硕士学位论文

# M 公司信息安全管理优化研究

# Research on information security management optimization of M company

学科专业　　工商管理（MBA）

专业领域

作者姓名

指导教师

2021 年 10 月

中图分类号 F273.1　　学校代码 10533
UDC 005.6　　学位类别 专业学位

**硕士学位论文**

# M 公司信息安全管理优化研究

## Research on information security management optimization of M company

作 者 姓 名
学 科 专 业　　工商管理（MBA）
专 业 领 域
研 究 方 向　　信息安全
二级培养单位　　商学院
指 导 教 师
副 指 导 教 师

论文答辩日期 2021 年 月 日　　答辩委员会主席

中 南 大 学
2021 年 10 月

# 学位论文原创性声明

本人郑重声明，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。尽我所知，除了论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，也不包含为获得中南大学或其他教育机构的学位或证书而使用过的材料。与我共同工作的同志对本研究所作的贡献均已在论文中作了明确的说明。

申请学位论文与资料若有不实之处，本人承担一切相关责任。

作者签名：_____　　日期：_2021_年____月____日

# 学位论文版权使用授权书

本学位论文作者和指导教师完全了解中南大学有关保留、使用学位论文的规定：即学校有权保留并向国家有关部门或机构送交学位论文的复印件和电子版；本人允许本学位论文被查阅和借阅；学校可以将本学位论文的全部或部分内容编入有关数据库进行检索，可以采用复印、缩印或其它手段保存和汇编本学位论文。

保密论文待解密后适应本声明。

作者签名：_____　　导师签名_____

日期：_2021_年____月____日　　日期：_2021_年____月____日

# M 公司信息安全管理优化研究

**摘要：**在移动应用、互联网等 IT 技术日益普及的背景下，企业经营管理越发依赖信息技术这项辅助性手段，但信息技术在提升企业管理效率的同时，也为企业带来一系列的信息安全风险。作为新技术运用的先驱者，软件与信息技术服务行业在近年来的发展中面对着许许多多的外部信息安全问题，所以一直致力于信息安全管理水平的提升。M 公司是一家从事软件研发行业的年轻企业，在探索业务发展措施与途径的过程中，其同样受到信息安全管理问题的威胁。因此，在内部管理与外部风险共同作用下，M 公司如何强化信息安全管理显得尤为重要。

本文以 M 公司为研究对象，深入分析公司当前的信息安全管理现状，并从中归纳出公司现有问题。基于木桶原理、PDR 安全模型 ISO27001 等理论，对公司的系统维护与开发、人力资源安全、信息安全组织等问题进行分析，发现存在以下问题：组织结构不合理、信息安全管理制度不科学、技术工具建设不到位、人员安全意识差。根据问题提出了合理的优化与改进措施，即强化运作安全管理、优化信息安全组织、改进信息安全策略以及人力资源安全提升等。此外，本文还制定方案的具体实施计划，并系统阐述了方案实施过程中的核心要素，确保整个方案计划能够有效落实。

本文通过探寻 M 公司信息安全管理的改进策略，既有助于 M 公司信息安全管理水平的提升，又有助于公司业务管理风险的防范，同时还能帮助同类型企业更好的加强信息安全管理，进而为软件与信息安全行业发展提供一定帮助。

图 20 幅，表 4 个，参考文献 60 篇

**关键词：**信息安全；管理制度；信息技术
**分类号：**F273.1

# Research on information security management optimization of M company

**Abstract:** With the increasing popularity of IT technologies such as mobile applications and the Internet, enterprise management increasingly relies on information technology as an auxiliary means. However, information technology not only improves enterprise management efficiency, but also brings a series of information security risks to enterprises. As a pioneer in the application of new technologies, the software and information technology service industry has faced many external information security problems in recent years, so it has been committed to improving the level of information security management. M company is a young enterprise engaged in software R & D industry. In the process of exploring business development measures and ways, it is also threatened by information security management problems. Therefore, under the joint action of internal management and external risks, it is particularly important for M company to strengthen information security management.

Taking M company as the research object, this paper deeply analyzes the current situation of information security management of the company, and summarizes the existing problems of the company. Based on the barrel principle, PDR security model ISO27001 and other theories, this paper analyzes the problems of the company's system maintenance and development, human resource security and information security organization, and finds that there are the following problems: unreasonable organizational structure, unscientific information security management system, inadequate construction of technical tools and poor personnel security awareness. According to the problems, this paper puts forward reasonable optimization and improvement measures, that is, strengthening operation security management, optimizing information security organization, improving information security strategy and

improving human resource security. In addition, this paper also formulates the specific implementation plan of the scheme, and systematically expounds the core elements in the process of scheme implementation, so as to ensure the effective implementation of the whole scheme.

By exploring the improvement strategy of M company's information security management, this paper not only helps to improve the level of M company's information security management, but also helps to prevent the risk of the company's business management. At the same time, it can also help similar enterprises better strengthen information security management, so as to provide some help for the development of software and information security industry.

**Keywords:** Information Security; System Processes; Information Technology
**Classification:** F273.1

# 目 录

# 第 1 章 绪论

## 1.1 研究背景与意义

随着云计算、大数据、物联网、移动互联网、人工智能等新技术新应用的高速发展，数据来源于人类的各式各样行为，如个人敏感数据、上网浏览数据、办公文档数据等等。在海量的数据中，有一些数据是与公司发展有着密切关联的，这些影响着公司的发展与市场竞争力，还有一些数据是与个人信息相关的，这些数据关乎着人们各方面的安全。数据已成为一种新的生产要素，数据安全问题上升到国家安全战略高度，近年来，国家先后发布了《网络安全法》、《数据安全法》和《个人信息保护法》，为数据安全提供法律法规保障。但是随着互联网的快速发展，网上的信息安全威胁越来越大，时常出现数据泄露现象，如 2020 年微博暗网出售的 5.38 亿条用户信息、2021 年宏基遭受网络攻击，尤其是宏基事件，因这次网络攻击让宏基蒙受了近 5 千万美元的损失，是至今为止网络敲诈中最大的一起案件。因此，数据安全方面的问题显得越来越严峻，这会给客户和公司造成严重的损失。为了保护客户和公司的共同利益，我们必须严格保护公司信息系统的安全、稳定的运行，确保数据不被窃取、盗用、误用和恶意破坏。可见，在公司发展过程中，信息的安全与否非常重要，故而公司在发展中要注重加强信息的安全保障能力。

### 1.1.1 研究背景

在信息技术高速发展的背景下，人类社会中的数据规模和种类呈高速发展状态，尤其是大数据的海量爆发，将人类社会引入了大数据时代。目前，无论是学术界还是工业界都将大数据的探索作为主要课题。一方面，有关学者正致力于计算机技术与大数据的有机结合，如数据发掘、网络、通信等[1-3]。政府机构与各大企业都希望从海量的数据中找出有效信息，以此提升自身经济效益。随着大数据的快速发展，人们生活中的各方各面都涉及到大数据的运用，如能源、交通、医疗等等[4-7]。另一方面，随着大数据运用范围的不断扩大，因之带来的挑战和风险也越来越大。由于网络技术的快速发展，网络信息安全性受到极大威胁，网上出现的信息安全事件比比皆是，如 2017 年出现的勒索病毒，在极短的时间内对 150 多个国家会产生不良影响，导致多个国家的基础设施信息受到不同程度的损害，如交通、通信、医疗、教育等，这些基础设施都因此次事件陷入一定程度的瘫痪。据相关统计显示，因本次勒索病毒带来的损失高达 80 亿美元，而且因之带来的影响也不断扩大。2020 年 2 月，微博股票因删库事件大幅下滑，间接导致的损失高达 30 亿元。同年 12 月，富士康的

服务器遭受网络攻击，工厂中的 1200 台服务器都被加密，遭受盗取的数据达 100GB，后来因之受到勒索达 2.3 亿元。

网络数据的快速发展在为人们带来便利的同时，也为人们带来诸多新的安全风险。信息安全问题既会为用户和企业带来经济损失，也会威胁到社会稳定与生命安全。因此，数据的安全管理显得非常重要。本文希望通过分析信息安全管理，找寻合理、高效的技术和管理措施，以便预防数据勒索、窃取、泄漏等，保障用户和公司信息的安全，避免公司的利益遭到威胁和破坏。

### 1.1.2 研究意义

在探寻大数据运用方法的过程中，M 公司非常重视信息安全管理。将信息安全作为根本要求，在满足根本要求的条件下，充分运用大数据来推动公司发展。2018 年至今，M 公司持续改进和提高系统安全性。通过信息安全计划的不断改进，迎合日益变化的信息安全风险和创新业务发展需求。

通过本课题的分析与研究，掌握有关经验和知识，并对照系统业务情况，探寻与 M 公司当前发展情况相匹配的信息安全管理措施。在数据审计、数据加密、细粒度授权等技术支撑下，防范信息安全事件的出现，规避此类事件带来的不良影响，与此同时，还可为公司防范信息安全问题积累一定经验，并为数据应用市场的发展提供些许帮助。

本文结合数据概念特征，分析 M 公司的数据运用状况，掌握公司现阶段面临的信息安全风险，并在识别信息安全风险的同时，落实信息安全治理和防范策略，进一步提高公司的信息安全运营能力，加强相关治理水平，强化管理力度，这些都具有非常强的启示和借鉴意义。对于传统企业而言，其安全诉求中的信息安全地位非常重要，通过分析信息安全既有利于传统企业掌握安全防范中的核心要点，又有助于提升信息安全管理水平，进而达到强化信息安全防范意识的目的。

相比于国外而言，我国的信息安全理论探索发展较晚，所以本文的探索对相关理论的丰富有着极大帮助。因此，本文将以实际案例为基础，结合信息安全能力成熟度模型，探索如何通过信息安全标准来进行信息安全风险的识别，并达到强化信息安全能力的目的。

## 1.2 国内外研究现状

在社会和全球经济快速发展的背景下，数据的作用及其产生的影响也开始从“量”向“质”方向转变[1-2]。在信息时代下，数据属于形式化表示信息的外在体现，人工智能、云计算和物联网的广泛应用加快了数据的发展与应用，所以大数据也随之诞生。大数据不仅拥有形式化信息载体的数据属性，而且还

可利用其对新知识和新信息进行挖掘，应用机器学习和统计分析等方法和技术发挥出其发掘作用，因互联网应用较为广泛，积累了大量信息，所以大数据的挖掘功能也代表其具有无限潜能[3-4]。2020 年，我国颁布了《中共中央国务院关于构建更加完善的要素市场化配置体制机制的意见》，其中明确指出，我国要加强对数据的重视力度，将其提升至和技术、资本、土地等并列的地位，即数据成为了新型生产要素[5-6]。在新时代背景下，数据逐渐成为生活生产的重要支柱，信息安全性也成为了保证国家安全、社会稳定和经济发展的基础[7-8]。在国际数字化转型竞争中，为了能够抢占战略先机，并为健康有序发展数据新兴产业营造较好的发展环境，世界各国开始积极创建公民隐私保护和信息安全立法，同时陆续制定了一系列相关规范标准和政策法规，要求企业需要严格根据相关规定保护数据，并注意保证数据合规性。

### 1.2.1 国外研究

在业务变化和技术变革的环境下，开始调整了法律合规要求，国外在 2009 年左右开始调整了原本的信息保护焦点，由最初的保护基础设施和边界发展为保护数据。与此同时，相关法案和制度日益增多，诞生了诸如加利福尼亚参议院 1838 条例、欧洲联合数据指引等相关法律文件，并且制定了行业标准如支付卡行业信息安全标准等，标志着各国开始重视信息安全。此外，在发展外包业务后，欧美地区选择去标识化数据等方式来保护数据，从而提高信息安全性。

（1）研究信息安全识别

近年来，移动互联网、大数据技术等得到快速发展，国际上在 2010 年后出现了很多分析和研究移动互联网、大数据平台中信息安全问题的学者，同时取得了一定研究成果[9]。美国是信息安全管理思潮和全球信息数据的发源地，相关领域研究和发展在国际上也较为领先，在企业管理体系和信息安全方面同样如此，且其研究成果拥有更高的详实度，因此在探究信息安全管理期间可以参考其研究成果。现如今，在信息安全管理领域研究中，研究内容主要包括下述几点：其一，基于大数据对信息安全管理进行研究；其二，信息安全管理方法和模式；其三，分行业信息安全管理和行业信息数据；其四，识别信息安全风险[10]。

英国 R.Brown 与 A.Lin 对 CDSA（通用信息安全架构）和 RBAC（角色访问控制）进行分析后，表示可以应用角色赋值策略和 KPI，并强调 PDL（安全策略语言）的引入也有利于强化传统信息安全访问控制能力[11]。

S. D. Hennessy（2013）对数据进行研究后，成功创建了以数据为中心的安全模型，表示该模型可以保护信息安全和隐私的作用，在研究过程中将数据划

分为三类，包括业务价值、处理程度和使用许可范围，最后从策略、角色控制和数据分类这几方面入手保证信息安全[12]。

2015 年，Mohammad Ahmadi 在国际会议中指出，在对云计算进行处理时，可以选择独立中间代理服务器进行数据保护、访问控制和用户授权等工作，强调在应用非对称加密算法 RSA 和对称加密算法 AES 进行信息交换时，又或是服务器在面对不可预测和可能共计的安全事件时，抵抗能力也会有所提升[13]。Archana R A 等三名印度尼西亚学者研究后表示，在大数据处理中，优化后的遮罩法可以取得较好的效果，相比于传统方法而言，该方法和空间利用率、执行空间具有一定联系，因此大数据平台应用该方法有利于提高自身安全性[14]。

Homer（2016）等人为了对信息安全风险等级和程度进行划分和识别，探究了企业信息安全和信息管理效率二者的平衡点，且在研究过程中创建了专门的信息安全控制应用情景框架[15]。

Rhee（2016）等人对新型信息安全风险处理和识别系统进行分析时，重点探究了其信息安全问题，并将该系统功能归纳为下述几点：第一，风险信息处理；第二，信息安全风险评估；第三，信息安全风险识别和发现[16]。

Niekerk（2021）等人研究后表示，企业在信息安全管理中，要注意考虑其带来的经济效应，确保企业预期资金可以满足安全防护和安全管理基本需求，避免因忽视经济因素而导致支持超出预算，如为了取得更安全的管理方案降低风险而不断增加投入[17]。

（2）研究各行业信息信息安全管理

Solms（2017）等人分析了美国数据处理情况，发现其政府在处理信息期间应用了“大数据研究和开发计划”，并表示其对国土安全起到强化效果[18]。

Hovden（2018）选择了案例分析法对游戏产业信息安全进行了分析，研究结果显示，该行业面临较大的信息安全风险隐患，并将其原因归纳为下述几点：第一，软硬件自身蕴含的安全风险；第二，互联网带来的威胁；第三，多样化的互联方式导致信息安全性存在较大差别，即互联通讯在互联网条件下面临较大安全威胁；第四，一些视频游戏通过收购其他企业扩大自身规模，在收购融合期间因系统融合不充分而面临信息安全风险[19]。

Solms（2020）对数据用户进行了分析，在分析过程中，主要借助挖掘应用程序研究了数据决策者、数据挖掘者等四类用户，重点研究了各类用户保护敏感隐私和用户隐私方面的问题，并给出了相应的应对方案[20]。

Santos（2020）等人选择了电力行业为研究对象，从防御网络信息安全角度入手对 IPFIX 传输、Net-flow 传输这两种数据传输方式进行了系统性分析[21]。

（3）研究信息管理模式与管理法

Rees（2016）等人研究后表示，各类网络攻击密切相关，具有明显的彼此依存关系[22]，Rezgui（2018）等对企业信息安全进行分析后表示，可以将贝叶斯与攻击图二者相结合，从而取得更好的评估效果[23]。

Dantu（2019）等人在计算企业攻击概率期间应用了贝叶斯网络，主要从信息安全管理员和企业数据层面出发，合理调整了企业原本安全设备部署和安全策略[24]。

Solms（2019）等人对安全事件入侵前后的变化情况进行分析后，表示可以用逻辑关联报警管理法来提高企业信息安全，即企业信息安全管理者可以借助警报信息来加强企业核心业务安全的保障力度，避免企业出现核心数据泄露情况[25]。

Gupta（2020）等人研究后表示，组织管理是影响信息安全的主要因素，认为信息技术、人力资源和组织结构是企业风险的主要来源，因此若企业组织结构不完善，则容易影响到相关利益者，从而增加企业信息面临的风险[26]。

Post（2020）研究后表示，人力资源在企业管理中是否发挥作用及其发挥怎样的作用是影响企业信息安全的关键，并表示企业可以从绩效考核、员工配置和企业政策这几方面入手提高企业信息安全[27]。

Von（2020）等人在研究过程中，借助安全评估共计图关联了企业经办，确保企业内部信息安全在受到攻击后，相关管理者可以及时相应并解决，从而降低信息泄露风险[28]。

（4） 研究大数据背景下的信息信息安全管理策略

在大数据背景下，西方部分学者对信息安全和信息信息安全管理进行了具体研究。如 Nosworthy（2019）等人对挖掘隐私数据进行分析后表示，挖掘无需对信息数据进行调节既可获得可执行数据，因此认为挖掘属于较为有效的一种方式[29]。

Venter（2020）研究后表示，为了保障用户敏感信息，可以开发安全可靠的信息共享协议，同时应用内联分析技术如 SQL 等代码，避免因程序员水平或经验无法满足要求而影响用户数据判断结果[30]。

### 1.2.2 国内研究

国内一些学者在研究信息安全管理时，研究重点和西方类似，同时也具有一定创新，接下来主要对国内研究进行介绍：

（1）研究信息安全管控现状

国务院在 2015 年颁布的《促进大数据发展行动纲要》中强调了数据的重

要性，表示数据逐渐发展为基础性战略资源，大数据也开始影响国家治理方式、社会生活方式、经济运行机制等众多方面，因此保障信息安全具有一定必要性，且其中明确指出可以通过创建安全保障体系的方式来保护信息安全。

刘念（2017）等人基于大数据背景探究了信息安全问题，找出大数据在发展过程中面临的安全挑战后，从管理、应用和存储几方面入手给出了提高大信息安全的方案对策，认为可以通过控制权限、统一认证身份、分离加密数据和密钥等方式来提高信息安全性[31]。

娄策群（2018）等人对企业信息安全管理现状进行分析后，认为可以将下述几点作为管理重点：其一，贯彻落实应用信息安全管理体系，对过程模型进行细化的同时，制定具体实施方案；其二，创建云安全体系框架和信息安全管理体系[32]。

丁先存（2018）研究后认为，企业在信息化时代背景下可创建信息安全体系，并表示现代企业要综合考虑外部环境和内部发展情况来创建安全体系，确保其和企业实际发展相符，不得盲目照搬[33]。

王长全（2019）主要从网络环境方面入手对现代企业信息安全现状进行了分析和讨论，研究结果显示，审核信息安全管理体系、创建安全管理体系框架等有利于保障企业信息安全[34]。

樊如霞（2019）对国内外信息安全管理进行梳理归纳后，根据所得结果给出了企业信息安全管理此后研究方向[35]。

王越（2020）等人分析了企业在互联网环境下信息安全管理现状，并分析了其在机密性和完整性方面面临的问题，最后根据分析结果给出了相应的优化方案[36]。

（2） 研究企业信息安全评估管理

尹淋雨（2015）选择了理论与实践相结合的方法，探究了企业创建安全评估指标体系现状，并在技术层面、管理层面和人员层面给出了加强信息安全评估管理的方案对策[37]。

汤淼淼（2016）研究后表示，可以根据实用性原则、系统优化原则和科学性原则等五个主要原则来创建信息安全评价体系，这样得到的评价体系更为合理，在实践中的应用效果也更好[38]。

杨洋（2016）主要从技术层面、人员层面和环境层面入手，分析了企业信息安全评价机制的创建情况，并在此基础上根据现代企业基本特点给出了相应的保障方案[39]。

孙红梅（2017）、王刚（2018）等人得到的研究结果相同，认为企业可在管理和技术的支持下，创建与企业自身相符的信息安全管理体系，为保证该体

系的应用效果，确保安全体系涵盖风险信息库模块、监测预警模块、目标管理模块等八大模块[40-41]。

杨鑫（2019）根据云平台内涵和技术手段，将入侵系统分为模块检测和异常入侵检测两类，为企业加强信息管理提供了一定参考[42]。

王大康（2019）研究后表示，可以从物理环境、系统建设运行和组织结构等方面入手对企业信息危险进行探究，并强调上述内容也属于企业评估管理的重要内容[43]。

江和平（2020）研究后表示，现代企业信息安全管理主要体现在两个层面，即信息安全管理标准和信息安全管理框架，并强调可以通过创建信息安全管控体系框架的方式加强对信息安全的管理力度，从而降低企业面临的信息安全风险[44]。

（3）研究各行业信息安全管控

凌捷（2015）选择高新技术企业为研究对象，分析了这类企业应对信息安全风险时的措施，他发现，由于高新技术企业特征，致使这类企业往往会出现海量数据，且这些信息的结构非常复杂，这导致信息管理难度大幅上升[45]。

陈左宁（2017）通过相关研究发现，在信息安全评估机制上，一些国有企业并不完善，这些国企需要从自身角度出发进行信息的合理划分，并针对不同信息实施差异化管理[46]。

李晓康（2018）等人以大型火电企业为研究对象，通过分析这类企业的信息安全管理现状发现，这类企业在管理时都是以 ISO27001 体系要求为根本建立相关的管理机制，且系统将随着实践不断改进，最终构成四位一体模式，即数据容灾、日志、人员风险、机房设备的四位管理[47]。

冯登国（2019）等人通过分析发现，现代企业面对的信息安全风险非常多，他认为，防范信息安全风险可通过构建安全管理框架来实现，其内容主要包含三方面，即技术保障机制、制度保障机制、组织保障机制[48]。

潘烨（2020）认为，一旦出现客户隐私泄露的现象，客户的财产和信息安全都将受到威胁，这时降低的还有企业信任指数，进而对企业经营发展产生一定影响[49]。

（4）研究大数据背景下的信息信息安全管理策略

随着大数据时代的到来，企业信息安全保障显得越发重要，而企业信息安全水平的提升则需从完善管理制度、深化法律法规、强化安全防护等方面出发[50-53]。

祝利锋（2015）通过深入分析发现，在海量数据的挖掘中，优选分布式架构非常重要，其认为信息安全保障可分为三个方面，即管理安全策略、应用安

全策略和储存安全策略[51]。

刘静芳（2016）通过分析发现，如果想要大数据时代下确保信息安全，既要构建信息安全管理系统，又要改进现有法律法规体系，进一步强化违法的处罚力度[52]。

宗文萍（2017）通过研究发现，大数据时代下的企业信息安全防范核心在于五点，即大信息安全、系统平台运用、网络安全、网络边界和系统终端[53]。

王建红（2018）通过调查发现，大数据时代下的企业信息安全与否主要取决于企业是否建立并完善云平台会计信息系统，完善的共享平台既能提高数据加密水平，又能保证高独立性和制度统一[54]。

张丽（2019）认为，大数据的安全防护可从两方面出发，一方面是审计管理，另一方面是访问控制[55]。

杨海平（2020）等人在《大信息安全标准现状和思考》一文中提出，我国是在遵循“关注重点、成熟先上、紧急先行”的原则下，对照《网络安全法》来制定信息防护标准，即《信息安全技术个人信息安全规范》，并加快大数据平台中的相关技术标准制定进度[56]。

### 1.2.3 文献评述

通过国内外的相关研究可知，在信息安全管理上，主要是从管理体系、技术体系、人员组织这三方面出发，满足敏感数据管理和信息安全保护的要求，而其核心理念主要包含三点，即场景化安全、角色收取那和分类分级[57-60]。建设信息安全时，通常都是按照构建组织、梳理资产、制定计划、控制流程、监管行为和不断完善的步骤，其目标是“激活数据，提高价值，让数据运用更为高效”。

企业信息安全管理最早是由美国学者所提出的，美国是目前世界上信息安全管理水平最高的国家，既有强大的信息安全管理技术，又有先进的信息安全管理经验，所以美国的相关成果可作为其他国家探索的重要经验。现阶段，在企业信息安全控制方面，西方学术界的探索成果众多，这些探索成果可作为我国学术界探索的根本。随着大数据的快速发展，国内的信息安全管理手段日新月异，探索层面也越发广泛。一些学者在相关论题的探索上是从企业信息安全角度出发，具体方向主要分为四大层面，即大数据时代下的信息安全与信息数据管理、各行业信息安全管控措施、企业信息评估管理对策、信息安全管控现状及问题分析，且随着探索的不断深入，细化程度也越来越高。然而当前的探索成果大多停留在理论层次，在信息安全管理的探索上，以某一企业为调查对象的研究少之又少，尤其是从某企业实际情况出发进行探索的更是非常少，故

而本文的研究仍需不断加强。

## 1.3 研究方法和论文框架

### 1.3.1 研究方法

近年来，学术界内开始兴起一阵探索信息安全的热浪，通过归纳和阅览信息安全管理文献，结合木桶原理、PDR 安全模型、数据安全能力成熟度模型和 ISO27000 信息安全管理体系标准等理论，以 M 公司为例，分析该公司信息安全管理状况，并根据现有问题提出合理的改进方案计划。本文分析过程中用到的研究方法主要如下：

第一，文献分析法：笔者通过知网、万方等文献搜索渠道搜索一些与本课题相关的文献，了解时下信息安全发展近况，为之后 M 公司信息安全管理的深入分析打下坚实的理论支撑，并希望从中找出合理的解决措施。

第二，案例分析法：本文以 M 公司为例，之所以选择 M 公司主要是因为笔者正在 M 公司从事相关工作，对公司的信息安全管理情况了解比较多，且方便搜集相关信息。

第三，图表分析法：本文通过图表相结合的方法，将变化情况和观点更直观的表述出来。

### 1.3.2 研究内容

本文致力于找寻信息安全管理措施，希望通过分析国内外信息安全发展近况和信息安全事件，实现木桶原理、信息安全法规标准、信息安全能力成熟度模型的有机结合。因此，本文以 M 公司为例，深入分析公司当前的信息安全管理策略，并从中找出合理的改进方法与对策，希望能在帮助 M 公司的同时，为数据应用市场的发展也提供一定帮助。

本文的研究内容具体如下：

第一章，绪论。本章重点介绍了课题研究背景、目的和意义，之后列举了国内外在信息安全管理上的探索成果，最后介绍了文中运用的研究方法和本文主要内容。

第二章，概念与理论基础。本章首先介绍了信息安全的有关概念，之后又详细介绍了文中运用的相关理论，如木桶原理、PDCA 循环理论、信息安全能力成熟度模型等，为下文的分析打下坚实的理论支撑。

第三章，M 公司信息安全管理现状和问题分析。本章是以 M 公司为例，首先分析了公司信息安全管理现状，之后从中找出公司存在的管理风险，最后列举出相关问题。

第四章，M 公司信息安全管理方案设计。本章针对上一章的问题提出合理的解决措施和方案，之后根据公司的实际情况提出具体的方案设计。

第五章，M 公司信息安全管理方案保障措施与预期效果。本章首先提出了有助于方案计划落实的保障措施，之后对本文提出的方案计划效果进行验证。

第六章，结论与展望。本章是对全文的总结与归纳，找出全文结论和创新点，并指出文中存在的不足之处和未来深入探索的方向。

如图 1-1，是本文的技术路线图。

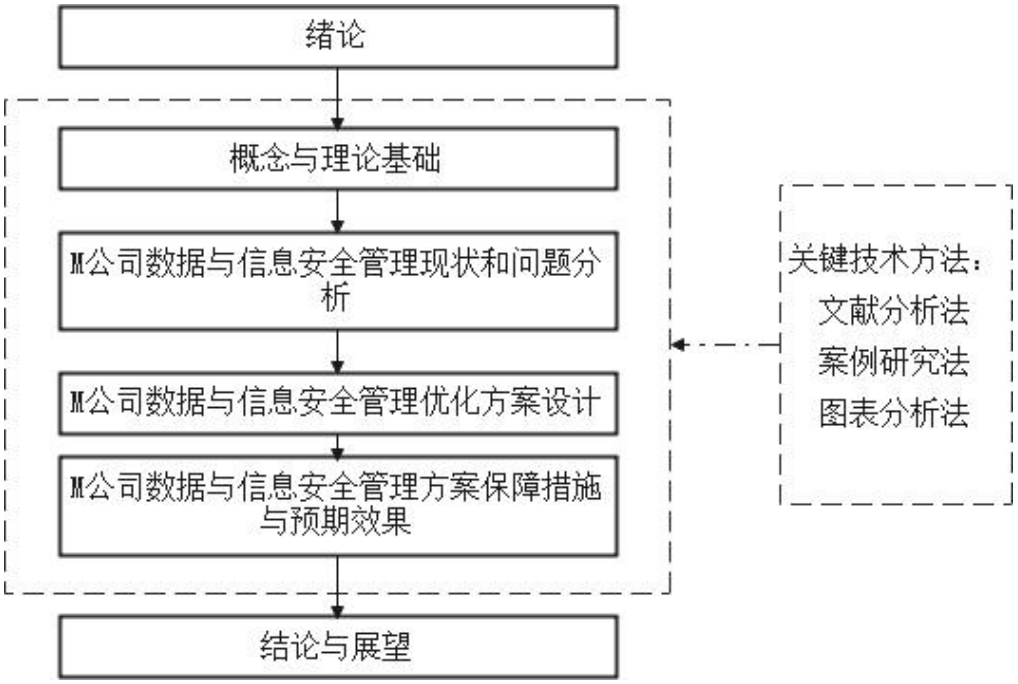


图 1-1 技术路线图

# 第 2 章 相关概念与理论基础

## 2.1 基本概念

### 2.1.1 数据相关概念

（1）电子数据

电子数据通常指的是如数字图像、数字音频等内容，是以连续或不连续形式和离散形式呈现出来的，这类二进制数字格式信息往往是由真实世界信息转换而来。

（2）数据生命周期管理

所有数据都有之生命周期的存在，阿里提出的信息安全成熟度模型中指出，销毁、存储、传递、使用、获取、创建这六步一同构成了一个数据生命周期。因此，想要分析是信息安全管理，那么就需要从数据生命周期入手。如图 2-1，是数据生命周期闭环图。


图 2-1 数据的生命周期

### 2.1.2 安全相关概念

（1）信息安全

在确保信息安全的条件下，对数据的机密性、完整性和可用性予以保障。

（2）安全策略

为实现网络安全目标，而提供的可防护网络安全的手段和措施即为安全策略。

（3）信息安全能力

在人员能力、技术工具、制度流程、组织建设等方面上，组织机构拥有的信息安全保障能力。

（4）能力成熟度模型

可衡量某组织机构的成熟度模型，其中包含了可代表进展与能力的模式、指示和属性等指标。一般都是通过实例开表述模型内容，本模型可为组织机构提供一个用于衡量当前能力水平的标准，并确定优先级与最终目标。如果某一特定行业中开始广泛运用本模型，那么这个行业中的组织机构成熟度就可用本模型进行评估。

（5）数据脱敏

由于是以模糊化等方法来处理原始数据，所以可通过敏感信息的屏蔽来保护数据。

（6）合规

所有数据都要遵循的法律法规。

（7）数据安全

是指通过采取必要措施，确保数据处于有效保护和合法利用的状态，以及具备保障持续安全状态的能力。

## 2.2 相关理论

本节重点介绍了信息安全管理的有关理论，参照国内外文献成果制定了本文接下来分析的理论框架。在信息安全管理过程中，能力成熟度模型主要起指导效果，确保整个管理全面而合规；木桶原理、PDR 安全模型等理论主要用于改进现有理论，并在此基础上，不断优化现有的管理措施与手段；基于上述理论和文献成果，对照 M 公司当前的发展情况和有关问题，从 M 公司实际角度出发，构建一个以数据为核心的安全管理体系。

### 2.2.1 信息安全能力成熟度模型

大数据时代下的企业都是以数据作为主要资产之一，所以数据的价值随着企业重视程度的提升而提升，其资产保护也就变得越发重要。正因如此，在阿里的牵头下，国内 27 家企业与研究机构一同提出了信息安全能力成熟度模型（简称 DSMM 模型），并交付信息安全标委会进行审核。本模型是以 CMM 模型为基础，结合阿里的数据域信息安全管理经验所建立的，只要组织机构存在信息安全管理需求，那么都可适用于本模型。

DSMM 模型标准指出，由于各组织发展状况有所差异，所以在 DSMM 模型使用过程中要根据实际情况做出相应调整，即根据标准规范和方法来开展信息安全管理工作。除此之外，DSMM 模型标准还涵盖了《信息安全技术个人信息安全规范》、CMMI 模型和信息安全生命周期框架等部分内容。

通过图 2-2 可知，DSMM 模型主要分为三个维度：第一维度，能力成熟度等级。这个等级主要分为五级，由上到下分别是五级的持续优化、四级的量化控制、三级的充分定义、二级的计划跟踪和一级的非正式执行。第二维度，数据生命周期安全。这一维度主要分两个层次，一个是生命周期各阶段安全，另一个是通用信息安全。第三维度，安全能力维度。这一维度主要包含四方面内容，即人员能力、技术工具、制度流程和组织建设。

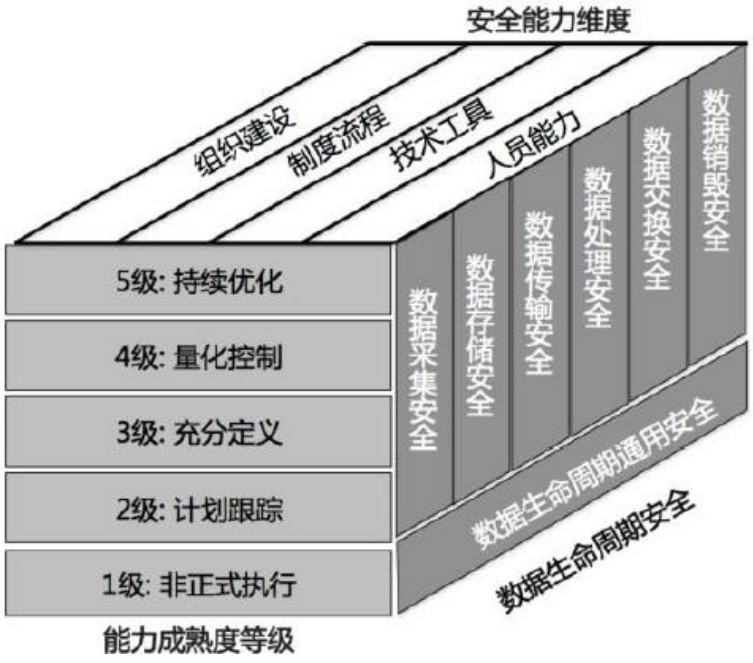


图 2-2 信息安全能力成熟度模型

如图 2-3，是 DSMM 模型下的数据生命周期各阶段安全内容。


图 2-3 数据生命周期各阶段安全

整个数据生命周期可划分为 6 个阶段。从安全定义角度来看，生命周期可分为两部分，一个是生命周期各阶段安全，另一个是生命周期通用安全。

根据 DSMM 模型要求可知，信息安全能力成熟度包含两方面，一方面是数据生命周期阶段基本实践，另一方面是数据生命周期安全通用基本实践。一般在安全能力的衡量上主要通过四大维度来完成，即人员能力、技术工具、制度流程和组织建设。

### 2.2.2 PDCA 循环理论

PDCA 循环理论最早出现在上世纪，是由美国学者休哈特所提出的，之后又由美国学者戴明引用到质量管理领域之中，故而 PDCA 循环又常被称作是戴明环。PDCA 循环是“计划—执行—检查—处理”的英文缩写，这一模型是以这四大要素为基础，整个过程循环往复。第一步，对本阶段质量问题进行收集，找出引发问题的相关因素和原因，并根据问题诱因提出针对性解决措施；第二步，根据解决措施开展相关工作；第三步，检查措施落实后的所获成效；第四步，归纳整个过程经验，并制定新标准，对未达预期效果的问题，可转入下一循环阶段中进行探索与分析。

### 2.2.3 PDR 安全模型

PDR 安全模型最早出现在上世纪 90 年代，是由美国国防部所提出的，是“保护—检测—响应”的缩写，这一多环节保障体系是以这三大要素为基础，由于其动态控制理念和闭环的稳定性，让该模型获得了飞速发展。进入 20 世纪之后，本模型中又引入了两个重要部件，一个是恢复，另一个是策略，截止到这时，整个模型开始以安全策略为核心，通过专业检测软件、ID 访问控制措施、防火墙等手段，系统入侵行为进行管控，并评估管理系统的实时安全情

况。上述的一系列操作和行为，代表以主动防御和闭环控制为根本的动态安全模型正式构成。

### 2.2.4 木桶原理

美国学者皮得率先提出了木桶原理，是指木桶能盛多少水主要由木桶中最短的木板来决定，所以这个理论也常被称作是短板理论。一般管理学中常用木桶原理解决一些实际问题。本文在分析 M 公司信息安全管理时，引入木桶原理，即从安全防护的各方面出发制定合理的防护措施。

### 2.2.5 信息安全管理体系标准 ISO27001

ISO27001 是在 2005 年由国际标准化组织颁布的一个针对信息安全管理体系的国际标准，是 ISO27000 标准族的一部分。2013 年 10 月国际标准化组织对旧版标准进行首次改版，新标准去掉 9 点控制措施，新增 17 点控制措施，并重组部分控制措施而新增一章，重组部分控制措施，关联性逻辑性更好，更适合应用；并修改了部分控制措施措辞。并推出信息安全管理体系标准新版本，命名为 ISO/IEC 27001:2013，一般简称为“ISO27001”。

作为信息安全领域认可度最高的信息安全管理体系标准，ISO27001 强调以安全控制点的方式来达到信息安全管理的目的，共涵盖了 14 个安全领域，35 个安全控制目标，114 个安全控制措施，标准包括 11 个章节：

（1）安全策略。指定信息安全方针，为信息安全提供管理指引和支持，并定期评审。

（2）信息安全的组织。建立信息安全管理组织体系，在内部开展和控制信息安全的实施。

（3）资产管理。核查所有信息资产，做好信息分类，确保信息资产受到适当程度的保护。

（4）人力资源安全。确保所有员工，合同方和第三方了解信息安全威胁和相关事宜以及各自的责任，义务，以减少人为差错，盗窃，欺诈或误用设施的风险。

（5）物理和环境安全。定义安全区域，防止对办公场所和信息的未授权访问，破坏和干扰；保护设备的安全，防止信息资产的丢失，损坏或被盗，以及对企业业务的干扰；同时，还要做好一般控制，防止信息和信息处理设施的损坏和被盗。

（6）通信和操作管理。制定操作规程和职责，确保信息处理设施的正确和安全操作；建立系统规划和验收准则，将系统失效的风险降到最低；防范恶意代码和移动代码，保护软件和信息的完整性；做好信息备份和网络安全管理，

确保信息在网络中的安全，确保其支持性基础设施得到保护；建立媒体处置和安全的规程，防止资产损坏和业务活动的中断；防止信息和软件在组织之间交换时丢失，修改或误用。

（7）访问控制。制定访问控制策略，避免信息系统的非授权访问，并让用户了解其职责和义务，包括网络访问控制，操作系统访问控制，应用系统和信息访问控制，监视系统访问和使用，定期检测未授权的活动；当使用移动办公和远程控制时，也要确保信息安全。

（8）系统采集、开发和维护。标示系统的安全要求，确保安全成为信息系统的内置部分，控制应用系统的安全，防止应用系统中用户数据的丢失，被修改或误用；通过加密手段保护信息的保密性，真实性和完整性；控制对系统文件的访问，确保系统文档，源程序代码的安全；严格控制开发和支持过程，维护应用系统软件和信息安全。

（9）信息安全事故管理。报告信息安全事件和弱点，及时采取纠正措施，确保使用持续有效的方法管理信息安全事故，并确保及时修复。

（10）业务连续性管理。目的是为减少业务活动的中断，是关键业务过程免受主要故障或天灾的影响，并确保及时恢复。

（11）符合性。信息系统的设计，操作，使用过程和管理要符合法律法规的要求，符合组织安全方针和标准，还要控制系统审计，使信息审核过程的效力最大化，干扰最小化。

# 第 3 章 M 公司信息安全管理现状和问题分析

## 3.1 M 公司概况

M 公司始建于 2001 年，是一家以超材料为主营业务的军民融合的上市公司，其分别在港股和深圳 A 股上市，公司生产的超材料主要用于穿戴式智能装备和尖端装备等领域。

在超材料领域上，M 公司的产品优势非常明显，一直处于尖端装备领域的领先地位，且呈现出规模化、持续性的发展态势。截止到 2020 年末，在超材料业务方面，公司实现了 13,859.76 万元年营收，相比去年上涨了 125.98%，约占合并营收的 61.46%，与去年相比上涨了 30.53%。其中，1,574.30 万元来源于超材料开发业务，相比去年上涨了 143.87%，而在研发项目上，与去年相比上涨了 105.56%；12,285.46 万元来源于超材料营销业务，相比去年上涨了 123.87%。由于公司在未来 5 年将进入大批研发产品交付阶段，所以公司营收规模将大幅提升，届时超材料业务也将呈现出逐年递增的态势。

在专利申请上，M 公司共有 107 项，其中 65 项为发明专利，且荣获 55 项授权，同时作为主编单位的 M 公司，其参与的国家标准实施活动还有 2 项。M 公司近年来完成了超材料设计超算中心的扩建，实现仿真计算效率的进一步提升，并在提高研发效率的同时，为高难度、超复杂的仿真计算打下坚实基础。

M 公司数据中心存储的是一些非常重要的信息，如超材料仿真计算、人资数据、办公文档、生产数据等，全部数据总量约为 5.26PB。超材料仿真数据为超材料的研发提供强有力的保障，这些数据一旦被窃取、盗用、或恶意破坏，将关乎着公司发展与生存，甚至对国家安全带来影响，所以要进一步提升公司信息安全的防护，以防出现数据勒索、窃取、泄漏等情况，保障公司信息安全。

## 3.2 M 公司信息安全管理现状分析

### 3.2.1 公司组织架构现状

现阶段，M 公司的信息化建设主要由流程与 IT 中心负责，其内容主要包含公司信息化的建设，如 ERP、OA；网络、服务器、终端的日常维护；公司网络安全、信息安全和数据安全的建设。在流程与 IT 中心之下，又建立了安全组、网络架构组、开发组等多个小组。其中，安全组负责内网终端、业务系统、服务器、公司网络的安全事宜。当前，流程与 IT 中心共有员工 40 人，具体结构如表 3-1。

表 3-1 流程与 IT 中心人员职能人数分布

| 序号 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
|---|---|---|---|---|---|---|---|---|---|
| 角色 | 总监 | 安全经理 | 安全工程师 | 研发经理 | 研发工程师 | 运维经理 | 网络工程师 | 服务器工程师 | 桌面工程师 |
| 人数 | 1 | 1 | 5 | 1 | 10 | 1 | 5 | 6 | 10 |
| 比例 | 2.50% | 2.50% | 12.50% | 2.50% | 25.00% | 1.25% | 12.50% | 15.00% | 25.00% |

现阶段，公司的安全事项都由安全组负责，并由之负责落实小组中的绩效考核和界定岗位工作内容。

### 3.2.2 信息安全制度流程现状

M 公司的信息安全管理制度是安全组根据 ISO27001 标准建立的，主要用于管理公司内部信息安全。在信息安全上，公司安全组只制定了一些管理办法，并未构建完善的管理制度。

### 3.2.3 信息安全技术工具现状

在信息安全防护上，M 公司的有关工具非常少，目前主要通过防火墙来防范网络层中的外部供给，并拦截一些恶意流量。除此之外，公司还将 DLP 系统引入到网络层中，以此检测由外网流出的数据中心是否有公司核心数据，如若发现流出的核心数据尚未被公司批准，这时可通过 DLP 系统来进行实时拦截。

在办公终端上，M 公司又引入了防病毒系统，以此对终端恶意代码进行拦截。此外，公司还建立了一个终端管理系统，用于终端的远程运作与维护和日志审计，并加密终端上的重要文档，以防出现公司重要文档在未获审批的情况下外流。

### 3.2.4 信息安全人员能力现状

安全组人员能力主要凸显在三方面，即渗透测试、信息安全、网络安全，尚未招入一些以安全数据为主要专业的人才。由于数据安全是近年来刚刚兴起的一门课题，所以市场中的人才培养体系尚不完善，致使一些相关领域的人才都是处于自学状态，希望以此来提升个人信息安全能力。

## 3.4 M 公司信息安全管理存在问题分析

对于信息安全管理而言，其影响因素通常来自各方各面，如安全人员能力有限，业内并无成功经验、安全建设需求资金庞大、领导重视力度不足等，这些问题的存在都已引发信息安全防护建设问题，进而威胁到信息安全。在信息安全防护技术的探索上，我国学术界正处于摸索阶段，各类防护产品的效果并不高，所以想在市面上找到与 M 公司发展情况相契合的信息安全产品非常难。

### 3.4.1 组织结构不合理

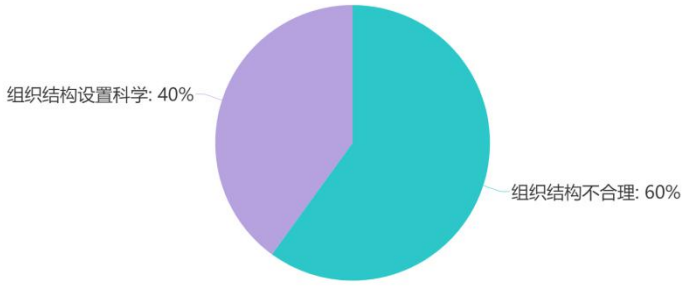


图 3-1 员工对信息安全管理组织结构态度

通过访谈（见附录）以及公司内部匿名统计数据可知，有 40%员工认为目前公司信息安全管理组织结构合理，能够很好的完成信息安全工作安排。但是 60%认为目前组织架构存在一些不足之处：通过分析公司组织结构发现，安全组是置于流程与 IT 中心之下，可见公司对安全组的重视力度并不高，这极易导致在建设项目过程中出现资金投入力度不足的情况。除此之外，M 公司内部也并没有一名专业的信息安全人才，现有一些安全人员都是“半路出家”，并未接受过专业培训。事实上，M 公司当前要将安全组提升到和流程与 IT 中心同一等级上，由公司总经理直接负责，如此才能更好的落实安全管理工作。

在信息安全管理上，M 公司虽然建立了一些相关制度，并加强了全体人员的重视程度，同时也引入了加密电子证书，但是尚未制定身份认证信息与交易信息的保护机制，由于缺少相应的保护机制，导致公司目前仍旧受到信息安全风险的威胁。故而，公司当前急需进一步完善信息安全管理机制。

### 3.4.2 信息安全管理制度不科学

一般来讲，透明化的信息安全管理既有利于资源的充分利用，又有助于安全防护水平的进一步提升，同时对“挂一漏万”现象的规避也有着很好的帮助。

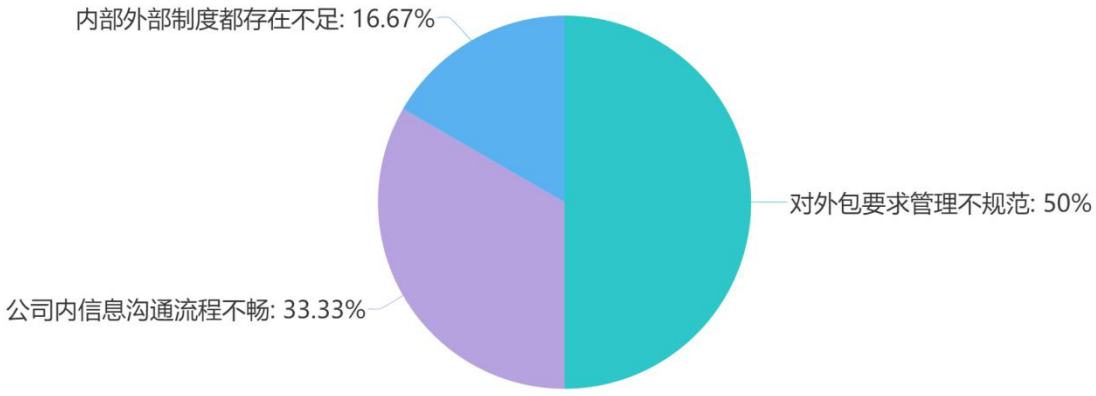


图 3-2 员工对信息安全管理制度态度

通过访谈结果可知，有 50%员工都提到项目中存在资质良莠不齐的外包服务商导致安全管理存在一些不足，33.33%认为是内部沟通导致信息安全管理工

作不理想，但是 16.67%员工认为除了客观存在的资质良莠不齐的外包服务商，内部沟通也是妨碍信息安全管理工作顺利进行的原因之一。具体公司内部目前组织架构存在的不足之处：

（1）对外包要求管理不规范

目前，M 公司虽然制定了一系列规章制度，并实施了多项认证机制，如信息管理流程认证、信息安全管理认证等，但是由于实际工作下的工作人员信息安全管理水平有所差异，导致管理工作上仍旧存在一些不足之处。近年来，随着我国航空业的快速发展，公司所获经济效益越来越高，但在快速发展的过程中不可忽视监督管理、制度建设等方面的工作，公司要在未来发展中不断探索与改进相关制度。因此，在系统项目的建设过程中，其外包表现具体如下：

在信息化建设方面，近年来的 M 公司虽然投入了非常大的物力、财力和人力，且由 IT 审计部负责考核信息安全工作的各项事宜，但是日常工作下的一些员工为了完成绩效目标，常忽视系统功能要求，导致一些项目开发的执行力度严重不足。在项目开发过程中，虽然乙方会根据安全管理现状提出其中存在的问题，并给出合理的解决措施，但在面对上述问题时，M 公司积极性明显不足，在处理问题时也经常选择治标不治本的处理方案，并且缺少能力制定、推行和检查信息安全管理体系、流程与制度等，导致上述问题一直无法得到根本解决。

目前，M 公司基本形成了完善的信息安全管理制度和体系，然而进一步分析可以发现，项目中还存在资质良莠不齐的外包服务商。从国内现行法律来看，关于信息安全管理方面的法律条例并不完善，缺少明确的信息安全监管制度和健全的 IT 行业安全风险评估标准，需要公司自身制定信息安全风险评估方案。与此同时，M 公司还缺少有效、专业的信息安全审核和网络安全监管，仅凭公司有限的信息安全监管人员取得的监管效果有限，若要追溯信息安全原因对技术也具有较高的要求，而在无法有效执行信息安全流程、制度和体系的环境下，犯罪成本却相对较低。在上述因素的影响下，容易出现个别员工或外包公司在个人利益的驱动下，非法获取 M 公司机密信息和数据，这种行为不仅会威胁公司安全，而且还会为国家带来安全隐患。

在公司经营发展中，公司具有明显的逐利性特点，所以在开发系统过程中也会将盈利能力作为考虑重点，即在开发期间加强对开发成本的控制力度和降低自身风险等。如选择服务转包、压缩项目开发人员等方式完成部分项目，在此过程中，公司面临的信息安全控制和管理风险与压力也会随之增加。在 IT 管理流程中，M 公司对实施和操作日常运维较为关注，在运维操作具体管理和控制等方面却并不完善，一些系统管理员在管理中并未严格根据公司规定流程

开展工作，忽视了服务外包、第三方风险评估重要性，同时并未制定监督控制方案，导致一些外包供应商资质不全，第三方能力不足，最终影响到项目安全和质量，未能实现预期开发目的。

（2）公司内信息沟通流程不畅

M 公司经过不断发展后，公司发展规模和部门数量较多，在日常工作期间，员工需要在遵守公司相关规章制度的同时，也要遵守部门内部要求。在开发采购管理平台系统过程中，需要 IT 部、人事部和采购部等多个部门共同参与，成立的项目开发小组将使用平台发布、梳理业务流程和实现平台功能作为开发重点，忽视了信息安全问题，所以在开发前期一直缺少信息安全和信息安全管理方面的人员参与其中，在基本完成项目即将上线运行后，信息安全管理部门需要审核系统回复、备份、代码等内容，最终导致无法顺利通过审核。在开发项目期间，M 公司主要从常识和经验入手，给出了多数信息安全漏洞的解决方案，然而对信息安全管理体系仍了解不足，甚至因规划的系统架构和公司规定不符等原因而返工操作。

### 3.4.3 技术工具建设不到位

现如今，在建设信息安全技术防护能力方面，公司还存在一定不足，如在创建期间忽视了数据在各阶段生命周期的安全需求，而是选择蕴含文档加密模块的终端安全管控系统、网络 DLP 和网络防火墙等保护措施来保护公司信息信息安全。事实上，数据各阶段的生命周期特点和需求存在差异，因此为保证保护方案的合理性，可从信息安全能力方面入手，结合成熟度模型制定具有针对性的安全防护措施，并建设组织通用安全系统。具体如下图所示：


图 3-3 信息安全技术工具

### 3.4.4 人员安全意识差

本文在调查过程中，选择匿名问卷的方式调查了 300 多名使用内部信息系统的员工，通过这种方式了解 M 公司员工当前的信息安全意识。本次匿名调查回复率为 21%，共收回 65 份问卷，有效问卷基本覆盖了事业部和全部职能部门。

通过总结归纳问卷内容后，得到了下述结论：

从 IT 人员记录结果中可知，M 公司每月处理的浏览器插件、病毒查杀等工作在十起以上，一些员工认为电脑运行较慢，而出现这一问题的主要原因是员工安装的安全软件数量过多，因软件冲突影响了电脑正常运行。

一些员工好奇心较强，在发现邮箱邮件后点击链接查看，一些员工在办工作文件夹中保存重要工作资料，并未根据公司规定将其放置在专门文件柜中。不仅如此，部分员工在办公期间随意应用移动存储介质，还有部分员工在咖啡厅、公共食堂等公共场合交流公司即将发布的产品和公司项目等。显然，M 公司员工人员安全意识较差，在一定程度上增加了泄漏公司信息的风险。

## 3.5 M 公司信息安全管理存在问题原因分析

### 3.5.1 企业文化对信息安全管理策略的影响

在公司经营发展中，企业文化对其管理方式和经营理念有着决定性作用。从跨文化企业管理可以了解，管理者不同的文化认知容易影响管理策略的实施及其取得的效果，严重时还会带来负面影响。西方跨国公司管理理念融入了人性化，即不仅重视管理制度和企业文化，对人更重视，在制定管理方案期间也会将人性化作为考虑重点。实际上，个体是否能够根据管理制度和企业文化开展工作，更多由其价值观、道德观、自我约束和判断来决定，所以经常在自我约束力强和综合素质高的环境下创建上述管理文化。在当前企业环境中，开始提倡融合原文化，在跨文化管理中体现的尤为明显，若企业管理文化脆弱性较强，仅凭个体道德水平与价值观无法取得预期管理效果，则容易出现危害企业的现象。

M 公司在经营管理中推崇“尊重个人”，且将其渗透到企业各环节。在快速扩展公司业务期间，M 公司一般都是从人员技能方面来选择人才，即注重选拔实用型人才，然而在选拔期间却并未严格审查个体背景和道德，促使选拔的人员素质存在较大落差，在信息安全、内部数据和组织结构不健全的环境下，为滋生人为不利安全因素如机会主义心理等创造了机会，最终威胁了公司业务经营活动安全。

### 3.5.2 内部安全审计管理不规范

审计内部管理行为的匮乏降低了审计作用，现如今，M 公司主要选择内部自查自纠的方式开展安全审计管理工作，而内部审计为内部职能部门，因此内部审计人员在集体利益关系的影响下容易出现默许内部不正当行为的态度，这种审计方式无法保证审计质量，审计作用也难以发挥出来。实际上，公司内部审计部门由管理层领导负责管理，所以无法明确内审工作定位，管理者意志对其工作态度和质量会产生较大影响，促使企业内部安全审计缺乏透明度，权威性与独立性也无法得到保障。M 公司经过不断的发展后，外包服务项目涉及领域较为广泛，对审计人员经验背景、分析能力等方面要求较高，然而从实际情况来看，一些审计人员却并未满足上述要求，如在经验、知识和技能等方面有所不足，企业也并未提供深入的具有针对性的培训，因此独立完成审计工作具有一定难度，审计质量也无法得到保障，最终难以取得预期审计效果和目的，导致审计工作流于形式。

### 3.5.3 技术管理能力薄弱

M 公司近年来增加了在信息技术方面的投入力度，为了加快信息技术的发展，聘用了更多的信息技术员工，负责信息安全管理的员工数量也随之增多。M 公司每年都会开发和升级系统，在工作量和工作难度不断增加的环境下，公

司相关人员却并未及时提高技术能力。与此同时，在公司内部，信息技术管理岗地位并不高，为低级别职位，所以在上报实际工作存在的问题后，容易因审批流程过于繁琐而稀释严重问题，并且公司管理者却并未形成较强的信息安全防范意识，最终导致实际问题无法得到有效解决。此外，公司业务部门与子公司为满足业务要求，在资金、技术和人员等因素的影响下，并未配置信息安全岗，这种管理方式也增加了公司内部资料、信息和数据面临的安全风险。

在开展工作期间，很多因素都影响公司信息安全和信息信息安全管理。

（1）在信息安全组织和策略上，若要保证管理机制的合理性和全面性，则需明确内部审计地位及其重要性，并在重要岗位中加强信息系统审计力度。然而从实际情况来看，因公司并不重视内部审计，所以即便制定的信息安全内部审计规章制度相对完善，执行效果和预期却存在一定差距，一方面，审计范围和审计对象不明确；另一方面，不合理的审计方法影响了审计结果准确性。实际上，M 公司信息安全部门管理也存在问题，如多数子公司并未配备专业人员，无法顺利开展一些工作。子公司在面对总公司发布的信息安全管理工作时，会由专门的人员负责相关工作，却因监督力度不足而无法保障执行效果，即便设立了人员监督工作，监督人员也容易因缺乏信息安全背景而影响监督效果。

（2）IT 固定资产管理。通常情况下，施工项目应向公司申请虚拟机资源、存储空间、网络 IP 等，因管理部门资产清单不全，所以容易出现无备用 IT 资源情形，并且整个申请流程和资源申请时间较长，因此对项目实施进度也会造成较大影响，甚至无法在预期时间内完成项目。

（3）业务连续性管理。从 M 公司当前管理现状可以发现，其在业务连续性管理方面的水平还需进一步提高，在下述几方面体现的尤为明显：

在系统架构上，规划系统架构是开发项目的重要工作，在规划中虽然考虑了冗余备份、单点故障等问题，在管理服务器跨机柜时却并未实现分节点部署虚拟机等，主机房虽然部署应用系统，但是却并未制定 CDN 规划和全作业备份，部分地区访问体验容易受到影响。在开发业务系统上，因公司严格要求开发采购管理平台进度，所以在执行和制定代码编写期间并未做到有效贯彻权限控制和优化数据库结构，在短时间爆发式访问或高峰期访问期间，容易在系统代码层和数据库语句结构、调用关系等因素的影响下，出现应用系统长时间响应的现象。M 公司当前对系统进行了监测，却仅监测了服务器和基础设施，并未有效监控用户体验层和业务程序成，单一的监测手段对监测结果也带来了一定影响，显然并未做到全方位、多系统的综合监测，因此无法通过监测及时发现和解决系统问题。

（4）维护和开发应用系统。在开发和维护采购管理平台期间，还存在下

述隐患：

在收集和分析需求期间忽视了安全因素。具体而言，相关业务部门和开发人员在收集和分析采购管理平台需求期间，未考虑应对恶意访问、恶意代码、身份验证等系统安全问题，促使平台面临的系统安全问题也随之增加。与此同时，在供应商开发系统过程中，M 公司从开始到最终交接，均未制定相应的验收标准和节点，在交接系统时虽然会同时交付备份手册、运维文档和部署文档等，然而和公司业务部门、IT 部门要求仍存在差距。

运行和测试系统。在完成开发采购管理平台工作后，压力测试工作可以在测试环境中完成，在测试时应注意平台业务的特殊性，因系统录入的开户行信息、账户名称等真实性有所保障，因此无需试运行。公司如果决定测试全业务系统，在实际操作期间要注意应用真实业务数据，因试运行便代表正式上线系统。M 公司业务部门和 IT 部门在开发系统之初并未考虑业务特殊性，所以进入开发后期后为了保证系统和生产环境相符，对架构体系和代码频繁调整。

在开发采购管理平台时，平台属于信息载体，其安全级别对信息安全会产生直接影响，在该项目中主要存在考虑信息安全不足，将功能需求作为开发主要考虑因素，因此在系统管理期和开发期，相关业务部门和采购部门一直将平台推广、系统功能作为关注重点。在系统正式上线后，IT 部才会加入项目，然而在此期间外包开发人员对公司内部信息安全管理流程、制度与体系等并不熟悉，IT 部门对开发业务系统的基本原理和架构体系也并不了解，从而对系统后期实践应用产生了影响。

整体来看，若要保证信息安全和网络安全，则需在树立管理理念、人员技术培训和资金等方面做出较高投入，并且为保证和公司当前发展需求相符，也要及时纠正传统理念。相比于信息安全而言，网络安全仅凭重建设网络层面难以取得预期成果，其需要系统管理员拥有一定能力，在后期维护方面也需要更多的成本。对于采购管理平台而言，需要重点保护业务和数据的连续性、安全性，以便于在源头上将防护工作做好，为实现这一点，在收集、整理数据等环节中，应做到始终贯穿安全制度和操作。

### 3.5.4 安全职责未纳入人员岗位招聘要求

第三方、员工和 M 公司主要根据合同规定形成了雇佣关系，并且在这种关系中，第三方和 M 公司并非直接隶属关系，因此在一定程度上增加了公司管理难度。公司在外包服务和日常工作管理中，主要根据商业行为准则对员工行为加以约束，在绩效评估中并未加入外包服务中员工安全职责，福利待遇和个人职业发展间未能形成关联机制，导致人为因素产生的负面影响不容易消除

[25]。对于公司管理者而言，更倾向于控制项目或者团队的工作效率与工作目标，忽视了考察个体安全行为的重要性，因此增加了客户与公司面临的潜在人员安全隐患和风险。

# 第 4 章 M 公司信息安全管理优化方案设计

## 4.1 优化目标与原则

### 4.1.1 优化目标

（1）保护企业信息安全免受外部威胁

在企业资产构成中，信息资产是较为重要的一项，与其他关键性商业资产价值等同。近年来，随着商业环境的不断变化，企业间的竞争日益加剧，商业信息的泄露、丢失等情况越发突出，这种情形既影响了企业自身发展，又损害了企业合作伙伴的利益，导致企业往往处于竞争中的劣势地位。故而，本文以 M 公司为例，希望通过探寻 M 公司信息安全改善对策为加强公司信息安全管理和免受外部威胁提供参考。

（2）确保业务可持续性

企业发展的根本目标在于实现股东利益最大化。业务营销和成本控制是企业盈利的根本，所以企业经营目标中包含降低经营风险和稳定业务发展。在企业管理体系中，信息安全管理属于重要的构成部分，其持续性和完善程度直接影响企业发展。故而，在 M 公司信息安全改善上，其另一目标就是对业务可持续性的保障。

### 4.1.2 优化原则

根据 M 公司当前发展情况可知，公司信息安全管理优化原则具体如下：第一，实现技术并重管理；第二，持续更新的、优化的动态机制；第三，实现企业的全面覆盖；第四，兼顾企业效益与信息安全；第五，迎合企业发展需求，解决发展中的实际问题。

## 4.2 信息安全组织优化

### 4.2.1 成立信息安全委员会

因之前公司信息安全管理工作是由流程与 IT 中心负责，为了更好的推进信息安全建设，在信息安全管理工作上，M 公司对照 IS027001 标准来建立信息安全委员会，由之作为最高决策机构。在信息安全委员会中，委员长由公司总经理担任，副委员长（党委书记）由公司副总经理担任。如图 4-1，是具体岗位分布情况。

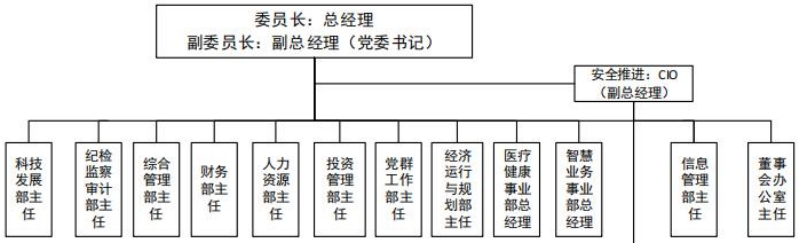


图 4-1 信息安全委员会组织架构图

委员会职责是审批信息安全的预算、项目和制度变革与制定，决策信息安全的重大事项和战略方向等。

在信息安全委员会中，委员会的正副主任主要负责指导和决策 M 公司的信息安全工作，而委员会成员既是相关工作领导，又是业务部、内审部、财务部等多部门领导，同时还要包含子公司领导，以便委员会决策更加全面、客观。M 公司还要通过委员会定期召开会议，对相关内容进行决策，如信息安全年度总结报告、信息安全预算、年度信息安全工作规划等。

信息安全委员会架构是公司正副总经理分别担任正副委员长，且下辖多个部门，如智慧业务事业部、医疗健康事业部、综合管理部、财务部等（如图 4-1）。

工作方式是以季度为单位，定期开展信息安全会议，整个会议是由正副委员长主持，在会议召开前的 2 周，对子公司和各部门征收议题。每年年初，委员会都会对全年信息安全规划进行审核，年末听取全年工作成效汇报。

在纪检监察审计部门的工作职责中纳入信息安全监察，由该部门与信息管理部一同负责监察公司信息安全管理情况，并根据规章制度处理违规行为。

M 公司构建的信息安全委员会既能高效的处理相关事务，又能通过正副总经理的备份机制来缓解总经理的工作压力。不仅如此，委员会还将纪检监察审计部作为相关工作检查的责任部门，并对以往职责混淆问题予以明确，进一步提升子公司相关工作管理水平，规避子公司负责人无法管理决策公司信息安全管理问题的风险。

4.2.2 成立信息安全管理部

在公司管理层会议同意的前提下，M 公司可以建立信息管理部，由之负责执行信息安全管理工作。信息管理部具体职责内容如下：第一，负责向 CIO 汇报全年工作；第二，协同纪检监察审计部审计、检查公司的信息安全；第三，负责开展公司内部信息安全培训工作；第四，负责制定信息安全技术架构，并确保整个架构的正常运作。在信息安全管理事务中，M 公司剔除了综合管理部的相关职责。

部门团队建设方式是在短期方式上，主要整合原综合管理部人员，并将子

公司的优秀专业人才上调；在长期方式上，主要通过内、外部招聘的方式，确保整个团队的专业性和规模。

工作的具体开展方式如下：

第一，在信息安全管理工作上，与子公司领导、公司高层、委员会成员进行沟通，明确最终的管理目标和方向；

第二，深入调查信息安全管理需求情况，并通过与各部门交流掌握相关需求；

第三，对公司信息安全管理制度不断完善，并制定各项相关操作细则和管理制度；

第四，合理划分信息安全项目，并实施预算申报和立项；

第五，协同纪检监察审计部的条件下，一同构建检查规则，并开展内部自查工作；

第六，构建年度培训方案，协同人力资源部一同开展相关培训工作。

第七，针对各类信息系统开展故障、维护、安全策略配置等方面的分析工作。

### 4.2.3 信息安全主要责任者

在信息安全管理方面，M 公司的主要责任者关系情况如图 4-2 所示。

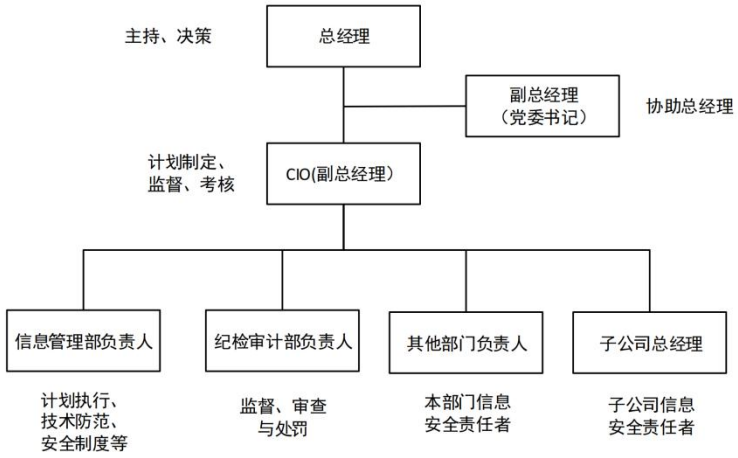


图 4-2 M 公司信息安全主要责任者关系图

总经理在整个信息安全工作中，承担总公司与子公司的指导任务，主持委员会的相关事项，负责听取年度报告内容，并负责对重大事项进行决策。

副总经理在整个信息安全工作中，负责协助总经理处理各项事务，当遇到总经理无法处理相关事务时，由之承担相关事务的处理责任。

CIO 在整个信息安全工作中，负责主持相关工作和制定年度工作方案，且负责接收子公司相关事务与信息管理部汇报的相关事务，落实子公司和信息管

理部的有关工作计划，同时还负责考核子公司和信息管理部的工作绩效。

信息管理部主任在整个信息安全工作中，既要负责落实相关工作方案，检查、维护相关技术，也负责更新信息安全手册和相关制度，并根据公司实际工作需求开展员工培训，同时还负责本部门的工作落实和成员考核工作。

纪检审计部主任在整个信息安全工作中，主要负责审计、监督总公司与子公司的相关工作，通过内部检查来找出违规行为，并根据公司规定给予相应处罚。

各部门负责人在整个信息安全工作中，主要负责管理各部门的相关事务，由本部门中选出主要窗口人员，由之配合信息管理部落实相关工作。

子公司总经理在整个信息安全工作中，子公司的相关工作主要由子公司总经理负责，既要对本公司内部信息安全管理事务进行处理，又要向 CIO 进行相关工作成果的汇报。

公司在开展下属企业信息安全管理工作的过程中，因为综合管理部并未获得授权，所以无权监管下属企业的工作开展情况。故而，为了进一步提升子公司信息安全监管水平，子公司总经理要向 CIO 或总公司的决策机构进行相关工作的定期汇报。

4.2.4 建立项目中的信息安全规章制度

根据信息安全管理要求可知，该工作可并入到项目管理工作中，也可作为项目构成部件来开展相关管理工作，为保证其管理效果，在实际管理中要对相关风险进行定期核查，并明确管理中的岗位职责和安全责任，因此，建立项目中的信息安全操作细则显得尤为重要。作为项目信息安全管理的主要负责人，项目经理可指派专人负责相关工作，将信息安全管理工作纳入到项目例会中，在强化项目外包人员管理的同时，进一步提升项目资料的保护力度。

对于 M 公司而言，相关管理细则的建立对项目信息安全的管理的帮助较为明显。在相关管理细则的建立上，主要参与部门如下：医疗健康事业部、智慧业务事业部、信息管理部，由这三大部门一同建立相关管理细则，最后交由委员会进行审核。

M 公司的项目一般分为三类，即申报类、自研类、商业类。其中，申报类主要指的经过国家有关部门的申报才可进行的一类科技项目；自研类主要指的是 M 公司自主研发和测试的一类项目；商业类指的是 M 公司人员通过现场为客户展示并外包的一类项目。

①商业项目中信息安全管理主要内容

强化项目外包人员管理力度，严格审查外包人员背景，项目外包人员信息由项目经理负责提供，而外包人员信息和背景则由人力资源部负责核对和备

案。如果公司的信息安全管理要求与外包人员背景情况相矛盾，这时人力资源部要及时发出合作终止指令，以此来终止项目合作。

通过信息系统权限来强化外包人员管理。外包人员的账号申请由项目经理全权负责，建立的账号内容中要包含岗位信息、项目负责人、项目名称等，在获得事业部经理批准之后，再由信息管理部执行相关工作。当账号过期之后，如果未到信息管理部续约，这时原账号将无法继续使用。

强化项目数据保护力度，制定项目文件管理规定。在项目的管理过程中，公司要配备专业的文档管理人员，由之来管理项目的重要交付物和过程文档，且在公司的文档管理系统中备份所有项目信息。

②自研型项目中的信息安全管理主要内容

充分运用产品与开源程序，在通过审评之后构建开源软件可信库。

在信息管理部、医疗健康事业部、智慧业务事业部、科技发展部的合作下，共同建立安全技术评估小组，由该小组来评估业务发展中涉及的软件、开源程序等情况。

③申报类项中信息安全管理主要内容

由公司的科技发展部负责管理申报类项目。在公司内部进行项目需求资料、背景资料的传递时，可以通过脱敏处理的方式来处理敏感信息，在此过程中要注意保存项目正式文档，严防拷贝行为，且阅览也要通过科技发展部授权。

策略的落实：在公司项目管理制度中纳入项目信息安全管理细则。在项目开展会议上，由信息管理部和科技发展部来阐述项目实施过程中的相关管理要求。在信息安全管理工作上，相关培训工作主要由项目经理主导并开展，同时在考核内容中纳入信息安全指标。

### 4.2.5 信息安全管理体系制度架构设计

在设计信息安全管理体系制度架构时，本文主要根据 ISO/IEC 27001 标准和等级保护确定设计方案，其中包含的管理内容共有 26 项，如内审管理、文件管理、变更便利、信息安全事件管理、人力资源信息安全管理等。除此之外，在设计制度架构时还梳理出各管理领域的接口关系，构成体系文件清单，以清单来编订体系文件。

为了确保公司信息安全管理技术标准和制度的有效性，本文在设计制度架构时尽量规避出现重复制订的情况，为实现这一点，主要通过阅览公司以往的相关技术标准和制度，将制订的文件合理归入到各个管理领域中，实现相关技术标准和制度与体系的有机结合。比如，公司现行的《文档加解密管理办法》、《局域网用户管理办法》等文件制度，可作为访问控制信息安全管理上的管理

文件，《消防管理办法》、《计算机机房管理办法》等文件制度，可作为物理与环境信息安全管理上的管理文件。除此之外，还有如《信息系统接口开发规范》、《信息系统验收规范》、等文件制度，可作为系统开发维护信息安全管理上的管理文件。

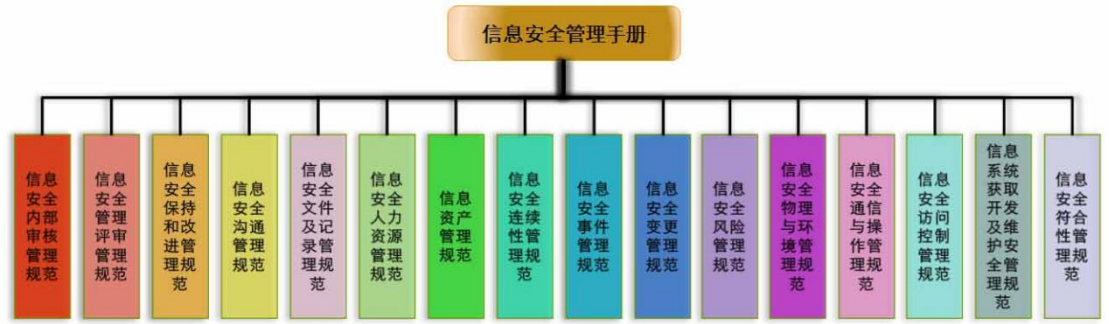


图 4-3　M 公司信息安全管理体系制度架构

## 4.3 信息安全工作制度流程管理优化

建立信息安全管理制度流程，可使企业在理论和思想上实现信息安全管理，然而企业在执行过程中无可避免的遇到各式各样问题，如果想要规避和高效的解决这些问题，那么建立高效、合理的处理流程具有一定必要性。通过高效、合理的处理流程既能及时处理相关问题，又能最大化的减弱安全故障带来的影响。

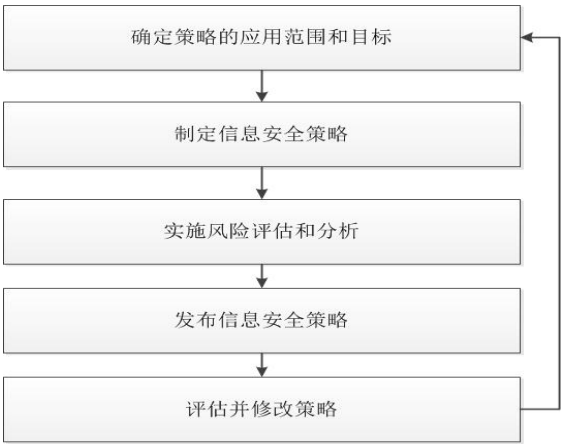


图 4-4　信息安全问题分析流程

### 4.3.1 汇报流程管理

在处理信息安全事件过程中，可以给出问题定义，以便于为技术人员定位问题提供依据。在信息安全事件中，信息安全管理人员属于首个接触人，其知识技能也是影响事件处理结果的主要因素，因此对其知识、技能和经验等方面具有一定要求，需要快速、准确的判断，为后续高效处理奠定基础。创建专门

的信息安全事件联系人清单，确保相关人员在评估、处理事件期间可以得到有效、最新的信息，避免因沟通不畅使信息安全事故更为严重。在制定信息安全风险应对预案后，要注意演练，从而保障业务连续性，在面对信息安全事故期间也能减少损失。信息安全管理员在评估和预判事件后，要及时向相关负责人申请风险紧急响应。信息信息安全管理负责人需要对信息安全事件报告单进行批复和审核。

4.3.2 问题分析处理流程

业务部门员工在开展相关工作期间，若发现问题并向信息安全管理员反馈影响或中断业务系统运转的问题，此时管理员可以按照事件定义文档确定此次事件是否属于信息安全事件，若判定结果为日常故障，直接根据处理普通事件方法处理即可，若判断结果为信息安全事件，需及时向信息安全管理负责人汇报事件相关情况，接下来由负责人按照评估流程评估处理，根据评估所得风险级别确定最终的处理流程。评估结果若为普通事件，根据一般信息安全管理事件处理方案进行处理即可，事件若定义为重大事件，需要业务部门和信息安全管理部门启动相应处理预案，在双方共同努力下及时消除事故对公司信息、数据和业务造成的影响。此外，在处理完成后，要做到及时归档并详细分析此次事件具体过程，归纳和总结处理方法，以便于为后续优化信息安全应对预案提供参考。具体如下图 4-5 所示：

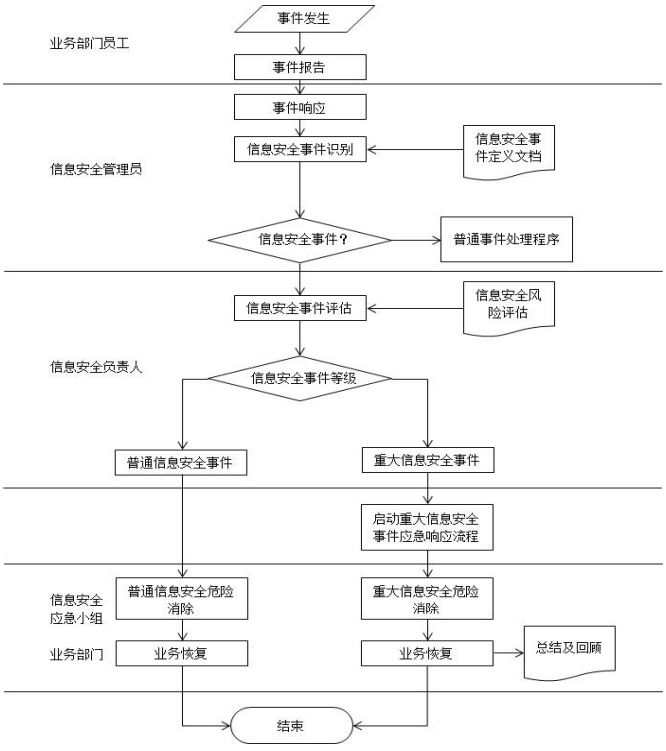


图 4-5　问题处理流程

## 4.4 信安全技术体系优化

现如今，主要在终端、应用、网络和物理等方面建设信息安全技术体系和实施信息安全技术控制方案，从而实现保护 M 公司基础架构系统、信息系统和网络可用性、完整性与保密性的目的。在有效落实数据和信息安全管理制度方面，安全技术管控的全面实施成为了较为重要且有效的手段。对此，M 公司可以综合考虑信息安全管理体系基本要求创建相应的体系框架，确保创建的安全技术体系框架和自身实际发展更为相符。

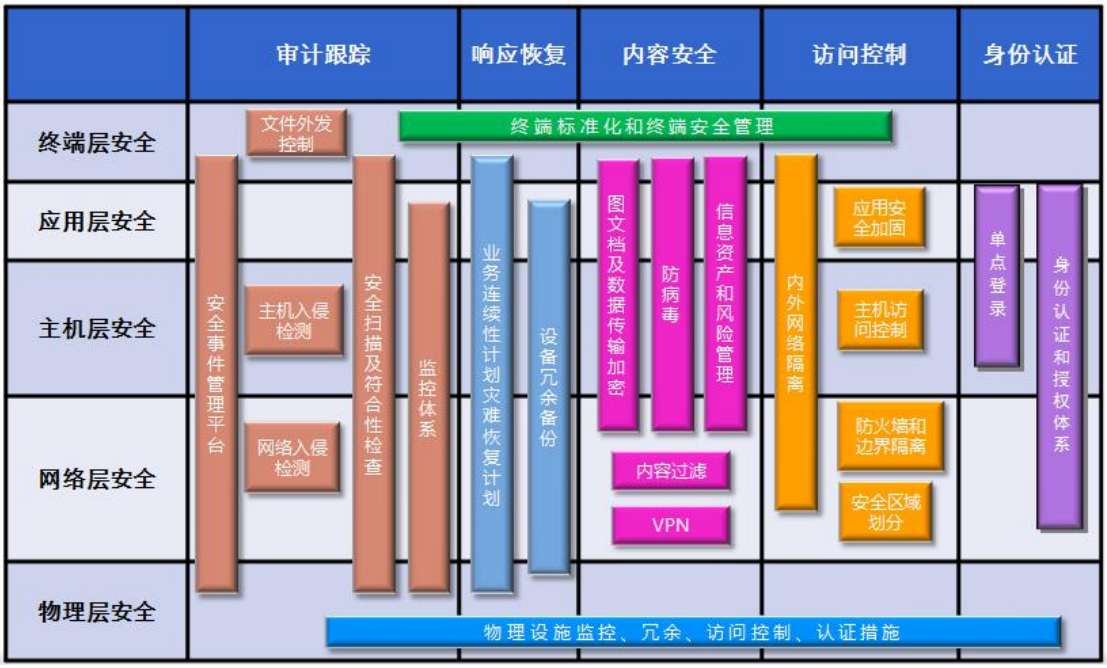


图 4-6　M 公司信息安全技术体系框架

### 4.4.1 物理安全策略

严格根据国家建设计算机机房对环境、布线和选址等方面的要求开展相关工作，在物理方面确保环境和安全要求相符。前端服务器、密钥服务器主机的应用系统，需要在电脑室放置，同时制定健全的安全监控设施机制，利用其来管控人员出入，在此过程中，也要注意划分安全登记，为日后审查出入日志奠定基础。

在信息安全技术管控中，设备物理安全属于管控基础，M 公司一直将管理数据中心作为信息系统服务器的主要内容，创建的 2 个服务器和国家数据中心要求相符，可以达到 A 级标准。通常情况下，作为一级涉密部位，数据中心配置机房一般会配置环境监控告警系统、视频监控以及多重门禁，其内部配备的安全措施主要包括三路外部供电、气体灭火装置和自动管控精密空调等，在一定程度上可以使数据中心环境安全和物理安全得到保障。与此同时，制定了严

格的数据中心审批制度，为了避免因人为原因而出现物理设备安全风险，也设置了专门的远程操作室。此外，M 公司选择冗余部署城域网链路、广域网、关键网络设备等，有效避免了系统因单一物理设备无法正常工作的风险，促使网络和系统在物理层面上得到保障。对于精密空调功率和机房方面存在的问题，可以通过加强日常巡检和健全维护制度的方式及时发现和解决问题。

4.4.2 网络与主机安全策略

在信息安全技术防护中，主机安全和网络安全属于防护的核心内容。在信息技术快速发展的环境下，出现了新的木马病毒、黑客等攻击手段，严重威胁了网络安全和信息系统安全。我国在 GB/T22239-2008 等级保护标准中指出，可以通过规划隔离网的方式创建两套逻辑隔离网络，利用其来隔离互联网与内网，由内网负责管理信息系统，在此基础上可直接通过制定内网实施安全准入控制的方式避免公司内部网络连接非授权信息，根据安全等级对外联、办公和研发网络等实施规划。根据最小访问原则，可以通过制定访问机制的方式管理重要区域，并通过审计和收集网络日志的方式冗余设计骨干核心设备与关键网络链路，从而避免因单点故障导致公司信息安全和正常经营受到影响。

创建隔离网可以将 M 公司网络安全、基础架构系统和网络信息系统面临的互联网威胁消除，有效避免内外部人员借助网络盗取机密信息，即 M 公司可以通过创建隔离网的方式提高自身网络和信息系统安全等级。为了继续提高公司网络和主机安全防护能力，避免未经授权的网络对信息系统进行非法访问，还需继续对公司信息技术进行分析，利用防火墙、管理网上行为、安全堡垒机、部署防火墙等软硬件信息安全产品，创建统一的安全技术手段和安全防护策略，促使公司内部网络的监控审计、防护边界和主机加固等方面可以显著提高安全技术管控能力，从而加强对非法访问和未经授权网络的控制力度，有效提高公司信息安全性。

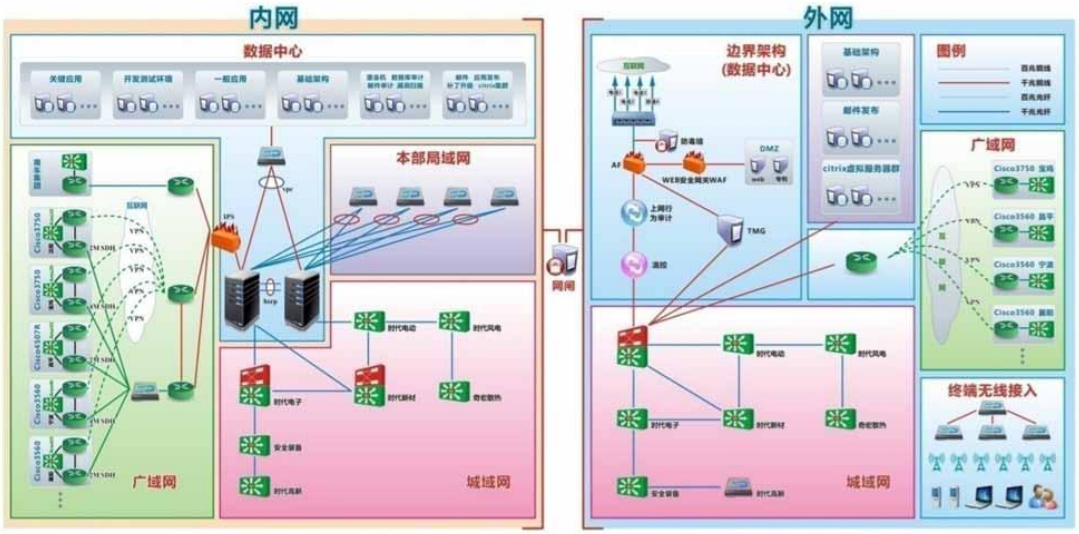

图 4-7 M 公司公司网络拓扑

### 4.4.3 应用安全策略

M 公司可以根据自身实际发展和面临的信息安全制定系统安全开发标准，在各阶段如分析需求、开发代码、验收上线等环节中确定建设信息安全的基本要求，严格根据安全标准建设开发应用系统。若信息系统已成功上线运行，此时可以对监控管理变更，同时借助堡垒机对维护活动进行监控，从而使变更维护系统期间做到安全可控。与此同时，要做到定期扫描信息系统服务器安全漏洞，如每年扫描两次，确保及时将安全漏洞找出并修补，不仅如此，为了降低公司信息面临的深层次安全漏洞风险如跨站脚本攻击、应用系统 SQL 注入等，每年也要转向安全测评核心信息系统。

黑名单管理是网络监控体系中的重要环节。在使用者层面上，软件黑名单、网络黑名单等黑名单管理功能有利于筛查复杂的网络信息，下图为设计黑名单管理功能的具体流程。通过观察设计流程可以看出，主要将黑名单管理功能分为软件黑名单、网络黑名单两方面。与此同时，在系统运行期间一直将设计网络拦截管理功能视为重要区域，在大量筛选税务局和互联网网络信息中起到了重要作用，并且在一定程度上也保障了关键信息安全。

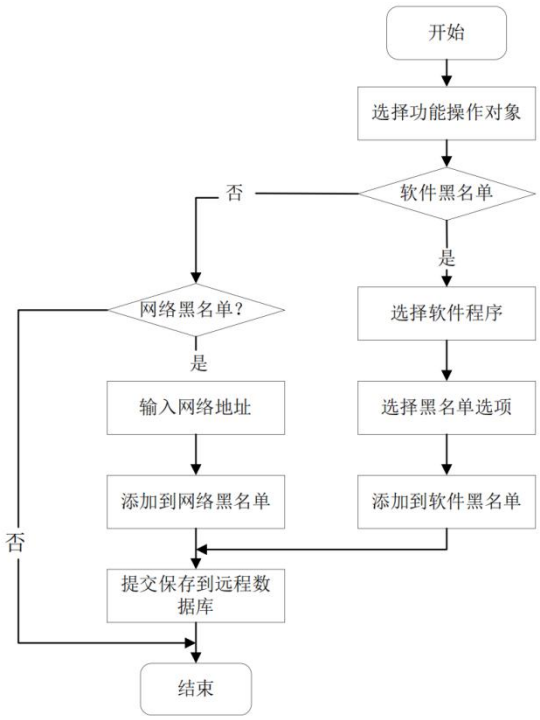


图 4-8 黑名单管理功能详细设计流程图

### 4.4.4 终端安全策略

M 公司在信息管理中，可以应用图文档加密系统，利用其加密客户端计算

机文档内容，并派遣专门人员负责管控审批文档解密，公司保密主管每季度也要审计系统解密记录，以便于及时发现问题和通报查办。通过这种方式有效提高公司文档保密安全，避免公司因为泄漏内部文档资料而受到影响，图文档加密系统架构如下图所示：

与此同时，公司客户端计算机也要安装信息安全管理软件、防病毒程度和安全监控等，以便于借助安全监控系统及时禁用非法软件、修复系统漏洞和禁用 USB 存储等，在计算机终端尽量保障信息安全，降低公司文件泄密风险。

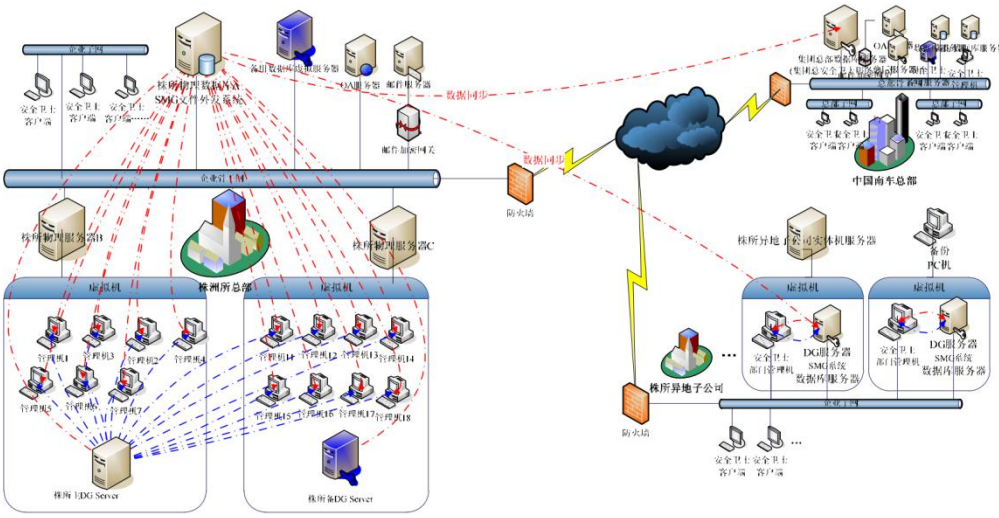


图 4-9 图文档加密系统架构

## 4.5 人力资源安全提升

### 4.5.1 信息安全科普培训

①受训对象范围及分类

信息安全培训和普及对象不仅包括 M 公司员工，也包括外包员工。在具体实施期间，可以按照员工所处岗位将培训对象分为外包人员、研发人员和职能人员等，在此基础上为不同岗位受训者提供相应的培训课程。

②培训内容的改善

现如今，M 公司还需进一步丰富原本的安全培训内容，及时更新和完善培训教材，添加知识产权、法律法规方面的培训内容，且为保证培训内容合公司需求相符，在制定期间也要将公司实际业务需求考虑在内。

③教育技术手段的提升

M 公司目前主要选择 PPT 讲解的方式进行培训，这种单一的培训手段取得的培训效果并不理想。对此，公司或培训团队可以选择市场调研来丰富培训教育手段，如引入新媒体、互联网、外部专业培训等培训手段，并在资金和人员方面为顺利开展培训工作提供保障。接下来，主要对三种培训形式进行介绍：

现场培训模式：公司在开展信息安全交流活动期间，可以邀请国内重要领导或行业知名专家讲座，同时向全体员工发放手册和印刷海报等。相比于其他培训方法而言，现场培训模式具有便于操作和理解的优势，然而若要实现这一点，需要做到不断重复和持之以恒，对资金需求也相对更多。

数字内容模式：是现代社会环境下常用的一种培训方式，可以借助宣传片强化员工安全意识。在选择该模式期间，可直接向公司索取，在播放和选择宣传片期间要注意和企业文化、公司业务相结合，确保重点突出。

学习平台模式：该模式主要包括调查问卷、在线安全课程等，可以结合 M 公司业务和管理实际情况制定具体针对性的问卷或课程内容。若要利用该模式提高员工安全意识，可以从员工日常工作入手确定具体内容，且要包括商业数据保护、员工信息保护和基础信息安全等内容。

实施培训：为保证培训效果，公司需要保证每年举办培训，且在举办期间要做到覆盖子公司。不仅如此，在培训签到后，也要及时收集反馈意见，或以信息安全、信息安全月为主题举办答题知识竞赛，从而使员工积极主动的丰富自身知识。

④安全意识教育的提升

现如今，滥用移动存储介质、恶意感染代码等问题成为了威胁 M 公司信息安全的主要问题。在 M 公司管理中，主要由人力资源部分策划安全意识教育培训工作，据培训对象所处岗位制定相应的培训内容，完成培训后进行考核，从而保证培训质量。

4.5.2 提高员工访问互联网安全意识

为了测试公司员工信息安全意识情况，M 公司信息管理部门需要根据规定每年测试安全意识。

在此期间，我们应用钓鱼邮件检测员工信息安全意识。在具体实施期间，可以按照员工职位信息、工作岗位等推动相应的钓鱼内容，对钓鱼结果进行统计分析后即可得到员工安全意识基本情况。

在推行测试时，我们制定选择定期和不定期相结合的方式，每年测试外部供应商全体员工两次，根据分析结果了解 M 公司员工安全意识基本情况。为保证测试效果，需要根据社会变化调整钓鱼邮件风格和内容，选择常用的工作场景如项目、休假和合同审批等内容。

测试三次结果，如下图所示。在最后一次测试中对测试风格与内容进行了调整，点击和开启邮件数量显著增加，标志着 M 公司还需要进一步强化员工安全意识。

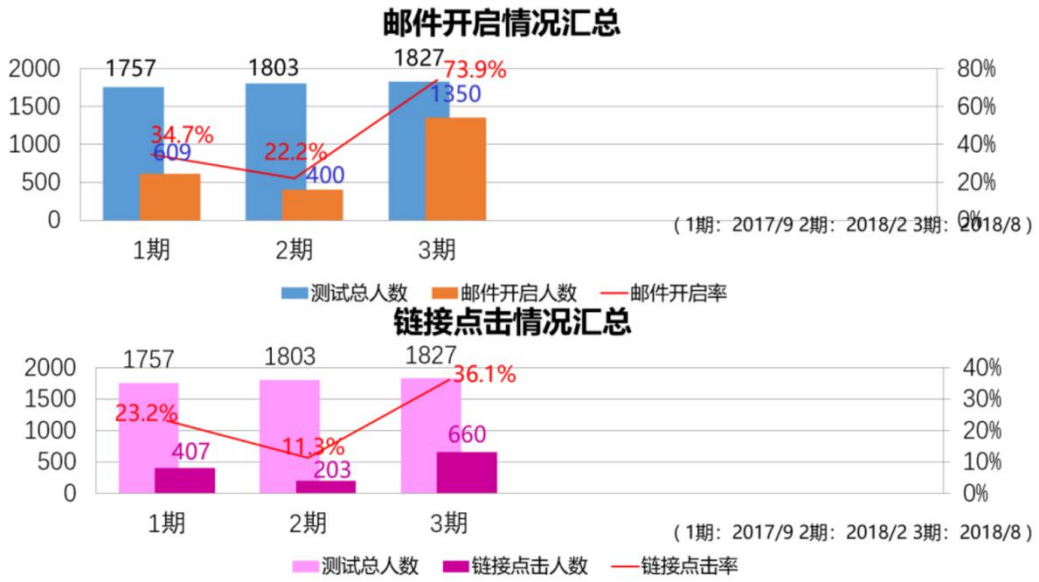


图 4-10 M 公司钓鱼邮件测试结果报告（2017-2018 年）

4.5.3 进一步加强员工基础安全防控

从前文分析可知，M 公司在基础安全防控方面存在不足，因此在此后的发展和管理中，M 公司可以加强对数据和信息安全管理在基础安全防控方面的管理力度。

（1）加强防护终端物理设备与信息安全管理

M 公司 IT 资产管理部门可以将身份验证管理、授权移动存储介质作为管理重点，并注意加强对终端信息交流活动的监控力度。与此同时，可以从实际情况入手简化 IAM 审批流程，适当缩减基于 VPN 账号和邮件的审批授权周期和员工身份账号识别周期，及时对访问日志进行审查，做到及时跟踪违规情况，以便于降低或避免因人为共享账号而造成的信息安全问题。严格根据公司规定对违纪员工进行处理，若情节严重或造成严重后果，可在开除后移交司法机关。此外，M 公司也要有效限制非授权访问，制定多重防护策略，M 公司优化后得到的身份授权关系如下图所示：

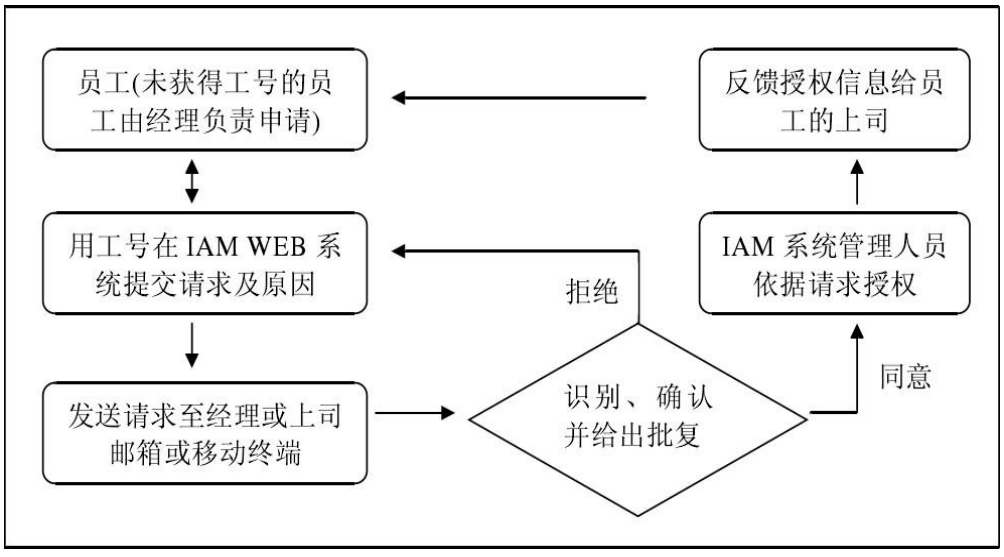

图 4-11　M 公司身份授权管理系统的主要流程优化

M 公司对身份授权系统进行优化时，可在管理日志记录期间将复制、下载和访问重要信息作为管理重点，通过配置管理流程和变更管理项目服务对客户敏感信息等项目资料进行追溯，以便于在遗失、加密和使用存储设备中加强技术安全防控力度。与此同时，在资产管理控制平台中可以对存储介质等物理接口进行实时监测，在加密访问记录的同时，也可以借助技术手段监管后台数据库，确保能够自动向本部门管理者和信息资产管理部门发送违规记录报告，及时发现非授权访问情况，进而做到及时处理。

（2）限制软件安装管理

公司信息若未限制软件安装管理，也容易面临信息外泄可能，因此 M 公司可以加强对软件安装管理的限制力度，确保内外网信息传递在公司控制范围内。在具体实施期间，M 公司也可以应用终端权限管控策略取消本地管理中的员工身份，安装本地软件工作统一由 IT 运维部负责，通过这种方法避免因非必要软件安全造成的信息安全事件，加强对公司内部信息的保护力度。此外，M 公司可以引入技术手段对服务器端进行处理，屏蔽恶意网站和非法网站，限制非法下载上传数据和互联网网站访问，降低公司内部网络感染病毒和泄漏信息概率，在日常信息管理中，应用邮件日志管理机制管理和审查外发邮电，及时发现并解决涉及公司重要信息的信息，避免因此造成严重后果。

（3）加强信息资产等级识别与分类保护机制建设

在公司经营发展中，识别信息资产是保护信息资产的关键性步骤和基础环节，也是公司分类信息资产的主要依据。根据识别信息资产基本思想可知，信息资产指标具有可用性、保密性和完整性的基本特点。

为了更好的对信息资产管理，我们建立了信息资产等级，分为对外公开类、内部公开类、机密类和绝密类四个等级，每个等级的原则和方法是对外公开类，外泄此类信息资产不会威胁员工、公司安全，属于公司向社会公众的信息资产，社会公众可以根据自身需求免费获取。

内部公开类，此类信息属于公司内部可公开的信息，若外泄此类信息，对员工和企业发展容易带来不利影响。

机密类，此类信息蕴含商业价值，若并未经过授权而私自使用或对外公开，则会损害员工和企业利益。

绝密类，此类信息蕴含巨大商业价值，公司内部仅有极少数人指导，所以一旦外协或未能授权被滥用，容易威胁企业正常经营发展，甚至增加企业破产风险。

M 公司制定分类资产方案可参考表 4.1，在完成资产分类工作后，创建专

门的资产分类保护机制，结合资产等级创建与之相符的资产信息保护细则与方案。与此同时，为了保证信息安全管理效果，M 公司要确定分类资产保护中各岗位承担的职责，以便于各部门和人员能够根据相关规定完整自身工作，在发现问题后也可以及时找到问题原因。

表 4-1　M 公司信息资产的种类划分

| 序号 | 保密级别 | 影响度 | 主要描述 | 事例 |
|---|---|---|---|---|
| 1 | 绝密级 | 重大 | 蕴含巨大商业价值，公司内部仅有极少数人指导，所以一旦外协或未能授权被滥用，容易威胁企业正常经营发展，甚至增加企业破产风险。 | 总经理会议纪要、投资战略、发展战略、未公开的财报等 |
| 2 | 机密级 | 严重 | 蕴含商业价值，若并未经过授权而私自使用或对外公开，则会损害员工和企业利益 | 高净值客户信息、商业计划、市场上关键理财产品报告、管理步骤与敏感信息等 |
| 3 | 内部公开级 | 有限 | 属于公司内部可公开的信息，若外泄此类信息，对员工和企业发展容易带来不利影响 | 会议记录、通讯录、备忘录等 |
| 4 | 外部公开级 | 无 | 属于公司向社会公众的信息资产，社会公众可以根据自身需求免费获取。外泄此类信息资产不会威胁员工、公司安全。 | 官网信息、对外披露的财务报告、年度经营报告等 |

4.5.4 加强人员安全职责管理机制建设

从前文分析中了解，在 M 公司信息安全管理中，人为因素是其面临的主要问题之一，因此，M 公司建设人员安全职责管理机制进行信息安全管理具有一定必要性。在具体实施期间，M 公司可以从下述两方面入手建设人员安全职责管理机制：

一方面，引导员工行政正确的信息安全责任意识。对于个体而言，行为主要由意识决定，因此可以从该角度入手管理人员安全职责，确保公司各阶层员工能够了解管理人员安全职责的价值和意义，在此基础上调动员工主观能动性，促使其可以规范自身行为，确保安全使用公司信息。若要实现这一点，M 公司内部可以积极宣传信息安全的重要性，引导员工树立正确的责任意识，明确损害企业信息安全对自身、对企业造成的影响和相关人员需要承担的责任，在此期间可以综合应用公司展示板、公司公众号和企业微信群等多种方式进行宣传，从而保证宣传效果和员工对信息安全的认识，避免因人为因素泄漏公司重要客户数据、知识产权和商业机密等。

另一方面，确定具体的信息安全职责要求。在制度层面上确定公司信息管

理中员工需要承担的信息安全职责，对于一些敏感岗位，可以和岗位员工签署信息安全责任状，明确其需要承担的信息安全责任，同时确定泄漏重大信息员工需要接受的间接责任处罚或直接责任出发，从而有效降低人为因素泄漏公司信息的概率。M 公司在招聘新员工期间，可以调查关键性技术岗位人员的背景和道德情况，对聘用合同保密协议继续优化和改进，确定员工在入职到离职期间需要承担的信息安全保护责任。不仅如此，M 公司也要加强对转岗人员的管理力度，重点管控权限变更，严格监控和审查离职员工交接情况。总之，M 公司要了解人为因素对信息安全造成的影响，并通过上述措施来确定信息安全职责要求，从而降低 M 公司信息泄露风险。

（1）进一步按照 PDCA 循环理论思想改善安全审计程序

M 公司可以根据 PDCA 循环理论思想对信息安全审计进行改进和完善，并从审后复核、审中监督和审前指导等方面入手进行信息安全审计，从而提高闭环的有效性与全面性，使公司信息安全得到保障。在具体实施期间应注意，首先，可以改进和优化审计流程和审计编制计划，降低人为因素造成的疏漏；其次，控制审计力度进一步加强，通过这种方式确保审计执行力度，这样得到的审计效果也更为理想；最后，创建审计档案，对审计内容进行完善，并保证审计资料能够及时归档，这样得到的审计程序更为规范。为保证实施效果，在实施期间要将 M 公司实际情况考虑在内，选择全覆盖性审计复核策略避免单人审核影响最终结果。例如，在审计某人工智能项目期间，需保证审计复核人员超过 2 人，在配备项目人员期间也要参考项目实际交易额。为实现这一点，需要对审计过程、审计计划进行复核和监督，确定推进人工智能项目期间面临的关键性风险和财务责任。此外，在完成审计工作之后，参与到审计工作中的审计人员都要提交一份相关的工作记录，通过交叉符合审计记录来更好的明确审计建议拥有的可操作性特征，进而以此来获得最佳的优化措施实施效果。

（2）着力提升内审人员知识素养

在 M 公司信息安全审计制度建设中，公司内部安全信息审计队伍的建设属于较为重要的环节。从 M 公司当前的发展情况可知，公司当前要招入一批主要从事 IT 项目审计领域的人才，致力于对内部审计人员分析能力与综合素养的提升，通过内外部培训来进一步提升公司审计人员整体水平，可以通过内外部机构来为公司审计人员补充相关理论和知识，同时注意合理应用外部培训进一步提升公司审计人员的专业水平，在具体实施期间，要重点鼓励和支持公司审计人员，引导公司审计人员不断提升自我，积极主动考取获得工作发展所需的各项认证，如“注册信息系统审计师”认证、“信息安全审计师”认证等等，这些认证都是具有较高权威性的认证，尤其是“注册信息系统审计师”认

证是级别最高的，如果 M 公司能招入或培养一位拥有这样认证的人才，那么公司的信息安全水平可以大幅提升，这时公司的信息系统安全也将得到有效保障。

# 第 5 章 M 公司信息安全管理方案保障措施与预期效果

## 5.1 保障措施

### 5.1.1 组织保障

在信息安全管理中，若要确保顺利落实相关方案，将优化方案效果发挥出来，M 公司研发部需要进一步强化组织保障。在优化方案的落实上，M 公司专项小组职能主要由信息安全管理委员会负责承担，而委员会的成员构成正是由第 4 章的各部门和正副总经理所构成。在优化方案的实施过程中，首先，作为组织保障的委员会首先要对原敏捷开发中的相关制度内容进行梳理，在了解和掌握相关制度的基础上，根据现有制度和公司组织架构来制定与实际情况相匹配的制度，为优化方案的落实提供所需环境；其次，M 公司还要根据产品运营数据和敏捷过程来制定合理的优化措施实施方案，并根据各岗位工作要求来划分职责内容，进而达到逐步落实的效果；最后，M 公司还要进一步提升各团队和部门负责人的沟通效率，保证所需资源能够如实如期到位。

### 5.1.2 人事保障

在信息安全管理优化上，M 公司的人事部要根据酒店业务来调整相关角色和组织，制定合理的人才战略发展计划。第一步，在推行方案之前，与组织进行沟通调整现有方案，确保职能团队敏捷成员可合理分离出来；第二步，实时掌握团队成员的技能水平，对一些技能水平未达标的成员，要及时制定合理的培训计划和方案，确保团队整体技能水平都满足相关要求；第三步，在落实优化方案之后，人事部还可以结合公司实际情况解剔除与新增岗位，根据具体情况制定合理的人才战略计划。

### 5.1.3 考核机制

考核机制是最常用的激励方式之一，若 M 公司想要持续实施信息安全管理优化方案，那么人事部与研发部的配合具有一定必要性，因此可以制定合理的考核机制来鼓励两部门工作者参与到优化制度的实施和质量提升中。考核机制推行的根本目的在于落实优化后的信息安全管理体系，在构建考核机制时，相关负责人和执行者既要参与到体系的落实上，又要探寻新方案实施过程中遇到的问题，并提出合理的解决与改进措施。为了充分发挥信息安全管理效果，考核内容中不仅要包含产品质量追踪效果，也要纳入考核团队计划实施成效。如果想要将优化措施持续性落实，则考核指标中需要加入产品运营的质量成本，通过质量委员会来分析和搜集相关数据，之后由团队成员配合落实相关计

划，其中的主次考核对象分别是质量委员会和团队成员。按照优化后的体系落实情况，结合质量改进和产品质量成本情况，构建与企业情况相匹配的考核机制，进而激励团队更好的落实优化措施。

## 5.2 预期效果分析

在分析预期效果时，主要通过测评 M 公司信息安全体系，获得相应的测评结果，并根据测评结果来判断最终的改进优化措施效果。在测评过程中，本节运用了两种方法，一个是模糊理论，另一个是层次分析法。在调查问卷问题的回答上，受调查者要根据 M 公司优化之后的实际效果进行填写，最后汇总调查数据获得最终评估所需数据。

表 5-1 实施优化方案后的 M 公司信息安全体系综合评判向量 E 计算结果

| 一级指标编号 | 一级指标名称 | 综合评判向量编号 | 综合评判向量 | | | | |
|---|---|---|---|---|---|---|---|
| | | | 优秀 | 良好 | 一般 | 较差 | 差 |
| $U_1$ | 信息安全方针 | $E_1$ | [0.1250 | 0.7500 | 0.1250 | 0.0000 | 0.0000] |
| $U_2$ | 信息安全组织 | $E_2$ | [0.4464 | 0.5536 | 0.0000 | 0.0000 | 0.0000] |
| $U_3$ | 人力资源安全 | $E_3$ | [0.1250 | 0.4263 | 0.2898 | 0.1590 | 0.0000] |
| $U_4$ | 资产管理 | $E_4$ | [0.1375 | 0.7563 | 0.1063 | 0.0000 | 0.0000] |
| $U_5$ | 访问控制 | $E_5$ | [0.0833 | 0.7760 | 0.1408 | 0.0000 | 0.0000] |
| $U_6$ | 密码学 | $E_6$ | [0.3750 | 0.6250 | 0.0000 | 0.0000 | 0.0000] |
| $U_7$ | 物理环境安全 | $E_7$ | [0.1875 | 0.6875 | 0.1250 | 0.0000 | 0.0000] |
| $U_8$ | 操作安全 | $E_8$ | [0.3003 | 0.5000 | 0.1998 | 0.0000 | 0.0000] |
| $U_9$ | 通信安全 | $E_9$ | [0.1250 | 0.8750 | 0.0000 | 0.0000 | 0.0000] |
| $U_a$ | 系统获取、开发和维护 | $E_a$ | [0.1250 | 0.6705 | 0.1648 | 0.0398 | 0.0000] |
| $U_b$ | 供应商关系 | $E_b$ | [0.3750 | 0.5000 | 0.1250 | 0.0000 | 0.0000] |
| $U_c$ | 信息安全事件管理 | $E_c$ | [0.1250 | 0.8750 | 0.0000 | 0.0000 | 0.0000] |
| $U_d$ | 业务连续性管理的信息安全方面 | $E_d$ | [0.1875 | 0.6250 | 0.1875 | 0.0000 | 0.0000] |
| $U_e$ | 符合性 | $E_e$ | [0.2655 | 0.6095 | 0.1250 | 0.0000 | 0.0000] |

表 5-2 M 公司信息安全体系 14 个控制域测评结果对比表

| 一级指标编号 | 一级指标名称 | 实施优化方案前测评结果 | 实施优化方案后测评结果 |
|---|---|---|---|
| $U_1$ | 信息安全方针 | 良好 | 良好 |
| $U_2$ | 信息安全组织 | 一般 | 良好 |
| $U_3$ | 人力资源安全 | 良好 | 良好 |
| $U_4$ | 资产管理 | 良好 | 良好 |
| $U_5$ | 访问控制 | 一般 | 良好 |
| $U_6$ | 密码学 | 良好 | 良好 |
| $U_7$ | 物理环境安全 | 良好 | 良好 |
| $U_8$ | 操作安全 | 一般 | 良好 |
| $U_9$ | 通信安全 | 良好 | 良好 |
| $U_a$ | 系统获取、开发和维护 | 良好 | 良好 |
| $U_b$ | 供应商关系 | 一般 | 良好 |
| $U_c$ | 信息安全事件管理 | 良好 | 良好 |
| $U_d$ | 业务连续性管理 | 良好 | 良好 |
| $U_e$ | 符合性 | 良好 | 良好 |

在 U 的综合评判向量 E 的计算上，不仅涉及到二级评判模糊矩阵 Q，而且还牵涉一级指标权重系数 P，即得出 E＝[0.1948 0.6447 0.1441 0.0164 0.0000]，并由此判断出 U 为良好，换言之，企业信息安全体系的测评为“良好”。按照国际标准目标可知，M 公司的整体水平达到“良好”评价标准。根据二级评判结果，M 公司的综合评价向量 E＝[0.1948 0.6447 0.1441 0.0164 0.0000]，根据模糊评语集可知，在信息安全体系整体水平上，M 公司的饼状图状况如图 5.3。通过图 5.3 可知，20%为优秀，64%为良好，一般比重为 14%，虽然 M 公司的整体水平良好，但是与未实施优化前数据对比，12%为优秀，61%为良好，一般比重为 25%，其整体水平得到明显提升，标志着本次实施的改进措施具有显著效果，如图 5-1。

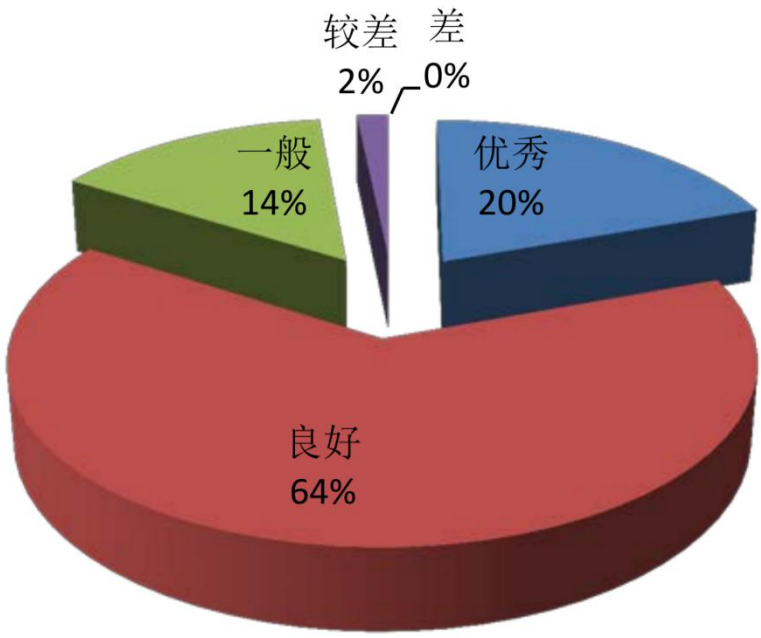


图 5-1 实施优化方案后的 M 公司信息安全体系整体水平饼状图

通过雷达图的制作，分类轴选为 14 个控制域，坐标刻度轴选为模糊评语集，以此构建雷达图坐标系。根据优化后的控制域管理水平、国际标准合格线、未优化的控制域管理水平，一同构建雷达图，具体如图 5.4。在测评结果上，主要以实心正方形代表“良好”，以实心三角形代表“优秀”，最终结果是用实心菱形来代表。如图 5-2。

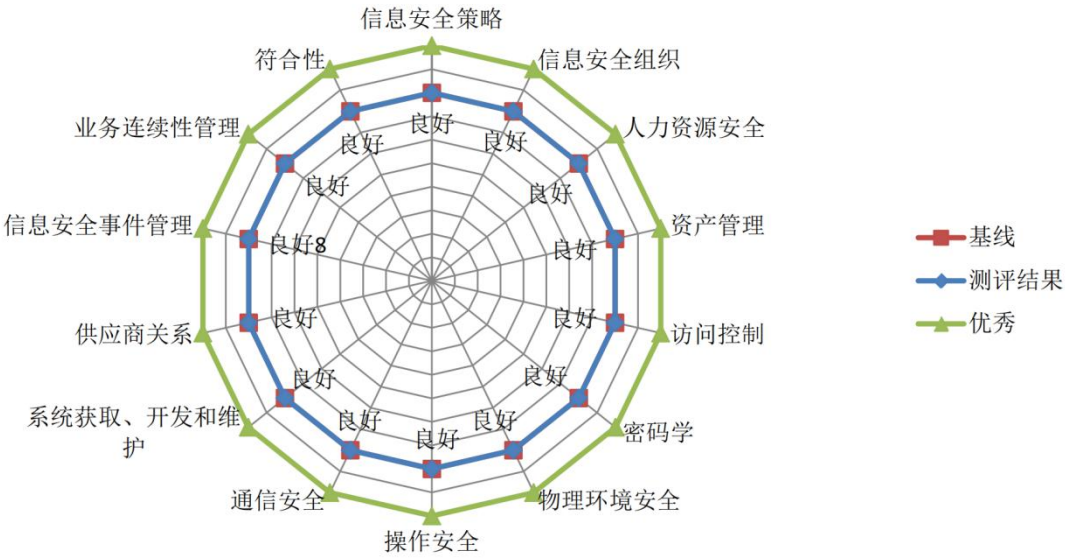


图 5-2 实施优化方案后的 M 公司控制域管理水平综合雷达图

通过图 5-2 可知，在未实施优化之前，M 公司只有供应商关系、操作安全、访问控制和信息安全组织，这 4 个控制域的评价为“良好”，在实行本文提出改进措施后，M 公司控制域的评价都为“良好”，全部控制域都达到最低标准。这代表本次的改进措施具有显著成效。

# 第 6 章 结论与展望

## 6.1 结论

（1）本文从项目实际问题出发，以 M 公司为研究对象，分析其信息安全管理现状找出公司现阶段存在的问题，分析后发现，随着公司规模的不断扩大，信息安全管理问题带来的风险也随之增加，甚至已影响到公司未来发展。由于 M 公司主营范围具有特殊性，所以对信息安全管理上要求相对严格。事实上，M 公司在信息安全管理方面的投入明显增加，但是获得的成效却并不明显，之所以出现如此状况，主要在于公司的转变主要集中在思想层面，即只注重管理意识上的提升，并未加强相关管理能力，导致公司的技术约束水平相对较低，无法起到高效管理公司信息安全的效果。

（2）对公司的系统维护与开发、人力资源安全、信息安全组织等问题进行分析，发现存在以下问题：组织结构不合理、信息安全管理制度不科学、技术工具建设不到位、人员安全意识差。

（3）针对 M 公司现存的信息安全管理问题，本文立足于信息安全管理体系模型的基础之上，提出了合理的解决措施与策略。实际上，优化信息安全方面管理需要时间来沉淀，所以本文提出的相关措施策略的效果仍需进一步观察。此外，如果想要提升管理效果，还需 M 公司全体员工的大力配合，并创造落实相关措施的有效环境。

（4）在分析预期效果测评过程中，运用了两种方法，一个是模糊理论，另一个是层次分析法。在调查问卷问题的回答上，受调查者要根据 M 公司优化之后的实际效果进行填写，最后汇总调查数据获得最终评估所需数据。在未实施优化之前，M 公司只有供应商关系、操作安全、访问控制和信息安全组织，这 4 个控制域的评价为“良好”，在实行本文提出改进措施后，M 公司控制域的评价都为“良好”，全部控制域都达到最低标准。这代表本次的改进措施具有显著成效。

## 6.2 研究展望

在信息安全管理上，相关工作的落实需要 M 公司全体员工的配合，事实上，相关管理工作本身无法提升信息安全水平，唯有将管理工作落实到各个岗位之上，引导公司员工积极主动的参与到管理中，才能实现信息化建设的全面覆盖，进而实现真正意义上的信息安全管理，保证公司信息安全。在 M 公司信息安全管理探索上，虽然本文开展了初步研究，但是相关措施尚处于初级阶

段，加之本人的学术水平有限，所以文中仍存在不足之处，在此后的研究中，还需进一步完善。除此之外，也希望本文提出的建议和措施可以为同类公司加强信息管理提供参考，帮助同类型公司更好的发展。

# 参考文献

[1] Posey C , Roberts T L , Lowry P B , et al. Bridging the divide: A qualitative comparison of information security thought patterns between information security professionals and ordinary organizational insiders[J]. Information & Management, 2019, 51(5):551-567.

[2] Herath T , Rao H R . Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness[J]. Decision Support Systems, 2019, 47(2):154-165.

[3] Crossler R E , Johnston A C , Lowry P B , et al. Future directions for behavioral information security research[J]. Computers & Security, 2018, 32(11):90-101.

[4] Myyry L , Siponen M , Pahnila S , et al. What levels of moral reasoning and values explain adherence to information security rules? An empirical study[J]. European Journal of Information Systems, 2019, 18(2):126-139.

[5] Lawrence, D, Bodin, et al. Evaluating information security investments using the analytic hierarchy process[J]. Communications of the ACM, 2018, 48(2):78-83.

[6] Chang S E , Ho C B . Organizational factors to the effectiveness of implementing information security management[J]. Industrial Management & Data Systems, 2016, 106(3/4):345-361.

[7] Siponen M , Pahnila S , Mahmood M A . Compliance with Information Security Policies: An Empirical Investigation[J]. Computer, 2019, 43(2):64-71.

[8] Lee W H . How to identify emerging research fields using scientometrics: An example in the field of Information Security[J]. Scientometrics, 2018, 76(3):503-525.

[9] Kraemer S , Carayon P . Human errors and violations in computer and information security: the viewpoint of network administrators and security specialists.[J]. Applied Ergonomics, 2017, 38(2):143-154.

[10] Ericsson G N . Toward a Framework for Managing Information Security for an Electric Power Utility—CIGRÉ Experiences[J]. IEEE Transactions on Power Delivery, 2017, 22(3):p.1461-1469.

[11] Meng X F , Cai L Z , Yang X L , et al. Information security system by iterative multiple-phase retrieval and pixel random permutation[J]. Applied

Optics, 2019, 45(14):3289-97.

[12] Ogiit H . The configuration and detection strategies for information security systems[J]. Computers & Mathematics with Applications, 2013, 65(9):1234-1253.

[13] Yangmengke Z Z X . Challenges and Solutions of Information Security Issues in the Age of Big Data[J]. China Communications, 2016, 13(3):193-202.

[14] Karabacak B , Sogukpinar I . ISRAM: information security risk analysis method[J]. Computers & Security, 2005, 24(2):147-159.

[15] Homer K , Eloff J . Information security policy — what do international information security standards say?[J]. Computers & Security, 2016, 21(5):402-409.

[16] Rhee H S , Kim C , Ryu Y U . Self-efficacy in information security: Its influence on end users' information security practice behavior[J]. Computers & Security, 2016, 28(8):816-826.

[17] Niekerk J , Solms R V . Information security culture: A management perspective[J]. Computers & Security, 2021, 29(4):476-486.

[18] Solms S H V . Information Security - The Fourth Wave[J]. Computers & Security, 2017, 25(3):165-168.

[19] Hovden J . The information security digital divide between information security managers and users[J]. Computers & Security, 2018, 28(6):476-490.

[20] Solms B V . Information Security — A Multidimensional Discipline[J]. Computers & Security, 2020, 20(6):504-508.

[21] Albrechtsen E , Hovden J . Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study.[J]. Computers & Security, 2020, 29(4):432-445.

[22] Rees J , Bandyopadhyay S , Spafford E H . PFIRES: A policy framework for information security[J]. Communications of the ACM, 2016, 46(7):101-106.

[23] Rezgui Y , Marks A . Information security awareness in higher education: An exploratory study[J]. Computers & Security, 2018, 27(7-8):241-253.

[24] Dantu Y , Mookerjee V S . Knowledge sharing and investment decisions in information security[J]. Decision Support Systems, 2019, 52(1):95-107.

[25] Solms B V . Corporate Governance and Information Security[J]. Computers

& Security, 2019, 20(3):215-218.

[26] Gupta M , Rees J , Chaturvedi A , et al. Matching information security vulnerabilities to organizational security profiles: a genetic algorithm approach[J]. Decision Support Systems, 2020, 41(3):592-603.

[27] Post G V , Kagan A . Evaluating information security tradeoffs: Restricting access can interfere with user tasks[J]. Computers & Security, 2020, 26(3):229-237.

[28] Von Solms B , Von Solms R . From information security to…business security?[J]. Computers & Security, 2020, 24(4):271-273.

[29] Nosworthy J D . Implementing Information Security In The 21 st Century — Do You Have the Balancing Factors?[J]. Computers & Security, 2019, 19(4):337-347.

[30] Venter H S , Eloff J . A taxonomy for information security technologies[J]. Computers & Security, 2020, 22(4):299-307.

[31] 刘念, 张建华. 互动用电方式下的信息安全风险与安全需求分析[J]. 电力系统自动化, 2017(02):84-88.

[32] 娄策群, 范昊, 王菲. 现代信息技术环境中的信息安全问题及其对策[J]. 中国图书馆学报, 2018(06):32-36.

[33] 丁先存, 王辉, 段华洽. 论电子政务中信息安全及法律保护[J]. 中国行政管理, 2018, 000(010):10-12.

[34] 王长全, 艾雱. 云计算时代的数字图书馆信息安全思考[J]. 图书馆建设, 2019, 10(001):50-52.

[35] 樊如霞, 郑志荣. 网络信息安全与防范技术[J]. 情报科学, 2019, 019(005):514-516.

[36] 王越, 杨平利, 李卫军. 涉密计算机信息安全管理体系的设计与实现[J]. 计算机工程与设计, 2020, 031(018):3964-3967,3971.

[37] 尹淋雨. 谈数字图书馆的网络信息安全[J]. 图书馆论坛, 2015(01):54-56.

[38] 汤淼淼. 信息安全评估标准、技术及其进展[J]. 计算机工程, 2016, 29(006):1-2.

[39] 杨洋, 姚淑珍. 一种基于威胁分析的信息安全风险评估方法[J]. 计算机工程与应用, 2016, 045(003):94-96,100.

[40] 孙红梅. 基于价值链理论的档案信息安全管理[J]. 档案学研究, 2017(01):38-42.

[41] 王刚. 档案信息安全保障体系的建设与思考[J]. 档案学研究,

2018(03):54-58.

[42] 杨鑫. 网络信息与信息安全探析[J]. 情报杂志, 2019, 20(004):44-45.

[43] 王大康, 杜海山, WANGDa-kang,等. 信息安全中的加密与解密技术[J]. 北京工业大学学报, 2019, 32(6):497-500.

[44] 江和平. 浅谈网络信息安全技术[J]. 现代情报, 2020, 24(12):125-127.

[45] 凌捷. 大信息安全与隐私保护[J]. 计算机学报, 2015(01):246-258.

[46] 陈左宁, 王广益, 胡苏太,等. 大信息安全与自主可控[J]. 科学通报, 2017(5):427-432.

[47] 李晓康. 网络安全扫描技术研究[J]. 计算机工程, 2018, 30(010):54-56.

[48] 冯登国, 张敏, 张妍,等. 云计算安全研究[J]. 软件学报, 2019, 22(1):71-83.

[49] 潘烨. 网络环境下的信息安全[J]. 中国图书馆学报, 2020, 28(002):44-46.

[50] 秦铁辉, 罗超. 基于信息安全的企业反竞争情报体系构建[J]. 情报科学, 2016, 024(010):1441-1445,1450.

[51] 祝利锋. 基于 VPN 技术的信息安全构架研究[J]. 武汉理工大学学报, 2015(05):62-64.

[52] 刘静芳, 陈赤培, 樊江涛. 电力系统一体化设计中信息安全防护体系研究[J]. 电力自动化设备, 2016, 25(2):83-85.

[53] 宗文萍, 郭莉珠. 论信息时代的档案信息安全保障[J]. 档案学通讯, 2017, 10(006):60-64.

[54] 王建红. 信息安全模型研究[J]. 小型微型计算机系统, 2018, 21(010):1078-1081.

[55] 张丽. 信息安全的新兴领域—信息隐藏[J]. 计算机应用研究, 2019(07):6-8.

[56] 杨海平. 网络信息安全研究[J]. 情报科学, 2020, 18(10):944-947.

[57] 程平, 周欢, 杨周南. 云会计下会计信息安全问题探析[J]. 会计之友, 2017, 000(026):28-31.

[58] 项文新. 档案信息安全保障体系框架研究[J]. 档案学研究, 2020(02):70-75.

[59] 何培育. 电子商务环境下个人信息安全危机与法律保护对策探析[J]. 河北法学, 2019, 32(008):34-41.

[60] 马仁杰, 刘俊玲. 论电子档案开放利用中信息安全保障存在的问题与对策[J]. 档案学通讯, 2020(3):56-60.

# 附录 A

M 公司信息安全管理中信息安全管理问题调查问卷

尊敬的先生/女士：

您好！为了对 M 公司信息安全管理问题进行全面的了解，提升我们信息安全服务水平，保护公司信息资产安全，特开展本次问卷调查，本问卷不记姓名，您所填写的一切信息都将进行保密，感谢您的合作。

一、您的基本情况

1. 性别

A. 男　B. 女

2. 组织结构设置

A. 组织结构设置科学　B. 组织结构设置合理

3. 管理制度

A. 内部管理制度完善　B. 内部管理制度存在不足

4. 信息沟通流程

A. 公司内部信息沟通流程顺畅　B. 公司内部信息沟通流程不畅

5. 外包管理

A. 对外包要求管理规范　B. 对外包要求管理不规范

6. 岗位

A. 部门负责人　B. 行政人员　C. 研发工程师　D. 网络工程师

E. 运维工程师　F. 架构师　G.信息安全工程师　H. 审计工程师

二、评分标准

表 A-1 评分标准表

| 分数 | 评价 |
|---|---|
| 10 | 关键因素之一 |
| 6-9 | 主要因素之一 |

| | |
|---|---|
| 1-5 | 次要原因 |

三、调查内容（请根据上面的评分标准进行打分）

表 A-2 调查内容表

| 序号 | 编号 | 问题 | 评分 |
|---|---|---|---|
| 1 | A1 | 您或您身边的人有没有因为个人信息泄露遇到过麻烦 | |
| 2 | A2 | 您是否对主机设置了屏幕保护并加了密码 | |
| 3 | A3 | 团队沟通不畅通 | |
| 4 | B1 | 您是否对本机重要文件和数据进行密码保护 | |
| 5 | C1 | 您是否设置所有的密码都一致 | |
| 6 | C2 | 公司缺乏有效信息安全管理体系 | |
| 7 | C3 | 您是否安装了杀毒软件，会经常升级病毒库吗 | |
| 8 | C4 | 您收到中午标题但不熟悉的发件人，或主题让你感兴趣的邮件后如何处理 | |
| 9 | C5 | 如果熟悉的邮件地址发来的自动播放 flash 动画或者邮件内部嵌入的网页，你会如何处理 | |
| 10 | C6 | 您的电脑是否遭到网络攻击 | |
| 11 | C7 | 管理制度不足 | |
| 12 | C8 | 信息安全是否顺利执行 | |
| 13 | C9 | 缺乏安全性检测 | |
| 14 | D1 | 缺乏有效回顾和监控 | |