33	记录文件	CZ银行信息安全法律、法规符合性评价报告	修订
34	记录文件	CZ银行系统测试计划	修订
35	记录文件	CZ银行信息安全记录一览表	新增
36	记录文件	CZ银行计算机信息网络系统容量规划	修订
37	记录文件	CZ银行信息设备转移单	修订
38	记录文件	CZ银行设备处置再利用记录	修订
39	记录文件	CZ银行设施系统更改报告	修订
40	记录文件	CZ银行信息资产识别表	修订
41	记录文件	CZ银行访问权限评审记录	修订

续表 5-2

序号	文件类别	文件名称	版本
42	记录文件	CZ银行外部网络访问授权登记表	修订
43	记录文件	CZ银行软件设计开发方案	新增
44	记录文件	CZ银行软件验收报告	修订
45	记录文件	CZ银行操作系统更改技术评审报告	修订
46	记录文件	CZ银行远程工作申请表	修订
47	记录文件	CZ银行敏感重要信息媒体处置申请表	修订
48	记录文件	CZ银行重要信息备份周期一览表	修订
49	记录文件	CZ银行文件修改通知单	修订
50	记录文件	CZ银行机房值班日志	新增
51	记录文件	CZ银行文件借阅登记表	修订
52	记录文件	CZ银行机房出入登记表	修订
53	记录文件	CZ银行文件发放回收登记表	新增
54	记录文件	CZ银行生产经营持续性管理战略计划	修订
55	记录文件	CZ银行文件销毁记录表	修订
56	记录文件	CZ银行生产经营持续性管理计划	修订

通过四级信息安全风险管理体系文件的建立，明确自顶至下的风险管理架构，并在相关风险管理上更容易被高层理解、接受，有利于信息安全保障目标的达成。同时，结合戴明环（PDCA）方式对相关管理制度进行执行和优化，提升信息安全风险管理制度体系对业务的契合度，促进小微贷款系统的安全风险水平达到很低水平。

5.3 人力资源管理风险优化对策

CZ 银行小微贷款信息系统的人力资源主要涉及信息科技部、小额贷款管理部、第三方外包人员等，特别是外包人员流动性大、人员多、管理分散，因此针对人力资源管理的信息安全风险笔者建议从如下方面入手进行安全风险控制：

(1) 针对全员签订保密协议，并阶段性宣贯培训。保密协议是针对 CZ 银行小微贷款系统相关业务人员、技术人员的保密约束协议，对工作中获取到的文档、数据、信息等具有保密的义务，一方面约束本行相关人员，另一方面约束第三方厂商外包人员，降低因人员流动造成的信息泄露风险。

(2) 完善人力资源入职、离职流程。CZ银行小微贷款系统业务人员具有较高的业务权限，技术人员具有系统控制权限，因此相关人员入职时的审查、离职时的约束都对小微

贷款系统的信息安全风险有较大的影响，因此笔者建议CZ银行针对人员入职或入场阶段开展必要的背景调查、职业道德评估、能力评估，离职或离场时保密协议、竞业禁止协议的签订，对小微银行相关人员的能力匹配情况、职业道德素质、保密与竞业约束进行全方面把控，提升人力资源管理水平，降低人力资源对小微贷款系统的信息安全风险影响，以保障小微贷款系统的信息安全。

(3) 阶段性开展尽职审查。CZ银行小微贷款系统相关工作人员均具备较高的权限，虽然具备完善的信息安全审计机制，但仍可能存在人员之间的舞弊、合谋等风险。因此，笔者建议CZ银行在人力资源方面阶段性开展关键岗位的尽职调查，识别关键岗位在使用技术或业务过程中是否存在串通、违规等问题，审计相关信息安全风险，达到威慑与识别风险的目的。

(4) 将信息安全指标纳入相关人员绩效考核。信息安全风险是动态的，具有较大的不确定性，安全风险存在于每一个与小微贷款相关的人，不仅包含系统管理员、网络管理员，甚至保安人员都有可能是信息安全风险的关联人员。因此有必要将相关安全管理责任要求到组织的每一个部门，从全员角度对信息安全有认知、有意识，自顶向下传递信息安全的责任，提升信息安全风险管理水平。

5.4 本章小结

CZ银行小微贷款系统的信息安全风险主要为人力资源管理、信息安全制度、信息安全培训三项指标，本章针对这三方面对CZ银行小微贷款系统的安全风险提出了建设性对策，以提升小微贷款系统的安全风险水平。人力资源方面，建议CZ银行从签订保密协议、完善人力资源入离职流程、阶段性开展尽职审查、将信息安全指标纳入相关人员绩效考核开展优化工作；信息安全制度方面建立四级风险管理体系制度，并采用PDCA开展制度落实与优化；信息安全培训方面从不同人员层次、不同周期开展信息安全培训，降低CZ银行小微贷款系统信息安全风险。

6 结论与展望

6.1 结论

商业银行信息系统的信息安全风险评估由于业务、组织、技术的复杂性面临着诸多挑战，本文通过对比评估方法，选取层次分析法（AHP）与模糊综合评价法（FCE）结合的模型对 CZ 银行小微贷款系统的信息安全风险进行评估。首先，采用德尔菲法对 CZ 银行小微贷款系统风险因素指标体系进行建立。其次，采用层次分析法（AHP）对指标体系进行递阶结果构建，并计算相关指标相对目标的权重。最后，采用模糊综合评价法（FCE）对 CZ 银行小微贷款系统进行风险评估，并对结果分析及给出风险控制对策。研究得到以下主要结论：

(1) 本文建立了 CZ 银行小微贷款系统的信息安全风险因素递阶层次体系，即准则层为物理、数据、运行、管理安全 4 项，方案层为机房环境安全、设备安全、通信线路安全、存储介质安全、认证与鉴权、访问控制、数据加密、抗抵赖与审计、系统容灾备份、恶意软件防护、网络攻击防护、人力资源管理、信息安全制度、信息安全培训等 14 项。该指标体系经文献检索与专家判断结合方式获得，科学性与合理性较强。

(2) 经层次分析法（AHP）对各指标权重计算，影响 CZ 银行小微贷款系统的风险主要因素准则层为数据安全和管理安全，对应的方案层指标为数据加密、访问控制和信息安全制度、信息安全培训，这些指标对商业银行信息系统的安全风险影响较大，具备较高的安全隐患，如果不加以控制容易造成严重信息安全事故。

(3) 层次分析法（AHP）结合模糊综合评价法（FCE）模型在对商业银行信息系统的信息安全风险评估场景中具有普适性。通过层次分析法对风险评估指标体系进行构建与权重计算，同时采用模糊综合评价法对被评估对象进行综合评价，解决了商业银行信息系统风险评价过程中模糊性定性结果到科学性量化结果的转化。通过实例证明，该模型可以应用在 CZ 银行小微贷款的评价过程中，因此可以推广到其他同类信息安全风险评估场景中。

(4) 从层次分析法指标体系、指标权重、模糊综合评价法结果来看，影响 CZ 银行小微贷款系统的信息安全风险来源不仅包含技术，还包含人员、制度流程，如实例中的信息安全制度、信息安全培训因素是影响 CZ 银行小微贷款系统的主要风险因素。人员风险、制度风险持续存在，相较技术风险更难优化改进。

6.2 展望

本文构建了 AHP-FCE 评估模型对 CZ 银行小微贷款系统的信息安全风险进行评估，具有一定的实践意义。鉴于信息安全风险具有动态性、系统性，笔者认为可以从如下方面开展进一步研究和探索：

(1) AHP-FCE 模型构建和应用过程中，考虑操作便捷与时间成本，分别采用德尔菲法对风险指标识别与指标评价，虽然参访人员经过一定规则的筛选，但过程存在一定的主观性，对指标项的确认、权重结果计算、综合评价结果有不同程度的影响，造成结果失真。因此，有必要研究结合客观的数据收集或数据校验方式对数据进行进一步优化，提升可信度。

(2) CZ 银行小微贷款系统的信息安全风险指标体系建立过程中，采用文献与德尔菲法方式开展，受限于笔者学识、资料完整度、专家因素影响，递阶层次指标可能会有一定不足，影响指标和权重的普适性。因此，针对指标体系的建立需要进一步对各因素指标进行深入探讨。

(3) 商业银行信息安全风险具有不确定性和动态性，本文采用的分析模型是静态评价分析方式，不能对信息安全风险进行动态识别与评价，因此对商业银行信息安全动态评价有必要进一步探索。

参考文献

[1] 薛莹,胡坚.金融科技助推经济高质量发展：理论逻辑、实践基础与路径选择[J].改革,2020(03):53-62.

[2] 陈红,郭亮.金融科技风险产生缘由、负面效应及其防范体系构建[J].改革,2020(03):63-73.

[3] 周健.云计算背景下的信息安全问题研究[J].现代电子技术,2017,40(11):84-87.DOI:10.16652/j.issn.1004-373x.2017.11.022.

[4] 林燕.网络信息安全的风险评估及管理策略[J].信息系统工程,2020(08):56-57.

[5] 李莉,魏巨升.信息安全评估评测体系研究及 ISMS 审核实践[J].电子产品世界,2020,27(11):79-83.

[6] KIM ZETTER.That Insane, $81M Bangladesh Bank Heist? Here's What We Know[EB/OL].https://www.wired.com/2016/05/insane-81m-bangladesh-bank-heist-heres-know/,2016-05-17.

[7] Saloni Shukla,Pratik Bhakta.3.2 million debit cards compromised; SBI, HDFC Bank, ICICI, YES Bank and Axis worst hit[EB/OL].https://economictimes.indiatimes.com/industry/banking/finance/banking/3-2-million-debit-cards-compromised-sbi-hdfc-bank-icici-yes-bank-and-axis-worst-hit/articleshow/54945561.cms,2016-10-20.

[8] Jeff Peters.Weekly Cyber Risk Roundup: Banks Threatened with DDoS Attacks and Researchers Investigate NotPetya[EB/OL].https://blog.surfwatchlabs.com/2017/07/03/14947/,2017-07-03

[9] 胡琳,卢九安.华夏银行技术处长给系统植入病毒 以测试 BUG 的名义上千次盗取资金[EB/OL].http://finance.china.com.cn/money/bank/20190203/4889731.shtml,2019-02-03.

[10] Ruby Hinchliffe.Chile’s BancoEstado falls victim to ransomware attack[EB/OL].https://www.fintechfutures.com/2020/09/chiles-bancoestado-falls-victim-to-ransomware-attack/,2020-09-09.

[11] Cryptocurrency.Hacker steals $200 million from PancakeBunny in a flash loan exploit[EB/OL].https://www.investing.com/news/cryptocurrency-news/hacker-steals-200-million-from-pancakebunny-in-a-flash-loan-exploit-2512754,2021-05-20.

[12] 于东智,夏小飞.构建银行信息科技风险管理体系[J].中国金融,2019(02):65-66.

[13] 谢治春,赵兴庐,刘媛.金融科技发展与商业银行的数字化战略转型[J].中国软科学,2018(08):184-192.

[14] 黄益平,黄卓.中国的数字金融发展:现在与未来[J].经济学(季刊),2018,17(04):1489-1502

[15] 俞勇.金融科技与金融机构风险管理[J].上海金融,2019(07):73-78.DOI:10.13910/j.cnki.shjr.2019.07009.

[16] 银行业金融机构法人名单(截至2021年12月末)[EB/OL].http://www.cbirc.gov.cn/cn/view/pages/govermentDetail.html?docId=1043881&itemId=863&generaltype=1,2022-03-21.

[17] 贾海云,谢宗晓.基于全面风险管理视角的金融网络安全管理标准框架[J].中国质量与标准导报,2018,(8):24-28. DOI:10.3969/j.issn.1004-1575.2018.08.015.

[18] 于东智,夏小飞.构建银行信息科技风险管理体系[J].中国金融,2019(02):65-66.

[19] 李莉,魏巨升.信息安全评估评测体系研究及 ISMS 审核实践[J].电子产品世界,2020,27(11):79-83.

[20] ISO,Common Criteria for Information Technology Security Evaluation[S]ISO/IEC 15408:1999.

[21] Guide to the implementation and auditing of BS 7799 controls:BS PD 3004-2002[S].

[22] 谢宗晓,许定航.ISO/IEC 27005:2018 解读及其三次版本演化[J].中国质量与标准导报,2018,(9):16-18. DOI:10.3969/j.issn.1004-1575.2018.09.016.

[23] Anomah and Aduamoah. PROPOSED ANALYTICAL PROCEDURE FOR THE CUSTOMIZATION AND IMPLEMENTATION OF COBIT 5, AN AUDITING TOOL: AN ACTION DESIGN RESEARCH APPROACH[J]. EDPACS, 2018, 57(3) : 15-34.

[24] 杨佩毅.基于 COBIT5.0 的银行信息系统审计评价体系构建[J].财会通讯,2021(23):138-141.DOI:10.16144/j.cnki.issn1002-8072.2021.23.027.

[25] 王惠莅,刘贤刚,李海东.美国 NIST 信息安全标准探究[J].保密科学技术,2018(01):19-25.

[26] Force J T. Risk management framework for information systems and organizations[J]. NIST Special Publication, 2018, 800: 37.

[27] 于品显.巴塞尔协议资本要求的发展变化、局限性及我国的应对策略[J].南方金融,2020(07):69-78.

[28] 韩杨.我国商业银行全面风险管理框架选择研究--基于巴塞尔资本协议与 COSO-ERM 的比较[J]. 中国商论,2016,(19):71-72. DOI:10.3969/j.issn.1005-5800.2016.19.039.

[29] Gao F, Zhang I X. The impact of the sarbanes-oxley act on the dual-class voting premium[J]. The Journal of Law and Economics, 2019, 62(1): 181-214.

[30] Ashbaugh-Skaife H , Collins D W , Kinney W R , et al. The Effect of SOX Internal Control Deficiencies on Firm Risk and Cost of Equity[J]. Journal of Accounting Research, 2010, 47(1):1-43.

[31] Enterprise Risk Management—Integrating with Strategy and Performance (2017)[EB/OL].https://www.coso.org/Pages/ERM-Framework-Purchase.aspx,2017.

[32] 高菁敏,李曼.基于 COSO(2017)新框架的我国商业银行风险管理模式构建[J].商业会计,2019,(6):41-44. DOI:10.3969/j.issn.1002-5812.2019.06.012.

[33] 张尧祯,刘昱.银行业信息科技风险防范及管理研究——兼析新加坡信息科技风险管理的主要做法[J].价格理论与实践,2020,(1):167-170. DOI:10.19851/j.cnki.CN11-1010/F.2020.01.093.

[34] 国家市场监督管理总局、中国国家标准化管理委员会.信息安全技术 网络安全等级保护基本要求:GB/T 22239-2019[S],2019.

[35] 高亚楠,刘丰,陈永刚.信息安全风险管理标准体系研究[J].信息安全研究,2018,4(10):928-933.

[36] 黄端.利用 IT 服务规避商业银行信息科技风险管理[J].银行家,2009,(12):106-108. DOI:10.3969/j.issn.1671-1238.2009.12.031.

[37] 中国银行业监督管理委员会.银监会发布《商业银行信息科技风险管理指引》[EB/OL].http://www.gov.cn/gzdt/2009-06/01/content_1329547.htm,2009-06-01.

[38] 李欲晓.商业银行内部信息安全战略管理体系的构建[J].农村金融研究,2015,(7):57-62. DOI:10.3969/j.issn.1003-1812.2015.07.015.

[39] 胡沛涛.关于金融网络安全的若干思考[J].中国商论,2020,(16):64-65. DOI:10.19699/j.cnki.issn2096-0298.2020.16.064.

[40] 杨宇焰.金融监管科技的实践探索、未来展望与政策建议[J].西南金融,2017(11):22-29.

[41] Dos Santos P H, Neves S M, Sant'Anna D O, et al. The analytic hierarchy process supporting decision making for sustainable development: An overview of applications[J]. Journal of cleaner production, 2019, 212: 119-138.

[42] Darko A, Chan A P C, Ameyaw E E, et al. Review of application of analytic hierarchy process (AHP) in construction[J]. International journal of construction management, 2019, 19(5): 436-452.

[43] Zadeh L A. Fuzzy sets[M]//Fuzzy sets, fuzzy logic, and fuzzy systems: selected papers by Lotfi A Zadeh. 1996: 394-432.

[44] Han L, Mei Q, Lu Y, et al. Analysis and study on AHP-fuzzy comprehensive evaluation[J]. China Safety Science Journal, 2004, 14(7): 89-92.

[45] Tran L T, Knight C G, O'Neill R V, et al. Fuzzy decision analysis for integrated environmental vulnerability assessment of the Mid-Atlantic region1[J]. Environmental management, 2002, 29(6): 845-859.

[46] Zhanwen F, Zhentang L, Zhonghui L. Risk prediction of coal and gas outburst based on analytic hierarchy process and fuzzy comprehensive evaluation method[J]. China Safety Science Journal, 2009, 19(3): 149-154.

[47] Ling X, Wu S. Using fuzzy analytic hierarchy process and fuzzy comprehensive evaluation in decision making for satellite mobile communication systems[C]//22nd AIAA International Communications Satellite Systems Conference & Exhibit 2004 (ICSSC). 2004: 3206.

[48] FU S, SONG D. An information security risk assessment method based on AHP and fuzzy comprehensive evaluation[J]. Research and Exploration in Laboratory, 2012, 31(6): 207-210.

[49] Xiao L, Dai Z K. Model of multilevel fuzzy comprehensive risk evaluation of information system[J]. JOURNAL-SICHUAN UNIVERSITY ENGINEERING SCIENCE EDITION, 2004, 36: 98-102.

[50] Peng X, Dai F. Information systems risk evaluation based on the AHP-fuzzy algorithm[C]//2009 International Conference on Networking and Digital Society. IEEE, 2009, 2: 178-180.

[51] 马永刚. 基于 FCE—AHP 的港口物流竞争力研究[J]. 经济管理, 2007(22):6.

[52] 赵伏军，谢世勇，杨磊,等. 基于层次分析法-模糊综合评价(AHP-FCE)模型优化矿井通风系统的研究[J]. 中国安全科学学报，2006，16(4):6.

[53] 赵彬，黄志坚，朱启明,等. 基于 AHP-FCE 法的指挥控制能力系统效能评估[J]. 火力与指挥控制，2018，43(5):4.

[54] 肖龙，戚湧，李千目. 基于 AHP 和模糊综合评判的信息安全风险评估[J]. 计算机工程与应用，2009，45(22):5.

[55] 韩霞,郭易鑫,王晖南,白建海,曹铠.基于 AHP 的电力运行信息安全管理风险评估的研究[J].国外电子测量技术,2018,37(05):32-37.

[56] Ng A W, Kwok B K B. Emergence of Fintech and cybersecurity in a global financial centre: Strategic approach by a regulator[J]. Journal of Financial Regulation and Compliance, 2017.

[57] Bruce Schneier.Secrets and lies : digital security in a networked world[M].John Wiley,2000.

[58] 黄水清,任妮.数字图书馆信息安全风险评估的方法与模型[J].图书情报工作,2014,58(02):14-20.

[59] 国务院印发 推进普惠金融发展规划(2016-2020 年)[J].中国金融家,2016(02):37-38.

[60] 《金融标准化“十四五”发展规划》发布（英文）[J].China Standardization,2022(02):8.

[61] Saaty T L. How to handle dependence with the analytic hierarchy process[J]. Mathematical Modelling, 1987, 9(3-5): 369-376.

[62] Yuan K, Li H, Jiang M. Research on AHP-fuzzy comprehensive evaluation method and application[C]//Journal of Physics: Conference Series. IOP Publishing, 2020, 1592(1): 012045.

[63] Pappaterra M J, Flammini F. Bayesian networks for online cybersecurity threat detection[M]//Machine intelligence and big data analytics for cybersecurity applications. Springer, Cham, 2021: 129-159.

[64] Boryczko K, Szpak D, Żywiec J, et al. The Use of a Fault Tree Analysis (FTA) in the Operator Reliability Assessment of the Critical Infrastructure on the Example of Water Supply System[J]. Energies, 2022, 15(12): 4416.

附录一 CZ 银行小微贷款系统信息安全风险指标因素调查提纲

尊敬的专家：

您好，根据相关文献资料与 CZ 银行小微贷款系统基本初步风险分析，识别如下信息安全风险指标因素，现针对相关指标要素和指标分类进行评判。

(1) 机房环境安全

(2) 设备安全

(3) 通信线路安全

(4) 认证与鉴权

(5) 访问控制

(6) 抗抵赖

(7) 系统容灾备份

(8) 恶意软件防护

(9) 网络攻击防护

(10) 人力资源管理

(11) 信息安全制度

针对如上研讨问题如下：

(1) 针对 CZ 银行小微贷款系统的信息安全风险评估指标，是否有修改、增加、删除项？

(2) 通过总结分类，初步形成了物理安全（机房环境安全、设备安全、通信线路安全）、数据安全（认证与鉴权、访问控制、抗抵赖）、运行安全（系统容灾备份、恶意软件防护、网络攻击防护）、管理安全（人力资源管理、信息安全制度）分类形式，请针对此初步分类给出分类优化意见。

附录二 CZ 银行小微贷款系统信息安全风险指标权重调查表

尊敬的专家：

您好，前期调研确认如下 CZ 银行小微贷款系统信息安全风险指标体系，现针对相关指标因素进行两两比较，跟重要性进行 1、3、5、7、9 或相应倒数的两两比较评价，请将结果反馈到如下空表格中。

目标层	准则层	方案层
CZ 银行小微贷款系统信息安全（Z）	物理安全（A1）	机房环境安全（B1）
		设备安全（B2）
		通信线路安全（B3）
		存储介质安全（B4）
	数据安全（A2）	认证与鉴权（B5）
		访问控制（B6）
		数据加密（B7）
		抗抵赖与审计（B8）
	运行安全（A3）	系统容灾备份（B9）
		恶意软件防护（B10）
		网络攻击防护（B11）
	管理安全（A4）	人力资源管理（B12）
		信息安全制度（B13）
		信息安全培训（B14）

1、目标层 Z 指标评价

信息安全（Z）	物理安全	数据安全	运行安全	管理安全
物理安全（A1）				
数据安全（A2）				
运行安全（A3）				
管理安全（A4）				

2、准则层 A1 指标评价

物理安全（A1）	机房环境安全	设备安全	通信线路安全	存储介质安全
机房环境安全（B1）				
设备安全（B2）				
通信线路安全（B3）				
存储介质安全（B4）				

3、准则层 A2 指标评价

数据安全（A2）	认证与鉴权	访问控制	数据加密	抗抵赖与审计
认证与鉴权（B5）				
访问控制（B6）				
数据加密（B7）				
抗抵赖与审计（B8）				

4、准则层 A3 指标评价

运行安全（A3）	系统容灾备份	恶意软件防护	网络攻击防护
系统容灾备份（B9）			
恶意软件防护（B10）			
网络攻击防护（B11）			

5、准则层 A4 指标评价

管理安全（A4）	人力资源管理	信息安全制度	信息安全培训
人力资源管理（B12）			
信息安全制度（B13）			
信息安全培训（B14）			

附录三 CZ 银行小微贷款系统信息安全风险指标评价打分表

尊敬的先生/女士：

您好，感谢您协助我们针对 CZ 银行小微贷款系统信息安全风险评估指标评价工作。根据前期工作中影响小微贷款系统信息安全风险的指标判断，形成如下指标矩阵，请您结合 CZ 银行小微贷款系统情况与信息安全技术相关内容，针对如下风险情况进行评价，在指定位置打“√”即可，谢谢！

风险因素指标	非常安全	安全	一般	危险	非常危险
机房环境安全（B1）					
设备安全（B2）					
通信线路安全（B3）					
存储介质安全（B4）					
认证与鉴权（B5）					
访问控制（B6）					
数据加密（B7）					
抗抵赖与审计（B8）					
系统容灾备份（B9）					
恶意软件防护（B10）					
网络攻击防护（B11）					
人力资源管理（B12）					
信息安全制度（B13）					
信息安全培训（B14）					