专 业 学 位 硕 士 学 位 论 文

BY 公司信息安全风险管理研究

Research on Information Security Risk Management of BY Company

作 者 姓 名：喻石

学科、 专业：工商管理

学　　号：41811459

指 导 教 师：李瀛

完 成 日 期：2021 年 6 月 6 日

大连理工大学

Dalian University of Technology

摘　要

近年来，随着企业信息化进程不断推进，企业信息安全事件频繁发生，这给企业的正常运营带来巨大安全隐患。现今企业对信息安全的重视程度不断提高，信息安全风险管理也已经成为企业信息安全管理的一个关注点，因此该领域研究的重要程度不可忽视。

本论文以 BY 公司为研究对象，在信息安全管理相关概念和理论应用的基础上，对 BY 公司现有信息安全风险的相关问题进行信息安全风险分析，基于风险分析的结果，提出相应的信息安全风险控制方案、信息安全管理体系建设方案以及保障措施。首先，本论文阐述了研究的相关背景，国内外研究现状，以及本论文的研究框架和研究方法；同时，介绍了信息安全相关的理论与规范，并对信息安全风险管理的各个过程做出进一步阐述。其次，通过对 BY 公司整体状况的深入了解，结合 BY 公司内部问题的调查结果，找出其目前信息安全管理存在的主要问题及原因所在；通过引入信息安全风险分析的标准规范和过程，对 BY 公司信息系统进行定性定量的信息安全风险评估及分析。最后, 本文结合 BY 公司信息系统信息安全风险的评估结果, 针对性的提出风险控制方案, 并对 BY 公司的信息安全管理体系建设工作和相应的保障措施做出进一步阐述, 确保 BY 公司信息安全管理问题得以解决。

本论文在研究的过程中，以信息安全管理理论为基础，同时还引用到了信息安全风险管理的理论，其中包括信息安全风险的定义、评估、分析和控制。在论文研究实践的过程中，本文将信息安全管理相关的理论切实的应用到了 BY 公司的实际问题分析和解决方案制定当中。虽然本论文研究过程中还存在很多不足之处，有待在后续的研究过程中进一步完善，但本论文的研究方向和研究方法可以为同类型公司作类似研究提供参考。

关键词：信息安全风险管理；信息安全等级保护；风险控制；信息安全管理体系建设

A Research on Information Security Risk Management of BY Company

Abstract

In recent years, with the continuous advancement of enterprise informatization, enterprise information security incidents have occurred frequently, which has brought huge security risks to the normal operation of enterprises. Nowadays, enterprises pay more and more attention to information security, and information security risk management has become a focus of enterprise information security management. Therefore, the importance of research in this field cannot be ignored.

This paper mainly takes BY Company as the research object, and aspects of the following are the main content of this paper: Firstly, this paper illustrates the concerned background of this paper research, the current research situation of home and abroad, as well as the research framework and research methods; The theories and norms related to information security are introduced, and the various processes of information security risk management are further elaborated. Secondly, through the in-depth understanding of BY company's overall situation, combined with the investigation results of BY company's internal problems, finding out its existing main information security management problems and their causes; in the meantime, introducing the standard and regulatory process of information security risk analysis, making qualitative and quantitative information security risk assessment and analysis of BY company's information system. Finally, this paper combines the information security risk assessment results of BY company's information system, proposing a targeted risk control plan, and further elaborates BY company's information security management system construction and corresponding safeguard measures to ensure BY company's information security management issues will be resolved.

This paper leverages several information security management related theories and risk management methods, which are applied into the analysis and solution finding of BY company's major issues. Despite of the shortcoming of the entire research process, the research direction and methods still could be taken as reference for other company.

Key Words：Information Security Risk Management; Information Security Level Protection; Risk Control; Information Security Management System Construction

目　　录

1 绪论

改革开放距今已经过去了 40 多年，在这个过程中，我国逐渐变成了一个世界级的信息产业大国。近些年来，随着信息技术手段的不断革新，众多企业的核心业务细节都存在信息技术的身影。在建筑、冶金、机械、能源等传统产业转型的过程中，产业信息化起到了至关重要的作用[1]。

现今企业为了谋求进一步的业绩增长，实现资源配置优化，顺应行业发展趋势，逐步已经将企业的信息技术能力和手段融入到企业发展及战略转型当中。然而，在信息技术为企业发展带来新希望的同时，它也让企业感受到了产业信息化带来的负面影响，给企业的正常运营带来了潜在信息安全风险，随之而来的企业信息安全问题与日俱增。

1.1 研究背景

互联网科技的迅猛发展，使得信息化环境下的数据，变成了人们赖以生存的精神源泉。而信息技术本身，具有其自身的脆弱性。企业越是依赖于信息化带来的便利，越会将企业自身暴露于信息化的风险当中[2]。比如，在 2018 年 6 月 19 日，圆通速递有限公司发生了 10 亿条快递数据信息泄露。这些数据被暗网明码标价，低价兜售，导致相关快递用户的地址、姓名、电话等信息流入不法商贩手中，造成了用户个人隐私泄露的信息安全风险；再如，在 2018 年 3 月，美国 Facebook 公司发生巨量用户信息数据泄露，导致超过 8700 万用户的个人社交习惯、社交喜好等信息流入互联网公共平台当中。

现今国内企业发展面临着巨大挑战，产品供应链不稳定，产品研发能力薄弱，产品销售利润微薄，再加上自从中国 2001 年加入 WTO 以来，众多国际大型企业进入中国市场，加剧了行业竞争。在经济全球化浪潮的洗礼下，国内企业的发展更是雪上加霜。企业为了增强核心业务能力，更好的适应瞬息万变的国内和国际市场，逐步倾向通过产业信息化来提高企业管理效率。然而，在企业信息化建设的过程中，企业往往只重视信息化为企业人员管理、业务流程管理等方面带来的便利，而忽略了企业信息安全问题给企业管理带来的潜在风险。企业信息安全风险如果不能得到有效的管理，可能会给企业的发展带来不可估量的损失。

BY 公司是一家跨国医药行业公司的中国子公司，其信息系统外部接口较多，使用人员纷杂，外部访客及驻场外部人员较多，信息安全的风险隐患较大。近些年来，BY 公司内部频繁发生信息安全事件，业务部门深受影响，效益损失严重。集团总部对于这些信息安全事件极为重视，迫切要求 BY 公司能够提出强有力的信息安全问题解决方案和未来公司信息安全风险控制方案。

1.2 研究目的和意义

本文通过对 BY 公司当前信息安全管理问题的风险分析和研究，找出其在信息安全管理制度、员工职责范围、信息安全培训等方面的问题。进而，针对找出的问题，提出相应的信息安全风险控制方案和信息安全管理体系建设方案，使 BY 公司具有完善的信息安全管理能力。

信息安全管理体系是一套系统管理组织敏感数据的政策和程序。它的目标是通过主动限制安全漏洞的影响来最小化风险并确保业务连续性。信息安全管理体系通常解决员工的行为和流程以及数据和技术等方面的问题。为了使组织的信息安全得到保障，我们可以针对特定类型的数据（例如客户数据等）进行管理，也可以以综合管理的方式来实施，使其成为公司文化的一部分。

本文的研究，以 BY 公司当前的信息安全管理现状为背景，对比信息安全管理体系标准规范及管理相关模型，制订出满足 BY 公司信息安全管理要求的策略，保证 BY 公司信息系统的平稳运行。同时也为同类型企业在信息安全管理策略及制度设计方面提供参考，为信息安全领域的进一步探索提供方向。

1.3 国内外相关研究现状

1.3.1 国外研究现状

从前，人们获取信息，是通过电视、报纸等传统媒体信息传输方式。而信息技术的出现，彻底改变了人们获取信息的渠道。随着信息技术手段的不断革新，如我们现在熟知的移动网络技术，改变传统信息基础架构的云技术，驱使推送个人定制偏好软件的大数据技术等，都在不断挑战信息安全领域的阈值；另一方面，随着信息安全需求的不断提高，也催生了信息技术的革新与发展[3]。

我们耳熟能详的国际跨国大型企业，如 HP, IBM, SAP 等科技型企业，在企业信息安全风险领域的研究主要从以下几个方面着手：首先，这些国际大型公司不再以信息技术手段本身作为重点突破口，而将更多的工作重心向信息安全管理手段转移；其次，过去的信息安全投资方向是以信息技术基础架构为核心，也就是我们所了解的基础设施层，而近些年的投资重点方向改成了信息技术的应用层，也就是我们所了解的应用系统和相关的应用软件；再次，信息安全管理本身也变成了公司管理体系的一部分，在公司运营的同时，有机的结合了信息安全管理和风险管理的概念和相关措施。

鉴于信息安全这个话题的重要性，欧美国家已经逐步将信息安全作为国家发展的重要议题，相关的理论研究框架和模型也比较多，其中主要包括风险管理的通用框架、风险关系管理模型、风险管理过程、风险管理流程等方面[4]。

例如，学者 Saleh M S 和 Alfantookh A 着重从信息安全风险管理的“范围”和“评估标准”两个方面来阐述信息安全风险管理框架，并从“流程”和“评估工具”两个维度来说明具体的执行操作步骤。该文献从战略，技术，组织，人员和环境几个方面对风险框架做出了进一步分析，并利用知名的六西格玛模型，具体说明了信息安全风险管理的流程[5]。学者 Fenz, Stefan 和 Andreas Ekelhart 从信息安全风险管理的“验证”，“校准”和“评估”三个维度进行分析，通过结合一个虚拟金融机构的案例，来充分说明企业信息安全管理在不同阶段的具体风险管理方法[6]。学者 Broderick, J. Stuart.将企业信息安全风险风险管理程度和风险对业务的影响进行比较分析，从信息的“敏感性”，“重要性”和“资产价值”的维度出发，说明了什么时候应该进行企业信息安全风险评估和管理，以及进行风险评估的具体方法[7]。

1.3.2 国内研究现状

本论文在进行研究的过程中，阅读了很多当前有关国内企业信息安全风险管理方面的研究文献。比如，任伟在一篇钢铁企业信息安全风险系统管理研究文献中，依据信息安全风险评估及控制理论，针对钢铁企业当前存在的信息安全风险问题，提出了集成技术与管理的钢铁企业信息安全风险管理多级控制系统框架[8]；再如，毛纪辉在关于烟草行业信息安全风险及防控的研究文献中，通过对烟草行业信息安全风险的分析，提出了具有建设性的烟草行业信息安全防控策略[9]。

本论文综合研究的相关文献，总结出国内企业在信息安全风险研究领域的特点如下：

首先，当前国内企业在信息安全领域的研究，更多的将研究重点放在整体信息安全管理的框架制定和整体规划上。国内企业在信息安全管理层面，更多的是借助于引用国外比较流行的信息安全管理框架，按照对应的理论框架制定管理计划，然而能够落地并结合企业信息安全风险实际问题的研究较少。

其次，有些研究文献将研究的重点放在了企业背景的介绍、企业怎样与信息技术相结合，以及信息安全管理的理论与概念的介绍上面。对于企业信息安全风险问题的分析不够充分，而更倾向于直接提出解决企业信息安全风险问题的建议和方案。

最后，各个企业在进行信息安全风险研究的过程中，更多的只是结合企业本身的问题和应对措施，缺少同行业企业之间有关企业信息安全风险管理的交流和探讨，具有很强的企业自身局限性。

1.4 研究内容和研究方法

1.4.1 研究内容

本论文的研究，主要是基于信息安全管理体系、信息安全风险管理以及信息安全等级保护等方面的概念，针对 BY 公司当前存在的信息安全管理问题，进行了定性和定量的信息安全风险分析。基于风险分析的结果，提出了具体的风险控制措施以及体系建设方案，最后总结了问题解决方案的保障措施。

本篇论文的结构和内容安排如下：

第一章 绪论：主要说明了信息化在当前传统企业转型过程中起到的重要作用，并提出信息技术为现今企业发展及战略转型带来的希望和潜在信息安全风险问题。

第二章 理论基础：本章主要介绍了与信息安全相关的一些重要规范，如信息安全等级保护的具体信息，信息安全管理体系的相关概念以及信息安全风险管理的全部过程，即信息安全风险是什么，怎样进行信息安全风险评估，信息安全风险的分析方法，以及信息安全风险的控制方式。

第三章 BY 公司信息安全管理现存问题及分析：本章首先介绍了当前 BY 公司的实际运营状况及发展历程，并重点介绍了公司的组织架构及部门职责。在 BY 公司当前信息安全管理问题调查和汇总的基础上，通过定性和定量的信息安全风险分析方式，分析出当前 BY 公司信息系统在信息安全管理方面存在的主要问题。

第四章 BY 公司信息安全管理解决方案：结合 BY 公司信息系统风险评估等级化处理结果，针对性的提出信息安全风险控制方案，并为 BY 公司制定切实可行的信息安全管理体系建设方案。

第五章 BY 公司信息安全管理保障措施：在第四章阐述风险控制方案和信息安全体系建设方案的基础上，从不同管理职能的角度来论述，为 BY 公司信息安全管理提供保障措施。

结论：回顾并总结本文研究的主要结论，对论文研究实践的启示，以及研究过程中存在的不足之处进行阐述。

1.4.2 研究方法

首先，本篇论文对国内外信息安全管理相关文献进行了文献综述分析。在深入研读国内外相关文献资料的过程中，了解到国外信息安全管理相关的理论研究框架较多，发展较早，尤其是一些国际大型跨国企业，将信息安全管理研究重点向信息安全管理手段、应用系统安全管理、以及信息安全管理和风险管理相结合的方向转移；而国内信息安全

管理方面的研究，主要局限在引用国际较流行的信息安全管理框架上，缺少针对企业面临实际信息安全风险问题的合理分析。

其次，本篇论文对信息安全风险领域的先进案例进行了研究和分析。通过重点研读相关案例，了解到当前能够较好落地的案例研究，更多倾向于通过对企业背景和企业面临实际问题的深入了解，通过定性定量的分析方法，提出具有可行性的风险管理方案，以解决企业面临的实际信息安全问题。

最后，本篇论文对 BY 公司企业背景和当前面临主要信息安全管理问题进行了实际调研，通过定性定量的风险管理方法，分析出 BY 公司面临的主要信息安全风险。基于风险分析的结果，针对的提出风险控制措施、信息安全体系建设方案以及相应的保障措施。

本篇论文的技术路线如下图 1.1 所示：

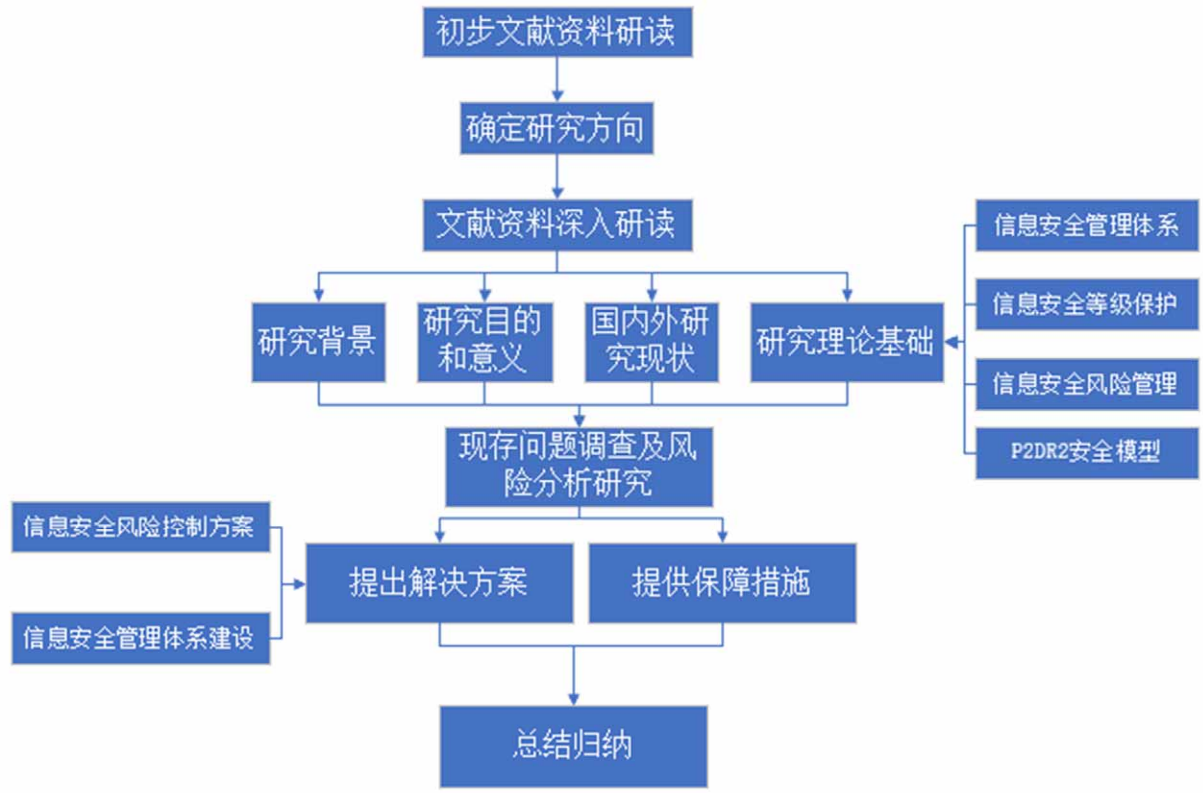

图 1.1　技术路线

Fig. 1.1　Thesis research framework

2 理论基础

2.1 信息安全相关理论和规范

2.1.1 信息安全等级保护

信息安全等级保护，是根据《中华人民共和国计算机信息系统安全保护条例》等有关法律法规而制定的办法，旨在提高信息安全保障水平和能力，维护社会稳定、公共利益和国家安全，保障和促进信息化建设。其具体方式，是通过不同程度的保护措施，将承载信息的信息系统、承载信息系统的安全设备进行分级别保护，同时针对信息系统当中发生的各种安全事件，进行分不同级别的处理和响应[10]。

从信息系统的重要等级上划分，可分为一般系统、重要系统和极重要系统；信息系统保护的等级划分从第一级到第五级；受保护的主体，主要分为国家安全机密、社会公共秩序和个人数据隐私合法权益；从受损害程度上来看，分为损害、严重损害和特别严重的损害；对应不同等级的监管方式，分别为“自主保护级”，“指导保护级”，“监督保护级”，“强制保护级”和“专控保护级”。

2.1.2 信息安全管理体系

ISO/IEC27001 一共分为两个部分，一个是信息安全管理实施的原则，另一个是信息安全管理体系的规范。其中信息安全管理体系规范的主导思想，是通过建立并实施信息安全管理体系规范，使企业的信息安全风险控制在可接受的范围之内，保证业务的可持续性运行，同时以文件化的形式阐述哪些是企业内部受保护的资产，其对应的风险管理方法以及风险控制程度。

基于 ISO/IEC 27001 的标准描述，信息安全管理体系的构建，主要由下面的几个方面组成[11]：

（1） 信息安全管理前期的准备工作：深入了解当前组织机构的运营情况，公司背景，以及相关信息系统的实际构成情况；在组织或公司的领导授权下，设立专门的信息安全管理调查小组，基于组织的人员工作安排，合理的制定信息安全管理体系构建计划。

（2） 风险评估：在信息安全管理体系构建计划的框架下，制定符合实际情况的信息安全风险评估计划。通过发放回收调查问卷，工作人员面谈等形式，收集并整理组织或公司的资产相关信息，识别相关资产，并对其威胁和脆弱性进行风险评估。

（3）风险分析 :在相关资产风险评估的基础上，进行各个资产风险值的结果判定，确认风险等级对应的控制范围。

（4） 风险控制和信息安全体系建设 :基于风险分析的结果, 确认风险控制的范围；在对应范围的基础上，构建信息安全体系建设的基准，比对并修订当前的信息安全管理标准，提出并构建新的信息安全管理框架。

（5） 内审机制：设立组织内部专门的内审部门，审查组织或公司信息安全管理存在的隐患和漏洞，并提出相应的改善建议和方案。

（6） 外审机制：联合外部专门的审查机构，进行定期外部审查，评价组织或公司当前的信息安全管理体系水平，针对性的基于现存信息安全管理问题提出专业性的意见和建议。

（7） 持续改进计划：制定信息安全管理体系的持续改进方针和计划，审查现存问题和可以改进提高的点，提出可持续性的、可实现的改进计划。

2.1.3 P2DR2 安全模型

P2DR2 安全模型从信息安全的策略、信息安全的保护措施、信息安全的检测方式、信息安全事件的响应方式和信息安全恢复这个几个方面，构建了基于闭环控制、主动防御的动态网络安全理论模型。在模型的实际应用当中，相应的操作人员素质、人员的技术水平和人员的操作方式是该模型体系能够正常运作的基本因素[12]。

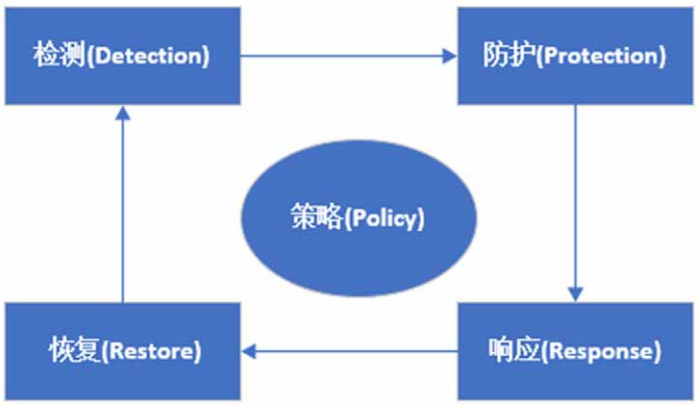

图 2.1 P2DR2 安全模型示意图

Fig. 2.1 Schematic diagram of P2DR2 security model

该模型通过网络路由及安全策略的制定与分析，为企业网络交互提供保护。通过在网络内部及边界建立实时监测及审计机制，采取实时动态相应安全手段，应用多样性的系统灾难备份恢复、关键系统冗余设计等方法，构造多层次、全方位和立体的区域网络安全环境。

学者吴军，李桃红和邵定宏从“时间域”和“策略域”两个维度对 P2DR2 模型做出理论分析，从“防护”，“检测”，“响应”和“恢复”这几个维度对该模型做出功能性分析，依据该模型理论为企业网络安全构建安全体系，并将理论研究应用到企业“网络监听”和“VPDN 通信”当中，实践证明企业网络安全防护效果良好[13]。

2.2 信息安全风险管理方法

2.2.1 信息安全风险定义

信息系统的运行和使用，以及这些系统运行所在的环境相关的威胁和漏洞，而可能对组织及其利益相关者造成的影响构成了信息安全风险。

2.2.2 信息安全风险评估

在风险管理方法的基础上，信息安全风险评估通过运用有逻辑性的科学方法，全方位分析出当前信息系统当中相应资产存在的威胁以及其脆弱性，使组织能够根据风险的严重性对风险进行优先级排序。它能够确定信息资产的重要程度，已经存在或可能存在的适用威胁和漏洞，现有控制措施，其对所识别风险的影响，潜在后果并最终确定其优先级。

“资产识别”，“威胁识别”，“脆弱性识别”是进行系统性信息安全风险评估的基本方法。在相应识别赋值的基础上，评估其资产出现信息安全问题威胁的可能性，以及出现威胁后带来的潜在影响，并最终提出风险控制措施，将可能造成的资产损失降低到可接受范围之内[14]。下图 2.2 为风险评估过程图。

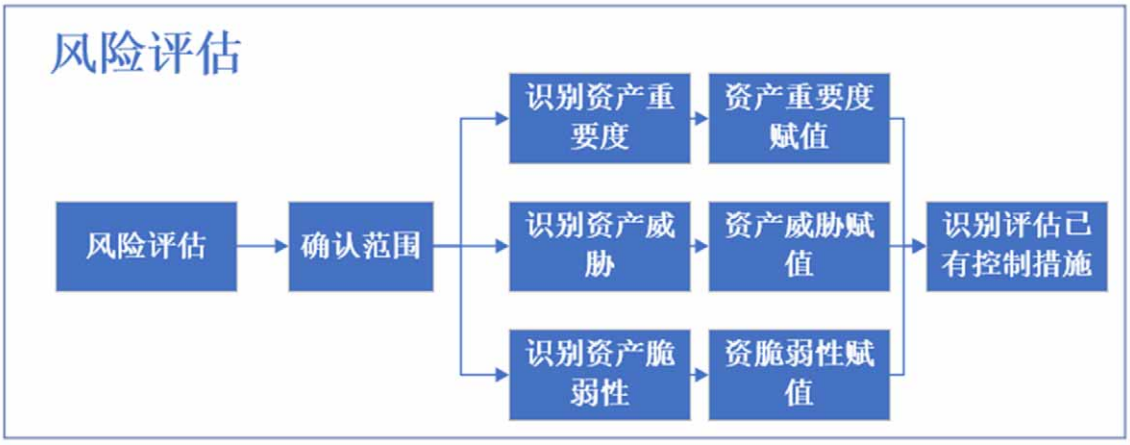

图 2.2 风险评估过程图

Fig. 2.2 Risk assessment flow chart

2.2.3 信息安全风险分析

信息安全风险分析的主要方法，首先，要识别和评估资产重要度，资产威胁、资产脆弱性和已有控制有效性，同时确定其相应的赋值。基于信息安全风险的计算模型，计算出不同资产的风险值。其次，通过对比风险控制标准，确定资产风险等级和进行风险控制的优先级。下图 2.3 为风险分析原理图[15]。

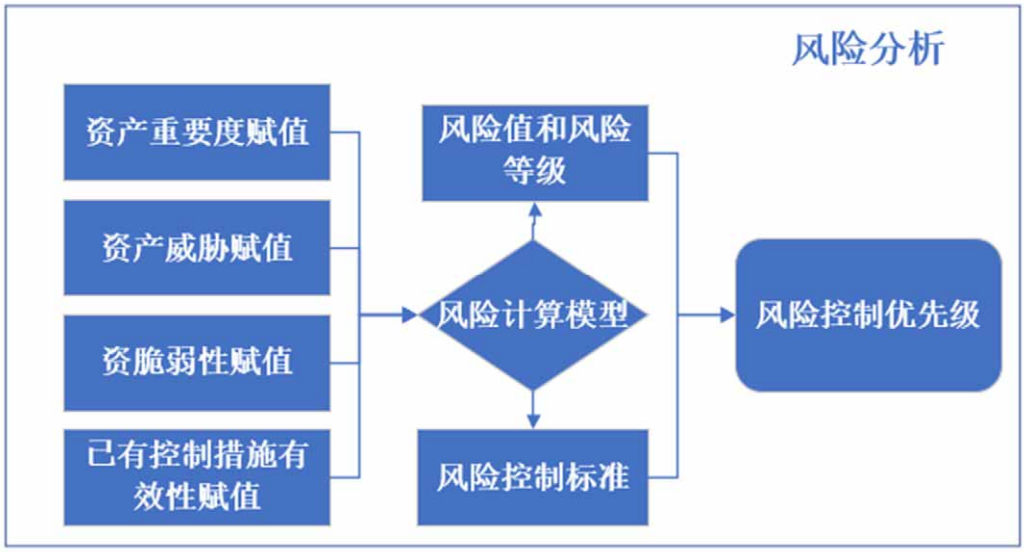

图 2.3 风险分析原理图

Fig. 2.3 Risk analysis schematic

2.2.4 信息安全风险控制

基于风险评估分析的结果，提出并制定相应的风险控制措施方案，如风险降低、风险保留、风险规避或者风险转移等。通过风险控制措施的实施，将组织或公司相关资产的风险水平控制在可以接受的范围之内。在制定风险控制措施的方案当中，要充分考虑到控制方案的可行性，即该方案是否可以在实际风险控制当中得到实现；还要充分考虑到该风险控制措施的经济效益，即该措施实施的性价比。下图 2.4 为风险控制过程图。

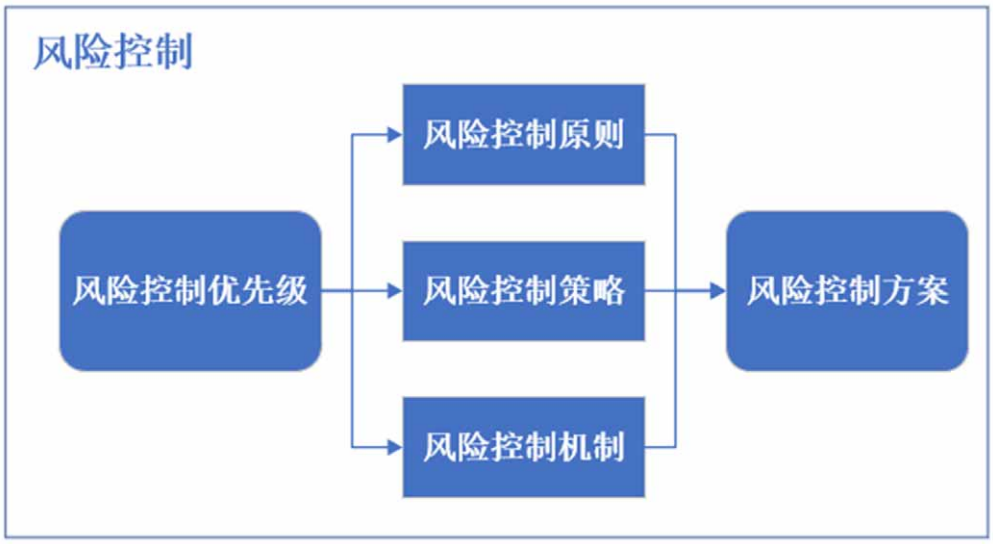

图 2.4　风险控制过程图

Fig. 2.4　Risk control flow chart

3 BY 公司信息安全管理现存问题及分析

3.1 BY 公司简介

BY 公司是 BY 集团下设在中国的直属分公司，主要负责 BY 集团在中国业务当中信息系统建设、运营及日常管理工作。BY 公司成立于 2010 年 10 月，整合了健康消费品、医药保健、动物保健等中国业务部门的全局基础设施管理和信息系统管理。自从公司成立以来，BY 公司在中国成功实施了医药仓储供应链优化项目、健康消费品业务可视化系统项目和动物保健业务基础设施及系统剥离等重大项目。

BY 公司信息系统一共覆盖 3 大主要业务部门，42 个业务子部门。与此同时，BY 公司信息系统的数据信息会与 BY 集团总部的信息系统相连，平行与世界 30 多个国家实现信息系统数据策略共享。自从公司设立以来，基于业务需求已经上线 100 多个应用系统和 6000 多个功能，基本实现了业务国内一体化管理，实现了业务内数据共享，信息联动，系统功能整合，使得工作效率大幅度提升。

3.1.1 BY 公司的发展历程

2010 年 10 月，BY 公司将总部设立在了中国上海。当时 BY 集团在中国下设的业务范围主要针对的是医药保健和健康消费品业务。由于 BY 集团在国外的信息技术部门为国外的业务发展提供了坚实的技术基础和新型解决方案，BY 集团希望将成型的信息技术经验应用到中国业务发展当中，因此，BY 公司应运而生。

2015 年 9 月，随着信息技术手段的迅猛发展以及不断增加的业务需求，BY 集团首次将信息技术部门作为一个主要职能部门，下放在集团业务服务部，主要负责集团信息技术解决方案的规划，全球信息系统整合以及区域信息技术基础设施和项目方案的协调。与此同时，集团面对竞争对手的巨大压力，为了防止客户、合作伙伴以及自主知识产权信息的泄露，构建了集团级别的信息安全管理体系，并将该体系普及到全球各大分公司以及相关信息技术职能部门，以满足当时业务的信息安全需求。

2017 年 10 月，BY 集团提出了“ IT 驱动变革 ”的口号，将信息技术的发展目标与业务战略发展目标紧密的结合了起来。BY 公司成立之初设立的七个部门，其工作汇报线改成了各个职能部门单独汇报给总部的模式，并由总部将 BY 公司各职能部门安排与中国各个业务线协同工作，共同完成业务目标。

2019 年 3 月，为了完成 BY 集团“ 共享健康，消除饥饿 ”的愿景，BY 公司在集团组织架构调整的基础上，重新获取了七个职能部门的管理权，整合国内业务工作，为业务运营的信息系统建设和日常管理工作提供支持。

3.1.2 BY 公司组织架构简介

在 2019 年战略调整后，BY 公司重新组建七个职能部门，共有员工 101 人，其中包括正式员工 73 人。BY 公司的组织架构和部门职责如下图 3.1 和表 3.1 所示：

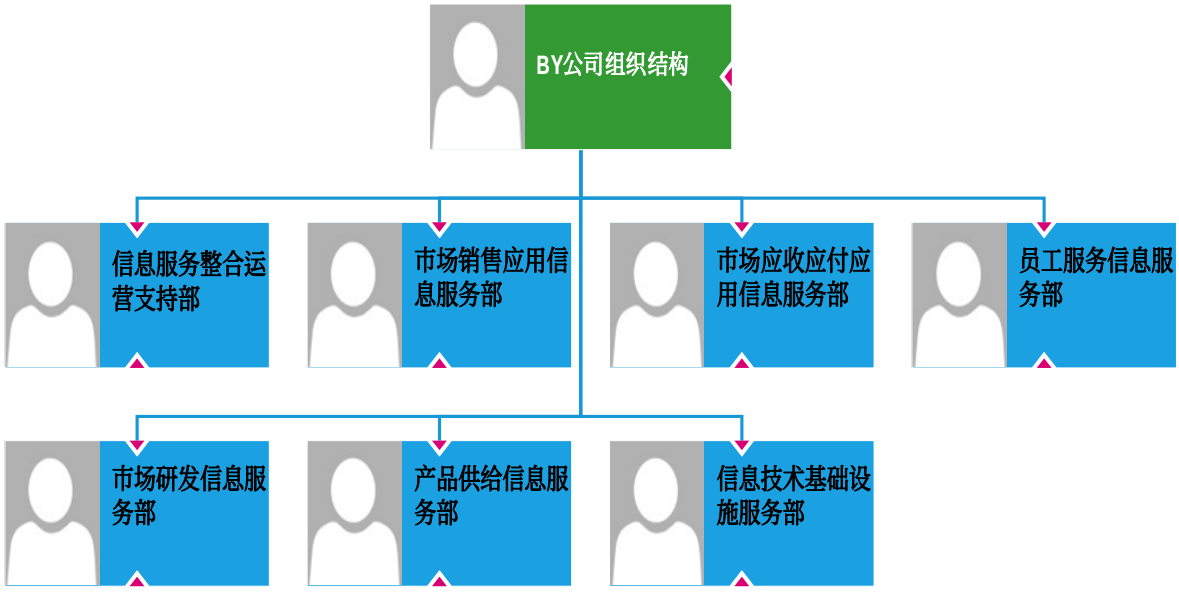

图 3.1 BY 公司组织结构图

Fig. 3.1 BY company organization structure chart

表 3.1 部门职责

Tab. 3.1 Organizational responsibility

编号	部门	职责
1	信息服务整合运营支持部	负责系统服务整合，跨领域运营，供应商管理，质量管理，变更管理等工作。
2	市场销售应用信息服务部	负责基于集团和国内市场营销业务需求，实施客户系管理，会议管理，电商管理，渠道管理，销售业绩管理等信息技术解决方案。
3	市场应收应付应用信息服务部	负责市场应收账款，应付账款等相关信息系统应用的整体信息技术解决方案，包括信息系统应用的立项、实施、管理和维护等工作；负责该领域应用系统中间件的管理、支持和维护等工作。

表 3.1 续

Tab. 3.1 Cont

编号	部门	职责
4	员工服务信息服务部	负责人力资源相关信息系统的规划、建设、实施和支持等工作；负责员工服务系统的支持和相关文档管理；负责员工服务系统的应用项目管理和变更管理。
5	市场研发信息服务部	负责市场早期开发及研发相关信息系统的规划、建设、实施和维护支持工作；负责执行集团和国内基于市场需求的新系统升级项目。
6	产品供给信息服务部	负责国内工厂产品供给相关信息系统解决方案的建立；负责非 SAP 信息产品的服务和项目管理；负责 SAP 相关信息产品的产品规划和质量管理。
7	信息技术基础设施服务部	负责信息系统基础设施设备相关服务管理；负责网络设施服务及中间件管理；负责应用系统平台架构建立及管理。

3.2 BY 公司信息安全管理现存问题

BY 公司成立至今已有将近 10 年的时间。在这个过程中，由于组织架构的调整以及公司策略的相应变化，信息系统架构也发生了多次重大调整。在公司成立之初，信息安全管理体系的确是依照当时的信息系统架构进行设计的。但在后来的信息系统架构调整过程中，信息安全管理体系没有随之进行相应的调整，缺少信息安全风险管理的概念和方法，在面对日益增加的信息安全风险问题时力不从心，因而导致现有安全体系无法满足信息安全的需求，也无法应对日新月异的信息安全威胁。

3.2.1 信息安全管理问题调查

（1） 调查概况

本文主要应用问卷调查和员工访谈的形式, 对 BY 公司信息安全管理问题展开调查。

① 问卷调查

问卷调查的内容一共分为三个部分：

第一部分：主要介绍了这次问卷调查的背景，以及本次调查的主要目的、意义和预期的反馈内容。

第二部分：主要是个人信息搜集。由于这次调查采取的是匿名调查的方式，因此主要向被调查员工收集部门信息、岗位信息以及工作年限等简要信息，以供问卷调查分析时做参考。

第三部分：问卷正文部分。题目的设计分为封闭式问题和开放式问题两种类型。封闭式采用李克特五点量表的方式，接受问卷调查的员工需要根据自己的实际情况真实的进行反馈，得出“非常同意”、“同意”、“不一定”、“不同意”或“非常不同意”五种回答之一。每一个设计问卷主题的得分，将取决于这个主题下细化问题总分的平均分。开放式问题采取调查者手动填写的方式，针对封闭式问题里填写“不同意”或者“非常不同意的”的回答，需要被调查者手动填写出具体不同意的内容。

由于本次问卷调查的时间和空间的局限性，无法面对面发放调查问卷以及回收，所以采取了电子调查问卷的形式进行问卷的发放和回收。

② 员工访谈

在调查问卷的基础上，本次论文研究还针对 BY 公司当前信息安全管理相关问题进行了员工面谈，听取相关员工在当前 BY 公司信息安全管理体系和技术体系方面遇到的问题和反馈。

（2） 调查结果分析

① 问卷调查员工分布情况

本次调查问卷一共发放 78 份，有效回收 69 份，问卷反馈率达到 88.46%，可以代表 BY 公司绝大多数员工的意见。下表 3.2 为调查对象入职年限表。

表 3.2 调查对象入职年限

Tab. 3.2 Respondents' working seniority

入职年限	对应人数
1 年以内	5
1-2 年	18
2-3 年	25
3-5 年	12
5-8 年	7
8 年以上	2

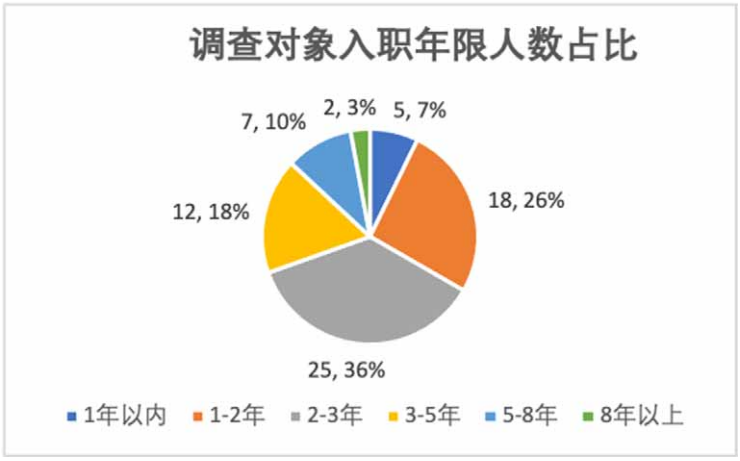

图 3.2　调查对象入职年限分析

Fig. 3.2　Analysis of respondents' working seniority

根据图 3.2 的调查结果可以看出，入职年限在 1-2 年和 2-3 年的员工是本次调查的主体对象，人数分别占总体调查对象的 26%和 36%，两者调查结果合计超过了总体调查样本的一半。基于这个调查结果可以看出，大多数被调查员工的入职时间在 5 年以内，对公司内部信息安全管理的问题调查表现出了很高的积极性，并且在日常工作过程中也经常遇到类似的问题，因此对信息安全管理问题的调查反馈积极，感触很深。

② BY 公司信息安全管理普及情况

针对 BY 公司信息安全管理体系和技术体系相关的问题，各项细化问题调查结果如下表 3.3 所示。

表 3.3　BY 公司信息安全管理普及情况调查表

Tab.3.3　BY company information security management popularization questionnaire

细化问题	正向回答比例
BY 公司的信息安全管理理念先进，制度明确，规范完整，具有质量保障。	12.49%
BY 公司技术人员对信息安全检测和报警有明确的安全分析报告及响应措施。	35.25%
BY 公司有明确的信息安全管理部门及相关人员。	16.73%
BY 公司经常组织具有时效性的信息安全管理相关培训。	18.22%
BY 公司信息系统补丁实施更新。	29.34%
BY 公司具有完整明确的网络分析报告。	27.45%
我对 BY 公司其他部门的工作职责内容十分了解，处理信息安全事件时得心应手。	15.89%

表 3.3 续

Tab.3.3 Cont

细化问题	正向回答比例
我对 BY 公司的物理设备安全十分放心。	30.9%
BY 公司几乎没有发生过网络安全事件。	25.88%
BY 公司的信息安全核心技术手段十分健全。	30.46%

从上述细化问题调查正向回答比例可以看出，BY 公司在信息安全管理技术体系层面的正向反馈比例适中，而在信息安全管理体系层面的正向反馈比例较低，对于像“ BY 公司的信息安全管理理念先进，制度明确，规范完整，具有质量保障 ”这样的问题，正向回答比例只有 12.49%，而像“ 我对 BY 公司其他部门的工作职责内容十分了解，处理信息安全事件时得心应手。”这样的问题，正向回答比例也只有 15.89%。由此可见，BY 公司在信息安全管理方面存在问题。

③ 员工访谈调查结果

本次研究员工调查人数 88 人，有效反馈 82 人，有效反馈率达到 93.18%，访谈主要针对 BY 公司当前信息安全管理的问题，和受访员工进行了开放式访谈，没有固定的问题及回答，主要是想了解公司员工对于当前遇到问题的细节反馈。经访谈发现，当前 BY 公司在信息安全管理体系和技术体系方面都存在着一些问题。比如“ 公司没有信息安全管理体系制度和规范 ”，“ 基本没参加过正式的信息安全相关培训 ”，“ 外部人员也可以连入公司内网查看一些信息 ”，“ 出现信息安全问题时，大家相互推诿 ”，“ 管理账号随便使用 ”，“ 有时候出现电脑无端中病毒的情况 ”等 20 多个细节反馈问题。

3.2.2 信息安全管理问题汇总

基于上述 BY 公司内部问卷调查以及员工访谈的调研结果，总结出当前 BY 公司在信息安全管理方面主要存在以下问题：

（1） 信息安全管理制度不明确

在问卷调查当中，有关于“ BY 公司的信息安全管理理念先进，制度明确，规范完整，具有质量保障 ”这一项的正向回答比是 12.49%，这个数值比较低。在与员工访谈调查当中，了解到随着近几年 BY 集团的战略调整，BY 公司主要将工作重点放在组织架构的调整和信息技术解决方案的实施上，并没有公布各个员工相关工作的信息安全管理规章制度，导致在没有明确信息安管制度的指导下，员工无法在工作的时候识别并预判信息安全事件，在发生信息安全事件后，无法第一时间合理的实施风险应对措施。

（2） 各部门员工职责范围不明确

BY 公司的各个职能部门经历过多次拆分和重组，一些员工在跨部门重组的时候被重新分配到其他部门。在重组之后，BY 公司并没有将各部门的职责范围和工作内容明确的进行协调安排，更多的是沿用拆分之前的工作流程进行工作，导致各部门对其他部门的负责内容和范围不了解，在具体工作当中，一些基本的操作工作没有权限，导致跨部门合作效率低下，无法按时完成总部或国内提出的业务需求。

（3） 信息安全培训不及时

由于缺少行之有效的信息安全管理制度，BY 公司在多次组织调整过程中，很少组织成型的信息安全员工培训，很大程度上依赖于员工自行阅读过去的公司文档。除了在问卷调查当中，“ BY 公司经常组织具有时效性的信息安全管理相关培训 ”该项的正向回答比较低, 在员工采访中, 一位员工表示, 希望公司能够定期举办信息安全相关培训，这样员工在工作当中，就更能够了解到哪些工作内容可能跟信息安全有关系，在工作当中的注意事项是什么，以及当出现信息安全问题事件的时候应该怎样去应对。

3.3 BY 公司信息安全管理问题分析

BY 公司存在的信息安全管理问题，一方面主要是由于组织架构调整造成的，另一方面，BY 公司从创立至今，一直也没有成型的信息安全风险管理概念和方法，缺少有效的风险评估、风险分析及风险控制方案。因此，对 BY 公司信息系统进行信息安全风险管理是十分必要的。

3.3.1 信息安全风险评估

信息安全风险评估，是一项体系化工作[16]，主要包括“ 确认范围 ”，“ 识别和评估资产风险 ”，“ 识别和评估资产威胁 ”，“ 识别和评估资产脆弱性 ”，以及“ 评估风险控制措施 ”几个方面。本文通过对 BY 公司信息系统相关资产的风险评估，可以充分了解对这些资产采取进一步风险控制措施的必要性和优先级。

（1） 确认范围

对 BY 公司的企业用户来说, BY 公司的信息系统充当了企业运营“ 数字引擎 ”的角色。为了保证 BY 公司信息系统能够正常运维，并确保业务的可持续运行，与其相关的基础设施, 信息系统, 人员管理, 甚至是组织架构都有可能对其信息安全管理产生影响。因此，本文将通过以下几个方面，对 BY 公司信息系统进行风险评估，具体信息如下表 3.4 所示：

表 3.4　BY 公司信息系统风险评估范围

Tab.3.4　BY company information system risk analysis scope

评估项目类型	评估项目描述
组织架构	BY 公司信息系统的管理组织架构特性；是否具有完备的信息安全管理组织架构等。
员工管理	信息安全管理制度；员工职责范围；员工工作流程；员工培训制度等。
基础设施	BY 公司信息系统运维相关的物理硬件设备、网络线路、物理设备所处环境等。
信息系统	系统运维相关的服务器操作系统，配置功能软件，监控软件等。

（2） 识别和评估资产重要度

信息系统相关资产，是指对公司或者部门具有实际应用价值的信息或者资源，也是信息系统安全策略需要重点保护的目标对象[17]。BY 公司信息系统底层的硬件设施、软件环境以及对信息系统相关制度和人员的管理，是保证 BY 公司持续稳定运营的企业资产，也是进行风险评估的重要对象。当信息系统遭遇攻击或者受到破坏时，这些资产价值的变化决定了公司或者部门受到负面影响的程度。

在对 BY 公司信息系统相关资产做出风险评估之前，本文首先需要了解要进行风险评估的资产是什么，以及具有哪些特点。因此，本文按照如下方式，对 BY 公司信息系统进行资产分类[18]，具体如下表 3.5 所示：

表 3.5　BY 公司信息系统资产分类表

Tab.3.5　BY company information system asset classification table

主要资产类别	次级资产类别	资产名称	资产描述
管理资产	组织关系	组织架构图	组织架构图，能够清楚的展现出当前 BY 公司的组织架构关系和部门职责范围。
	文档	信息安全管理制度	具有指导性意义的信息安全管理制度信息，是 BY 公司信息安全保障的依存框架，确保 BY 公司内部员工能够按照其具体规章制度工作。
		员工职责范围	清楚的阐述员工的具体工作内容，工作职责，工作范围等。

表 3.5　续

Tab.3.5　Cont

主要资产类别	次级资产类别	资产名称	资产描述
管理资产	文档	信息安全培训制度	针对提高员工信息安全防护意识和信息安全管理态度的系统培训机制。
技术管理资产	物理安全	基础设施	BY 公司信息系统运维底层的基础设施结构，如物理硬件环境、网络链路等信息。
		服务器	承载 BY 公司运维系统的服务器物理硬件。
		网络设备	维持 BY 公司信息系统正常运维网络链路上的网络物理设备，如交换机、防火墙、中继器等。
	信息系统	服务器系统	承载 BY 公司信息交互服务器系统。
		数据库系统	处理 BY 公司信息系统数据请求、数据交换等信息的数据库系统。
		数据库软件	处理 BY 公司信息系统数据请求、数据交换等信息的数据库软件。
		应用系统	支持并处理 BY 公司应用信息交互的应用管理系统。

在确认进行本次风险评估的资产信息后，本文需要进一步确认这些资产的重要程度，并对其划分等级和赋值。资产的重要程度等级，主要取决于资产的可用性、完整性和保密性这三个属性对业务的影响。赋值大小可以分为从 1 到 5 五个赋值等级，等级越高，其影响也越大。

这里以 BY 公司“信息安全管理制度”的资产重要度赋值过程为例。BY 公司 “信息安全管理制度”的可用性赋值是 5。其性价值最高，公司如果没有信息安全管理制度，所有信息安全相关管理将毫无章法，对业务影响非常大；BY 公司“信息安全管理制度”的完整性赋值是 5。其性价值高，信息安全管理制度的完善不是一蹴而就的工作，难以快速拟定制度，并且对业务运行影响较大；BY 公司 “信息安全管理制度”的保密性是 4。因为公司的“信息安全管理制度”属于公司内部的秘密信息，如果该信息泄露会对公司造成重大影响。

基于上述资产赋值方法，并结合信息技术人员咨询结果以及相关行业经验，对 BY 公司信息系统进行资产赋值，如下表 3.6 所示：

表 3.6　BY 公司信息系统资产属性赋值表

Tab.3.6　BY company portal information system asset attributes assignment table

资产属性	资产名称	资产重要度等级赋值
保密性	组织架构图	4
	信息安全管理制度	4
	员工职责范围	3
	信息安全培训制度	3
	基础设施	1
	服务器	1
	网络设备	1
	服务器系统	3
	数据库系统	2
	数据库软件	2
	应用系统	3
完整性	组织架构图	5
	信息安全管理制度	5
	员工职责范围	5
	信息安全培训制度	5
	基础设施	5
	服务器	3
	网络设备	3
	服务器系统	3
	数据库系统	2
	数据库软件	2
	应用系统	3
可用性	组织架构图	5
	信息安全管理制度	5
	员工职责范围	5
	信息安全培训制度	5
	基础设施	5
	服务器	3
	网络设备	3
	服务器系统	4
	数据库系统	2
	数据库软件	2
	应用系统	4

由上表可以了解到 BY 公司信息系统资产在保密性、完整性和可用性三个维度的赋值情况，综合上述数据，通过资产等级赋值加权计算的方式[19]，可以得出 BY 公司信息系统的资产重要度赋值等级，如下表 3.7 所示：

表 3.7　BY 公司信息系统资产重要度赋值表

Tab.3.7　BY company information system asset importance assignment table

资产名称	资产重要度综合赋值等级
组织架构图	4.6
信息安全管理制度	4.6
员工职责范围	4.2
信息安全培训制度	4.2
基础设施	2.9
服务器	2.1
网络设备	2.1
服务器系统	3.3
数据库系统	2.0
数据库软件	2.0
应用系统	3.3

（3） 识别和评估威胁

威胁是指公司或组织所使用的资产引起不可预见的事故，而对公司或组织的利益或者安全造成损害的可能性[20]。为了确保 BY 公司信息系统能够持续稳定运行，保证业务运营不受到影响，对信息系统资产威胁的识别，需要通过风险评估过程，确认可能对其资产造成潜在风险的威胁，并分析其威胁发生的概率，从而多维度了解当前 BY 公司信息系统的资产威胁。

BY 公司信息系统的正常运行，受到物理环境，网络环境，运营管理等多重因素的影响。功能模块底层软硬件的故障，信息系统安全管理制度的不完善等，都有可能对门户网站的稳定运行造成威胁。因此，根据其不同来源的信息安全威胁，BY 公司信息系统的威胁可以分为 11 个大的类别。具体威胁分类和相关描述如下表 3.8 所示：

表 3.8　BY 公司信息系统威胁分类表

Tab. 3.8　Threat classification table of BY company information system

威胁主类	威胁子类	威胁描述
软件硬件故障	基础硬件设施故障，系统软件应用故障等。	业务应用系统相关软硬件设施的软件不可用、系统缺陷和硬件等。
操作失误	操作指导手册错误，操作方法错误等。	运维人员执行错误的操作，或者没有按照要求进行操作。
物理环境的影响	静电影响、地震影响、灰尘影响等。	底层基础设施内部物理环境、外部自然环境等对信息系统的正常运行造成的影响。
管理疏忽	管理规章制度不健全，监管不力，职责划分不明确。	由于管理问题的，造成信息系统安全管理隐患和问题。
越权或滥用	未经授权访问公司内部网站、未经授权访问公司内部存储媒介等。	内部工作人员通过利用技术手段，越过本应该遵守的信息安全管理流程，来访问未经授权的信息系统模块信息。
恶意代码	病毒、木马、流氓软件、垃圾邮件等。	在信息系统上留下的恶意执行代码程序。
物理攻击	故意破坏物理基础设施、偷窃物理设备等。	通过物理形式的接触，对信息系统相关的软硬件进行破坏。
篡改	篡改网络配置信息、篡改用户访问权限信息等。	通过非法利用的技术手段，篡改或者破坏信息系统的可用性或者完整性。
网络攻击	窃取用户使用数据、网络攻击应用服务器、非法模拟用户身份下载信息系统内部资源等。	通过网络途径，利用非法技术入侵和破坏信息系统。
泄密	内外部信息系统信息的泄露等。	将系统内部信息泄露给不应该接触该信息的人员。
抵赖	接触信息抵赖、自发抵赖或者他方触发抵赖等。	对通过非法途径得到的信息系统相关信息，或者发生不应该存在的交易和操作不予以承认。

不同威胁类型，同时还具有不同的威胁特性。对资产产生威胁的不同特性，可以从威胁的“攻击能力”，“威胁发生概率”和产生威胁之后的“影响程度”这三个方面进行考察，其考察标准如下表 3.9 所示：

表 3.9　BY 公司信息系统威胁特性表

Tab. 3.9　Threat feature table of BY company information system

威胁特性	威胁程度	威胁值	具体描述
攻击能力	高	3	威胁的攻击能力强，发生攻击之后对信息系统的影响巨大，短时间内难以修复。
	中	2	威胁的攻击能力适中，发生攻击之后对信息系统的影响一般，一段时间内可以修复。
	低	1	威胁的攻击能力小，发生攻击之后对信息系统的影响很小，可暂时不进行修复。
威胁发生概率	高	3	威胁发生的可能性很大，出现威胁后，信息系统很可能会受到影响。
	中	2	威胁发生的可能性一般，出现威胁后，信息系统会受到影响，不过影响程度一般。
	低	1	威胁发生的可能性很小，即使出现该威胁，信息系统也可以正常运行。
影响程度	高	3	出现威胁后，信息系统受到巨大影响，造成的损失很大。
	中	2	出现威胁后，信息系统受到影响适中，造成一度程度的损失。
	低	1	出现威胁后，信息系统几乎不受影响，造成的损失也可忽略不计。

在了解不同的威胁类别以及其对应的威胁特性后，本文需要对 BY 公司信息系统资产的潜在威胁进行赋值。

这里以 BY 公司“信息安全管理制度”为例。该资产威胁的主要类型属于“管理疏忽”。通过人员面谈调查了解到，BY 公司各个部门经历多次拆分和重组后，其信息安全管理制度并没有随着公司组织架构的变化和当前信息技术方案的需求进行完善调整，导致工作人员在处理信息安全管理事件的时候无章可循。由于缺少成型的信息安全管理制度，出现信息安全事件的可能性很大，对信息系统的影响巨大，造成的损失也很大，因此其威胁特性“攻击能力”的赋值是 3，“威胁发生概率”的赋值是 3，“影响程度”

的赋值是 3，通过加权计算的方式得出 BY 公司“信息安全管理制度”这个资产的威胁赋值是 3。

依据上述分类和赋值方法,得出 BY 公司信息系统资产的威胁分类和威胁赋值信息,如下表 3.10 所示：

表 3.10　BY 公司信息系统威胁分类赋值表

Tab. 3.10　Threat classification and assignment table of BY company information system

资产名称	威胁主类	攻击能力	威胁发生频率	影响程度	威胁赋值
组织架构图	管理疏忽	3	1	2	1.8
信息安全管理制度	管理疏忽	3	3	3	3.0
员工职责范围	管理疏忽	3	3	3	3.0
信息安全培训制度	管理疏忽	3	3	3	3.0
基础设施	物理环境影响	3	1	3	2.1
服务器	软件硬件故障	3	1	3	2.1
网络设备	网络攻击	2	1	2	1.6
服务器系统	篡改	3	2	3	2.6
数据库系统	越权或滥用	2	1	2	1.6
数据库软件	软件硬件故障	2	1	2	1.6
应用系统	泄密	2	3	3	2.6

（4） 识别和评估脆弱性

为了保证 BY 公司信息系统的持续稳定运行，需要其既能保证具有合理的公司管理制度、安全管理策略，又要保证其基础设施稳定，信息系统运行环境优良。这些基本因素可能被攻击或者利用，也有可能产生漏洞或者具有薄弱环节。因此，识别 BY 公司信息系统资产脆弱性的目的，是为了确认哪些因素构成了 BY 公司信息系统正常运行的脆弱性，并分析其可能对资产造成潜在信息安全风险的损害程度。

BY 公司信息系统资产的脆弱性，主要可以分为资产管理脆弱性和资产技术脆弱性两个方面[21]。具体分类信息如下表 3.11 所示：

表 3.11　BY 公司信息系统脆弱性分类表

Tab. 3.11　Vulnerability classification table of BY company information system

脆弱性分类	脆弱性识别对象	具体描述
管理脆弱性	组织管理	BY 公司组织架构关系，部门职责范围清晰度，组织文化等。

表 3.11　续

Tab.3.11　Cont

脆弱性分类	脆弱性识别对象	具体描述
管理脆弱性	制度管理	信息安全管理制度的完整度，可执行度等。
	员工管理	员工的工作内容，工作职责范围，工作流程等。
	系统运维管理	系统操作，系统配置，系统分析，系统维护等。
技术脆弱性	基础设施	信息系统底层基础设施物理环境防护能力。
	物理设备	信息系统相关物理设备防护能力。
	操作系统	服务器系统，软件系统等的信息安全防护能力。
	应用系统	应用系统的数据应用和数据传输等方面的防护能力。

资产脆弱性具有不同的特质，可以从“资产脆弱性暴露程度”，“脆弱性被利用难以程度”以及“脆弱性流行程度”几个方面进行判定，其判定标准如下表 3.12 所示：

表 3.12　BY 公司信息系统资产脆弱性特质表

Tab. 3.12　Vulnerability feature table of BY company information system

脆弱性特质	脆弱性程度	脆弱性赋值	具体描述
资产脆弱性暴露程度	高	3	信息系统资产脆弱性暴露程度很高，如被威胁利用，产生的损失巨大。
	中	2	信息系统资产脆弱性暴露程度一般，如被威胁利用，产生一定的损失。
	低	1	信息系统资产脆弱性暴露程度很小，即使被威胁利用，产生的损失也可以忽略不记。
脆弱性被利用难易程度	高	3	信息系统资产脆弱性很容易被资产的威胁利用。
	中	2	信息系统资产脆弱性在一定程度上可能被资产威胁利用，难度适中。
	低	1	信息系统资产脆弱性很难被资产的威胁利用。
脆弱性流行程度	高	3	信息系统资产的脆弱性十分普遍，被威胁利用的可能性非常高。
	中	2	信息系统资产脆弱性的流行度适中，被威胁利用的可能性一般。
	低	1	信息系统资产脆弱性不流行，被威胁利用的可能性很小。

在确认进行资产脆弱性识别的对象后，本文还需要对 BY 公司信息系统资产的脆弱性进行赋值。

这里以 BY 公司的“员工职责范围”为例。BY 公司员工在信息安全管理方面的职责范围不明确，流程不清晰，当出现信息安全问题的时候相互推诿，推卸责任，导致信息安全事件不能得到及时有效的解决。可见该资产脆弱性在公司内部十分普遍，很容易被威胁所利用，暴露程度很高，给业务部门的稳定运行带来巨大风险隐患，产生的潜在损害程度严重。因此，该资产脆弱性特质的赋值分别为：“资产脆弱性暴露程度”的赋值是 3，“脆弱性被利用难易程度”是 3，“脆弱性流行程度”是 3，通过加权计算的方式得出 BY 公司信息系统资产“员工职责范围”的脆弱性赋值是 3。

依据上述分类和赋值方法，得出 BY 公司信息系统资产的脆弱性分类和赋值信息，如下表 3.13 所示：

表 3.13　BY 公司信息系统脆弱性分类赋值表

Tab. 3.13　Vulnerability classification and assignment table of BY company information system

资产名称	脆弱性识别对象	资产脆弱性暴露程度	脆弱性被利用难易程度	脆弱性流行程度	脆弱性赋值
组织架构图	组织管理	2	2	3	2.3
信息安全管理制度	制度管理	3	3	3	3.0
员工职责范围	员工管理	3	3	3	3.0
信息安全培训制度	员工管理	3	3	3	3.0
基础设施	基础设施	2	1	2	1.6
服务器	物理设备	2	1	2	1.6
网络设备	物理设备	1	1	1	1.0
服务器系统	操作系统	2	2	2	2.0
数据库系统	操作系统	1	1	1	1.0
数据库软件	应用系统和软件	1	1	1	1.0
应用系统	应用系统和软件	3	3	3	3.0

（5） 评估已有的风险控制

在对 BY 公司信息系统相关的资产信息，资产威胁和资产脆弱性进行评估后，本文需要评估当前已有的风险控制措施[22]。这样做的目的主要分为两个方面：第一，为了保证 BY 公司信息系统的稳定运行，确认当前既有的信息安全风险管理措施是否有效。行之有效的管理措施将继续进行使用，不再重新规划对应管理措施，避免造成资源浪费；

第二，确认 BY 公司信息安全风险管理的漏洞，查看在哪些方面的管理措施需要更改、修正或者完善，达到建立完整风险管理体系的目的。

当前已有风险控制措施，可以通过以下方式进行赋值和定义，具体如下表 3.14 所示：

表 3.14　BY 公司信息系统风险控制有效度定义表

Tab. 3.14　Risk control effectiveness definition table of BY company information system

控制措施有效程度	有效程度赋值	具体描述
很好	1	当前已有的风险控制措施很好，BY 公司信息系统资产威胁利用脆弱性产生的风险很大程度都被控制住。
一般	2	当前已有的风险控制措施一般，BY 公司信息系统资产威胁利用脆弱性产生的一部分风险被控制住。
不好	3	当前已有的风险控制措施不好，BY 公司信息系统资产威胁利用脆弱性产生的风险完全不受控制，对业务影响巨大。

BY 公司在拆分和重组的过程中，并没有将重点放在公司资产的信息安全管理上，很大程度上是维持原有的管理政策。因此，按照上述已有风险控制措施的判定标准，结合 BY 公司员工面谈的调查结果，总结出当前 BY 公司信息系统资产的风险控制措施有效程度，如下表 3.15 所示：

表 3.15　BY 公司信息系统风险控制有效度赋值表

Tab. 3.15　Risk control effectiveness assignment table of BY company information system

资产名称	风险控制措施有效程度	有效度赋值
组织架构图	一般	2
信息安全管理制度	不好	3
员工职责范围	不好	3
信息安全培训制度	不好	3
基础设施	很好	1
服务器	很好	1
网络设备	很好	1
服务器系统	不好	3
数据库系统	很好	1

表 3.15　续

Tab.3.15　Cont

资产名称	风险控制措施有效程度	有效度赋值
数据库软件	很好	1
应用系统	不好	3

3.3.2　信息安全风险分析

在对 BY 公司信息系统资产的进行风险评估后，要对这些资产进行信息安全风险分析，定量计算得出对应的风险值。通过对比风险控制标准，来判定是否针对某些资产风险采取进一步风险控制措施。

本文主要采用“ 相乘法 ”来定量计算 BY 公司信息系统对应资产的风险值，其具体公式如下：

$$R = A \times T \times V \times M \tag{3.1}$$

在这个公式中，R 代表该资产的风险值，A 代表资产重要度综合赋值等级，T 代表资产威胁赋值等级, V 代表资产脆弱性赋值等级, M 代表已有风险控制措施的有效程度。

这个公式主要体现出资产风险和资产重要度等级，资产威胁等级，资产脆弱性等级和已有控制措施有效度之间的关系。资产越重要，其受威胁产生风险的潜在影响越大；资产威胁程度越大，资产脆弱性越明显，其资产产生风险的可能性越大；如果已有的风险控制措施效果不好，则风险产生的影响也就越大。

（1） 信息安全风险计算实例

这里以 BY 公司信息系统资产“ 信息安全管理制度 ”为例。如前文所述，该资产重要度综合赋值等级为 4.6，资产威胁赋值等级为 3，资产脆弱性赋值等级为 3，该资产对应已有风险控制措施的有效程度为 3，因此，根据本文所采用的风险值计算模型，得出 BY 公司信息系统资产“ 信息安全管理制度 ”的风险值为 125。

因此，本文基于 BY 公司信息系统资产风险评估结果和上述风险值的计算方法，总结出 BY 公司信息系统资产风险值如下表 3.16 所示：

表 3.16　BY 公司信息系统资产风险值表

Tab. 3.16　Asset risk value table of BY company information system

资产名称	重要度赋值	威胁赋值	脆弱性赋值	风控措施有效程度赋值	风险值
组织架构图	4.6	1.8	2.3	2	39

表 3.16　续

Tab. 3.16　Cont

资产名称	重要度赋值	威胁赋值	脆弱性赋值	风控措施有效程度赋值	风险值
信息安全管理制度	4.6	3.0	3.0	3	125
员工职责范围	4.2	3.0	3.0	3	114
信息安全培训制度	4.2	3.0	3.0	3	114
基础设施	2.9	2.1	1.6	1	10
服务器	2.1	2.1	1.6	1	7
网络设备	2.1	1.6	1.0	1	3
服务器系统	3.3	2.6	2.0	3	52
数据库系统	2.0	1.6	1.0	1	3
数据库软件	2.0	1.6	1.0	1	3
应用系统	3.3	2.6	3.0	3	78

（2） 信息安全风险值判定

在确认采取进一步风险控制措施之前，首先确认要进行风险控制的标准。本次风险评估的控制标准，将主要分为以下三个风险等级进行定义和判定，具体如下表 3.17 所示：

表 3.17　BY 公司信息系统风控判定标准

Tab. 3.17　Risk analysis control standard of BY company information system

风险等级	风险值	风险等级描述
高	100 – 150	资产风险程度很高，如已有风险控制措施方案，需立即采取风险控制措施；如还没有风险控制方案，需立即制定并采取风险控制措施方案，防止资产风险带来的潜在业务影响。
中	50 – 100	资产风险程度一般，如已有风险控制措施方案，需按照计划采取风险控制措施；如还没有风险控制方案，需按计划制定并采取风险控制措施方案，防止资产风险扩大。
低	0 - 50	资产风险程度很小，带来的潜在业务影响较小，积极观察风险是否会进一步扩大，暂不采取任何风险控制措施。

因此，对比上述风险控制标准，总结出对 BY 公司信息系统资产风险控制的优先级如下表 3.18 所示：

表 3.18　BY 公司信息系统风险控制优先级

Tab. 3.18　Risk analysis priority of BY company information system

资产名称	风险值	风险等级
信息安全管理制度	125	高
员工职责范围	114	高
信息安全培训制度	114	高
应用系统	78	中
服务器系统	52	中
组织架构图	39	低
基础设施	10	低
服务器	7	低
网络设备	3	低
数据库系统	3	低
数据库软件	3	低

通过上述定性定量的风险评估和风险分析方式，可以看出 BY 公司信息系统资产“信息安全管理制度”，“员工职责范围”和“信息安全培训制度”的风险等级“高”。由于这些资产缺少已有的风险控制措施，因此要立即制定并采取风险控制措施方案，防止这些资产风险带来的潜在业务影响。

3.3.3　信息安全风险成因

通过对 BY 公司信息系统风险问题的综合评估和分析，总结出当前 BY 公司信息系统存在的主要风险及原因如下：

（1）　信息安全管理制度不健全

BY 公司在成立之初，制定了适应当时公司运营环境的信息安全管理制度。但是近几年来，BY 集团进行了多次战略调整，促使 BY 公司为之服务的信息系统架构发生了多次改变。然而在这个变化的过程中，BY 公司的信息安全管理制度并没有及时更新。各个职能部门在经历多次拆分和重组后，也只是各负其责，并没有针对公司信息安全管理制度的问题开展深入探讨，导致全公司缺少统一的信息安全管理制度，给集团的业务运营造成了重大影响。

（2）　员工职责范围不明确

各个职能部门在经历多次拆分和重组的同时，各部门员工的工作内容和工作范围也随之发生了变化。一些员工在组织变动的过程中，从一个部门调到另一个部门，而工作内容没有进行完整的交接工作，这就导致在进行实际工作的过程中，无法很清晰的界定哪些工作由哪些同事负责，只能在遇到具体问题的时候又各部门领导相互协调；当遇到信息安全事件相关的问题时，由于缺少统一规范的工作流程，同事之间更是相互推诿，推卸责任。

（3） 缺少成型的员工信息安全培训

BY 公司在拆分和整合的过程中，并没有制定成型的信息安全培训相关流程。公司的高层管理者主要将工作重心放到了支持集团业务运行的运维活动和项目活动中，信息安全管理这个话题并没有引起管理人员的重视，因此，也没有安排成型的员工信息安全培训。也正是由于这样的原因，员工缺乏信息安全管理防护意识，信息安全事件频频发生，给业务的持续稳定运行造成了巨大影响。

本章首先通过对 BY 公司的介绍，了解到 BY 公司主营业务方向、公司发展历程以及组织人员架构；其次，通过问卷调查和员工访谈的形式，了解到 BY 公司在 BY 集团战略发展调整过程中的重要地位，以及组织架构变动带来的潜在信息安全管理问题，如信息安全管理制度不明确，各部门员工职责范围不明确，信息安全培训不及时等，同时简要分析其原因；再次，通过对 BY 公司信息系统进行定性定量的风险评估和风险分析，了解到 BY 公司在“信息安全管理制度”、“员工职责范围”以及“员工信息安全培训”方面存在信息安全风险。这些问题亟待解决，否则将继续对 BY 公司所支持的 BY 集团业务造成重大影响。

4 BY 公司信息安全管理解决方案

4.1 BY 公司信息安全风险控制方案

前文通过对 BY 公司信息安全管理问题的调查以及对 BY 公司信息系统对应资产的风险分析，了解到当前 BY 公司现存信息安全风险的主要问题。下面将基于不同风险控制的原则[23]、风险控制的策略[24]以及风险的控制机制[25]，针对性的对现存主要问题提出信息安全风险控制方案。

4.1.1 信息安全管理制度

BY 公司信息安全管理制度不健全，是当前 BY 公司信息安全管理面临的主要问题。近几年，尽管 BY 集团做了多次战略调整，BY 公司的信息安全管理制度并没有随之改变，导致员工在面对信息安全这个话题时候缺少指导理念，给集团的业务运营造成了重大影响。

因此，针对 BY 公司“信息安全管理制度不健全”的信息安全风险，将主要从以下几个方面进行风险控制：

（1） 制定完善的信息安全管理制度

首先，在 BY 公司内部大力宣传信息安全管理的重要性，通过 BY 公司各管理部门共同商定，将信息安全管理作为 BY 公司文化管理的一部分；其次，为了规避缺少明确信息安全管理制度的风险，BY 公司各管理部门共同商定，废除旧的信息安全管理条例，并重新制定完善的信息安全管理制度。同时，将不同信息安全管理制度的颁布时间和开始执行日期通知给每一个 BY 公司的员工。

（2） 信息安全管理制度文档管理

BY 公司将制定多条信息安全管理制度，每条信息安全管理制度都包括详细的执行流程和文档信息，如果仅通过电子邮件或者纸质文档的形式存储，这些管理制度信息很容易发生丢失或者泄露。因此，将开发并实施 BY 公司内部专用的文档管理系统。这种管理系统不仅可以保存信息安全管理制度信息，还可以配置子系统网站，用于各部门的内部交流信息存储；同时，还可以将文档管理系统进行安全分级配置，从而保证存储文档的安全。

（3） 信息安全管理制度执行管理

在颁布新的信息安全管理制度之后，由 BY 公司各部门领导主管各部门员工信息安全管理政策执行的情况。对于未按照政策要求执行的人员，各部门领导需要制定员工信息安全再培训计划，要求员工按照培训方案再次学习信息安全管理制度细则并予以执行；

对于执行情况屡次出现问题的员工，各部门领导将首先给予部门内部薪资处罚；情节严重者，将进行公司级别的通报批评，并予以开除。

（4） 信息安全管理制度风险控制实例

这里以“信息安全管理制度文档管理”的实施方案为例。在确定具体的实施方案之前，首先要考虑到执行该计划涉及到的成本，通过成本效益分析的形式，来确定执行该方案的可行性和有效性。

BY 集团当前已经具有成型的文档管理系统框架，同时还有 BY 集团指定的系统开发合作供应商。从控制成本的角度出发，BY 公司可以将此项提案与 BY 集团进行商定，以最优惠的价格选择 BY 集团指定的当地供应商。根据 BY 公司当前的部门职责划分，信息服务整合运营支持部经理将主导该项风险控制方案的具体协调和实施。对于该文档管理系统的功能性要求如下表 4.1 所示：

表 4.1　BY 公司文档管理系统功能及描述

Tab. 4.1　Function and description of BY company document management system

功能项目	具体描述
系统模块管理	可以用来增加或者删除文档管理系统模块，具有方便文档进行上传，编辑，下载，整理等功能。
文档权限管理	将文档管理系统的访问用户，通过授予不同权限，来限制用户对文档进行修改的程度和范围。
文档分类管理	通过该文档系统的筛选选项，可以通过点击该选项来自动筛选不同安全分级的文档。

该项实施方案的具体执行流程，如下图 4.1 所示：

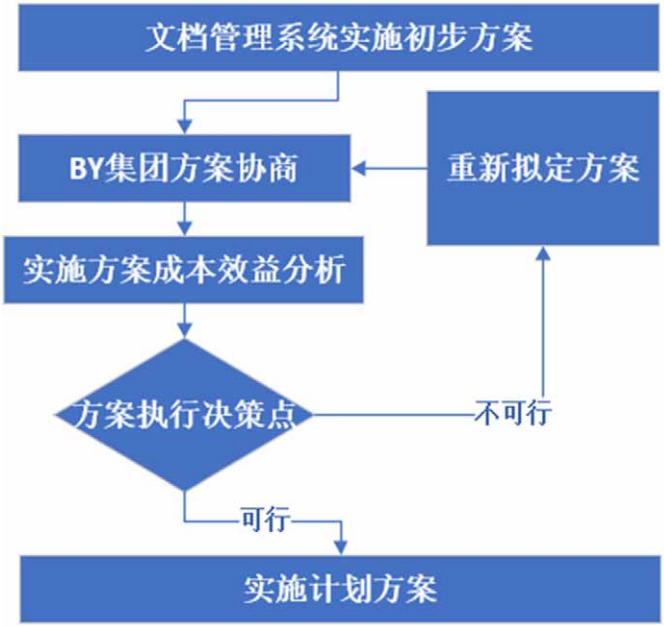

图 4.1　BY 公司文档管理系统实施方案流程图

Fig. 4.1　BY company document management system implementation plan

4.1.2　员工职责范围

BY 公司在经历了多次部门的拆分和重组后，没有明确说明各个员工的职责范围。当面对信息安全事件相关的问题时，由于缺少统一规范的工作流程，员工在工作的过程中相互推诿，无法及时有效的解决信息安全问题，给业务部门造成了重大影响。

因此，针对 BY 公司“ 员工职责范围不明确 ”的信息安全风险，将主要从以下几个方面进行风险控制：

（1） 明确各部门员工的工作内容和工作职责范围

首先，BY 公司各部门领导一起开会，将各部门当前的主要工作目标和工作内容透明化，清晰明了的展示给其他各部门领导人员，如“ 市场销售应用信息服务部 ”要陈述哪些 BY 公司应用属于市场销售应用，这些应用的针对业务群体是哪些业务部门，业务部门对口的是哪些同事，哪些同事是系统策略管理员，哪些同事是系统应用管理员，哪些同事是系统资产管理员等；其次，由“ 信息服务整合运营支持部 ”牵头，将 BY 公司各部门工作内容和工作职责范围整理并文档化，以流程图的形式展现各部门之间的关系、以及各部门和业务部门之间的关系。

（2） 明确各部门员工的信息安全相关工作流程

首先，BY 公司各部门领导负责协调普及部门员工信息安全知识，让部门员工具有信息安全防范意识；其次，发生信息安全问题的时候，由发现该问题的员工将安全问题

反馈给部门领导。该部门领导再通过安全问题反馈邮件组，以电子邮件的形式通报给信息安全管理部门及其他领导部门；最后，根据 BY 公司信息安全管理的不同策略，由信息安全管理部门判定该信息安全事件的处理方案，如需部门同事进一步进行操作，将由该部门同事共同协调处理，直至信息安全问题得以解决。

（3） 员工职责范围风险控制实例

这里以市场销售应用信息服务部的“应用经理”岗位设计为例。首先，该部门经理需将这个岗位的具体信息，呈现给其他部门经理一起商讨其工作内容和工作职责范围的合理性和可行性，具体岗位信息如下表 4.2 所示：

表 4.2 市场销售应用信息服务部“应用经理”岗位初步设计

Tab. 4.2 Initial design of position “Application Manager” in ITO MS department

工作项目	岗位具体信息
岗位名称	应用经理
岗位级别	经理级 VS1.1 级别
岗位工作内容	基于集团和国内市场营销业务需求，制定并实施客户系管理系统，会议管理系统，电商管理系统，渠道管理系统，销售业绩管理系统等信息系统解决方案。
岗位职责范围	负责集团和国内市场销售应用管理。
岗位合作部门及联系人	市场销售应用信息服务部职能经理；供应商应用管理服务部项目经理；国内市场销售业务部门协调经理；集团市场销售应用信息部协调经理。

其次，根据各部门领导对于此岗位设计的反馈，提出相关的意见和建议，并在此基础上重新定义此岗位设计的具体内容，其工作流程如下图 4.2 所示：

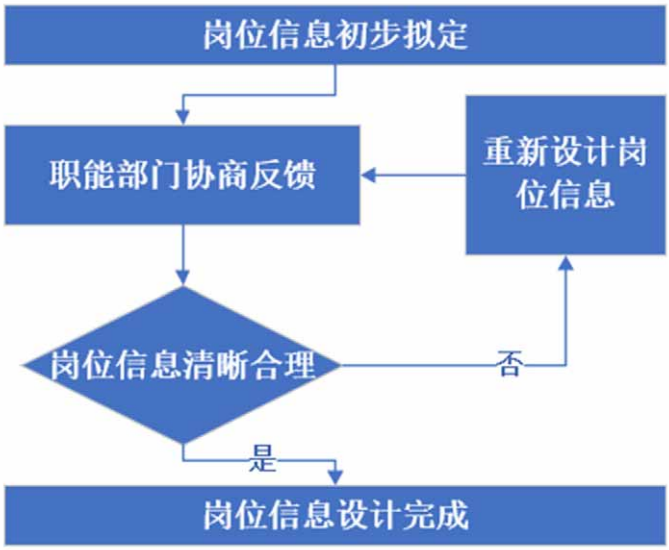

图 4.2　BY 公司员工岗位设计工作流程图

Fig. 4.2　BY company employee position design working flow

比如，在市场销售应用信息服务部经理提出的第一版“ 应用经理 ”岗位工作信息之后，其他各部门职能经理表示，当前这个职位的工作内容和职责范围比较清晰，不过缺少有关信息安全管理方面的具体职责和工作流程。如果缺少这些信息，该部门将无法进行有效的信息安全管理，同时当出现公司级信息安全管理事件时，部门之间的沟通和协调仍会存在障碍。

因此，在全体各部门职能经理一致同意的基础上，最终该“ 应用经理 ”岗位的工作项目和工作具体信息如下表 4.3 所示：

表 4.3　市场销售应用信息服务部“ 应用经理 ”岗位设计

Tab. 4.3　Final design of position “Application Manager” in ITO MS department

工作项目	岗位具体信息
岗位名称	应用经理
岗位级别	经理级 VS1.1 级别
岗位主要工作内容	基于集团和国内市场营销业务需求，制定并实施客户系管理系统，会议管理系统，电商管理系统，渠道管理系统，销售业绩管理系统等信息系统解决方案。

表 4.3　续

Tab. 4.3　Cont

工作项目	岗位具体信息
岗位附加工作内容	在运维管理本部门应用系统时，提高信息安全防范意识。当本部门可能出现信息安全风险，或已经发生的信息安全问题时，及时将实际情况汇报给本部门职能经理，并由本部门经理和信息安全管理部门负责人共同商定进行风险控制的措施以及应对信息安全问题的方案。
岗位职责范围	负责集团和国内市场销售应用管理。
岗位合作部门及联系人	市场销售应用信息服务部职能经理；供应商应用管理服务部项目经理；国内市场销售业务部门协调经理；集团市场销售应用信息部协调经理。

4.1.3　信息安全培训

BY 公司缺少成型的员工信息安全培训机制。公司内部的信息安全管理文化十分匮乏，在这样的工作环境下，员工缺少信息安全防护意识和强化信息安全管理的态度，从而导致 BY 公司的信息安全问题无法得到有效控制。

因此，针对 BY 公司“缺少成型员工信息安全培训”的信息安全风险，将主要从以下几个方面进行风险控制：

（1）　明确员工信息安全的培训内容

在信息安全管理部门的指导下，明确当前 BY 公司信息安全管理工作的工作重点，安排对当前业务运行起到积极影响作用的培训内容，如“员工钓鱼邮件防护安全培训”，“禁用 U 盘拷贝文件安全培训”，“个人隐私安全防护培训”等；信息安全管理部门的领导，要定期跟踪并分析公司内部潜在的信息安全风险，同时结合当前国内外比较热门的信息安全事件管理办法，制定安排合理的培训内容。

（2）　确定员工信息安全的培训形式和培训频率

BY 公司信息安全培训将通过线上和线下培训相结合的形式进行。线上通过员工培训系统，每个月安排一次员工必须完成的线上培训，并将员工是否完成线上培训的报告发送给各位员工的直属经理；线下每 3 个月安排一次信息安全管理宣传大会，由信息安管部门进行会议安排，并要求全员参加该线下培训；同时，与外部信息安全培训专家合作，进行年度信息安全理念教育培训，确保全体员工的信息安全防护理念得到逐步提升。

（3）　跟踪分析员工信息安全培训的效果

线上培训的形式，在员工每次参加培训之后，需要进行线上答题。信息安全管理部门在员工培训系统后台，可以跟踪员工的答题情况，对于员工普遍存在的问题需要进行进一步的培训分析，确定是否需要针对特定话题进行员工再培训；线下培训的形式，将同时结合员工答题和调查问卷的形式，了解线下培训的实际效果，确保全体员工能够理解并认识到信息安全防护的重要性和防护要点。

（4） 信息安全培训风险控制实例

这里以“跟踪分析员工信息安全培训的效果”的实施方案为例。首先，本文总结出部门和员工在这个执行方案当中的责任划分，具体如下表 4.4 所示：

表 4.4 信息安全培训职责细节

Tab. 4.4 Responsible details of information security training

执行人员和工具	执行项目和工具细节
信息安管部门培训负责人	负责主导 BY 公司全体员工的信息安全管理培训；根据公司运营实际情况，定期通过线上和线下的形式安排培训；制定培训效果评估标准，对未达成培训效果的员工制定再培训计划。
全体员工	有义务参加由信息安管部门主导的信息安全培训，按期参加线上和线下培训，参与信息安全知识线上和线下考试。如按照要求参加或者通过考试，则需要参加信息安全再次培训计划。
线上培训系统	是一个在线培训和考试系统，信息安管部门培训负责人可根据实际安排，定期上传线上培训内容及试题。
线下培训试题和问卷	由信息安管部门培训负责人拟定用来测试全体员工信息安全管理知识的试题和问卷。

由于 BY 公司一直以来缺少成型的信息安全培训方案，因此，需要尽快执行该方案，确保全体员工得到有效的信息安全培训，具体实施流程如下图 4.3 所示：

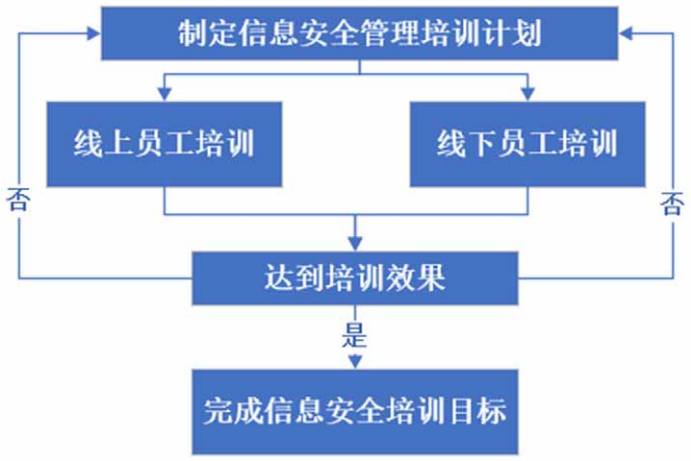

图 4.3　培训效果跟踪工作流程图

Fig. 4.3　Training effectiveness follow up working flow

4.2　BY 公司信息安全管理体系建设

4.2.1　总体目标

BY 公司信息系统平台应用于多个国内业务部门，涉及到的业务人员较多，系统信息复杂，并且存有相当数量的业务敏感信息。鉴于该系统的复杂性和特殊性，以及业务部门对系统稳定性和安全性的依赖，BY 公司管理层对信息系统安全体系的建设十分重视。

BY 公司信息安全体系建设不是一次性的工作，其主要针对的不只是控制 BY 公司现存的主要信息安全风险，而是通过体系化的建设，使 BY 公司系统平台的信息安全得到保障，使得业务部门能够稳定和安全的使用 BY 公司系统，同时还能够保证信息安全体系的可持续性和有效性。

因此，BY 公司进行信息安全体系建设的总体目标，将主要分为如下几点：

（1） 通过对 BY 公司信息系统资产进行全面风险管理，将相应资产的风险控制在可接受的范围之内。

（2） 在信息安全等级保护和 ISO/IEC 270001 信息安全管理标准的指导下，制定出行之有效的信息安全管理政策和管理计划，并对信息安全相关资产进行分级保护。

（3） 依据 P2DR2 安全模型，构建 BY 公司内部网络安全体系结构。从信息安全的策略、信息安全的保护措施、信息安全的检测方式、信息安全事件的响应方式和信息安全恢复这个几个方面，为 BY 公司企业网络构建动态安全防护模式，并将“ 身份验证 ”，

“访问控制”，“安全通信”，“安全分析”融入该模型当中，主动防御网络安全漏洞，有效响应网络安全事故，将 BY 公司企业网络安全风险降到最低的状态。

（4） 从组织，部门和员工几个方面进行反思和梳理，从本质上调查出影响 BY 公司信息安全管理的关键因素，确保 BY 公司的信息安全得到保障，同时能够保证体系运作持续有效。

（5） 从文化建设角度出发，营造出全公司的信息安全防护文化，同时将信息安全管理体系的具体内容进行文件化管理。

4.2.2 建设原则

BY 公司体系建设目标能否实现，与公司进行体系建设的原则有很大关系。作为 BY 公司体系建设的指导纲领，BY 公司体系建设将按照如下原则来执行：

（1） 制度合理性：虽然 BY 公司当前缺少行之有效的信息安全管理制度，然而仅仅为了重新建立制度，而忽略了制度的合理性，将违背 BY 公司进行信息安全体系建设的初衷。BY 公司新建立的信息安全管理制度是否合理，将对 BY 公司整体信息安全管理起到决定性作用。

（2） 权责分明：在 BY 公司运营管理的过程中，不同部门具有其不同的职能范围，而不同的员工也具有其不同的工作责任范围。只有部门和员工清楚的了解并能够履行其相应的权力和责任，相互配合，这样 BY 公司的信息安全管理才能得到保障。

（3） 验证有效性：需要针对 BY 公司信息安全管理体系建设的效果进行验证，确保其具有可检查性和有效性，同时对体系建设是否有改进的空间要进行评审。

4.2.3 建设内容

（1） 构建信息安全风险管理框架

正式由于缺少成型的信息安全风险管理概念和方法，BY 公司的信息安全风险一直无法得到有效控制。因此，在进行本次 BY 公司门户网站风险评估的基础上，总结出 BY 公司信息安全风险管理框架如下：

① 确认风险评估范围：确认要进行风险评估的范围，其中包括织架构特性，员工管理的合理和有效性，基础设施安全以及信息系统安全等。

② 识别和评估资产重要度：将 BY 公司信息安全相关资产进行分类，从“可用性”，“完整性”和“保密性”三个维度，对资产的重要度进行综合赋值。

③ 识别和评估资产威胁：确认威胁类型，根据不同威胁的特性，对 BY 公司信息安全资产进行赋值。

④ 识别和评估资产脆弱性：对 BY 公司信息安全资产进行脆弱性分类，根据不同的脆弱性特质，对其资产进行赋值。

⑤ 识别和评估已有控制措施：将已有风险控制措施的有效程度进行定义和分类，并对 BY 公司信息安全资产进行控制措施有效性赋值。

⑥ 风险值计算：依据风险计算模型，在 BY 公司资产风险评估赋值的基础上，计算出对应资产的风险值。

⑦ 风险标准对比：将资产的风险值和风险控制标准进行对比，根据不同的风险等级来确认风险控制的优先级。

⑧ 制定和执行风险控制方案：针对 BY 公司存在的主要信息安全风险问题，依据风险控制的优先级，制定风险控制方案，并按照既定计划来执行。

⑨ 残余风险管理：在执行风险控制计划后，确认是否存在残余风险和可能存在残余风险的接受程度，来做出相应风险控制或者风险保留的决策。

（2） 组织架构优化

一直以来，BY 公司缺少进行统一规划和指导 BY 公司信息安全管理的职能部门。BY 公司信息安全管理部门的建设，是 BY 公司信息安全管理措施得以高效执行的前提。针对国内业务部门信息系统安全管理维护的需求，BY 公司将设立国内专职信息安全管理部门，安排其主要工作内容如下：

① 规划 BY 公司新版信息安全管理制度，确保该制度的合理性和有效性。

② 积极与其他职能部门配合，将其他部门提供的信息安全相关信息进行综合分析，提出具有可行的信息安全管理方案。

③ 主导 BY 公司信息安全风险管理，定期评估和分析当前公司存在的信息安全风险，对是否执行，怎样执行信息安全风险控制措施做出决策，提供指导意见。

④ 构建信息安全防护文化，积极沟通和宣传信息安全法律法规，普及信息安全意识和遵守信息安全管理制度的重要性。

与此同时，还要明确各个职能部门在信息安全管理体系建设当中的职责和义务：

① 遵守 BY 公司新版信息安全管理制度，将信息安全管理制度融入到各项日常运维和项目工作当中。

② 与信息安全管理部门积极沟通，保持合作，及时将在日常工作活动实践当中发现的信息安全问题和潜在问题，汇报给信息安全部门，确保信息安全防护及时有效。

③ 当各部门经理与信息安全部门就信息安全管理出现意见分歧时，积极沟通，通过线上或线下会议的形式，就有意见分歧的问题展开讨论。必要情况下，需要得到 BY 公司总经理的支持，对信息安全管理问题做出最终决策。

（3） 信息安全管理制度建设

BY 公司的主要信息安全问题，主要在于已经存在的信息安全风险，和即将发生的信息安全风险两个方面。因此，新版信息安全管理制度的建设，也将主要从这两个方面出发：

① 信息分级管理制度：将 BY 公司内部信息根据其影响，划分为“内部信息”，“保密信息”和“绝密信息”。通过该分类，也可以看出信息受保护的等级。为了方便进行信息分级管理，将所有已经识别出的信息进行归类，通过信息创建、命名和信息说明，构建不同信息类别。

② 访问权限管理制度：构建 BY 公司员工用户身份识别唯一标识码，用于管理员工访问 BY 公司信息系统相关软件和硬件的权限。由系统管理员根据员工身份，对其访问权限进行分组，同时保证当员工离职后，取消其访问 BY 公司信息的权限。

③ 系统运维安全管理制度：由指定的一名或者多名系统运维管理人员，对 BY 公司的运维系统定期进行系统漏洞分析、网络交互分析、系统版本分析等，将分析结果总结成系统运维分析报告，统一由信息安全管理部门进行综合分析管理。

④ 数据安全管理制度：对应用程序接口的设计和开发，进行加密管理，确保数据在进入公共传输网络之前，进行数据加密；对内部网络数据传输过程中，存在的异常数据传输类别和数据访问量进行监控，制作分析报告。

在建设新版信息安全管理制度的基础上，为了确保信息安全管理制度能够灵活应对企业发展战略的变化，还要明确未来信息安全管理制度变更的相关工作流程：

① BY 公司总经理将持续参加 BY 集团信息安全管理战略小组例会，将集团最新的信息安全管理战略及时更新给信息安全管理部门，为本地信息安全管理制度调整做统一规划安排。

② 信息安全管理部门要结合 BY 集团的信息安全管理战略标准，本地企业运营环境法律法规和信息安全管理实践活动反馈，灵活调整信息安全管理制度条例，确保其具有实用性和有效性。

③ 信息安全管理部门和其他各职能部门经理设立月度例会，保持在公司信息安全管理制度策略和运营实际活动上的及时同步。

（4） 人员管理

BY 公司的人员管理，是 BY 公司进行信息安全体系建设当中最重要的一环。员工的工作态度和安全防护意识,直接决定了 BY 公司信息安全管理是否能够得到有效执行。因此，在 BY 公司信息安全管理总体方针的指导下，主要将从以下几个方面重点建设和管理员工信息安全相关活动：

① 明确职责划分。明确在 BY 公司的信息安全管理活动当中，不同职能部门的职责，不同员工的职责。同时，明确信息安全防护事项，信息安全事件处理流程，保证员工在处理信息安全事件时有据可循，按章办事。

② 定期培训。除了新员工培训的内容里面要安排信息安全管理相关的培训内容，针对员工的日常工作活动，定期通过内外部培训的形式，提高员工的信息安全防护意识，确保其把信息安全的理念代入到工作活动当中；针对举办的培训内容，开展相应的问卷测试，以考察员工对信息安全相关培训的理解层度；针对不同权限的系统管理相关人员，定期进行对应层次的信息安全培训。

③ 定期例会工作总结和分享。信息安管部门主导信息安全管理规章制度的更新内容，通过月会的形式，将最新的管理制度和注意事项普及给全体员工，以提高其防护意识；各部门设立短时长周会，让员工重点分享在工作当中可能遇到的信息安全相关问题，由各部门领导及时总结并汇报给信息安管部门做进一步分析跟进。

5 BY 公司信息安全管理保障措施

为了保证 BY 公司信息安全问题得以解决，信息系统安全风险得到控制，企业能够安全稳定的使用 BY 公司信息系统资源，除了需要落实前文提出的风险管理控制方案和信息安全体系建设方案，还需要确保这些方案措施能够在有效的企业条件和环境下顺利实施。

因此，本文还将从 BY 公司管理职能的计划、组织、指挥、协调和控制这五个维度进行论述[26]，为 BY 公司信息安全管理提供保障措施。

5.1 明确公司信息安全管理计划

（1） 保证本地和 BY 集团总部信息安全管理计划的一致性

BY 公司本地要制定的信息安全管理计划，将隶属于 BY 集团总部全球信息安全管理计划的一部分。当前总部集团信息安全管理的总体方向，是以风险管理为基础、以数据为驱动、以员工为核心来创建信息安全管理计划。因此，BY 公司也将以核心方向此为立足点，构建本地信息安全管理计划。以风险为基础：根据对信息安全风险的评估结果，开发安全工具与服务；以数据为驱动：通过设计，在每个流程中嵌入最新的安全措施；以员工为核心：寻找创新的解决方案，保障现代工作方式的灵活性。

（2） 保证本地信息安全管理计划与本地业务可持续性发展战略协调统一

2019 年 3 月，BY 集团提出了“ 共享健康，消除饥饿 ”的愿景。为了实现这个远景，业务部门与 BY 公司在信息技术的多个维度开展深化合作，共同打造数字化变革的可持续性发展战略。当前业务部门的工作重点，主要着眼于保障业务流程相关系统的可持续性运行。在新旧系统更新迭代的同时，业务部门不只关心业务流程是否会受到系统变更的影响，还关心在新系统设计、新旧系统数据迁移过程中的信息安全问题。因此，BY 集团在构建按本地信息安全管理计划的同时，还要考虑到业务部门可持续性使用 BY 公司信息技术服务的安全问题。

（3） 制定组织内部运维管理和项目管理安全策略

制定组织内部安全管理策略。权责分离策略：在对员工进行职责定义时，将有可能产生相互冲突的职责和责任进行分割，以降低未授权访问、无意识修改等带来损失的可能性，如管理岗位与操作岗位权责分离，系统开发岗位与系统运维岗位权责分离等。利益相关方联系管理策略：信息安全管理部门人员，应保持与外部执法部门、政府部门等利益相关方就信息安全事务保持联系。当出现重大安全事件时，应及时与相关方联络并协助其介入处理企业信息安全问题。同时，信息安全管理部门还可以针对信息安全管理

相关的最佳实践和最新知识、信息安全管理应用和维护所需的技术支持，向外部安全专家和特定外部组织寻求信息安全方面的建议和意见。

制定项目管理中的信息安全策略。在项目管理过程的各个阶段，应将信息安全管理制度和方法有机结合到项目管理方法当中，确保在项目管理的过程中，实时将信息安全风险管理作为项目管理的一部分。如将信息安全目标同时纳入项目管理目标；在项目准备阶段，将信息安全风险评估结果纳入项目风险管理列表等。

5.2 构建与公司信息安全管理相适应的组织架构

如前文所述，BY 公司将设立国内专职信息安全管理部门。在设置该部门后，BY 公司新的组织结构图将如下图 5.1 所示：

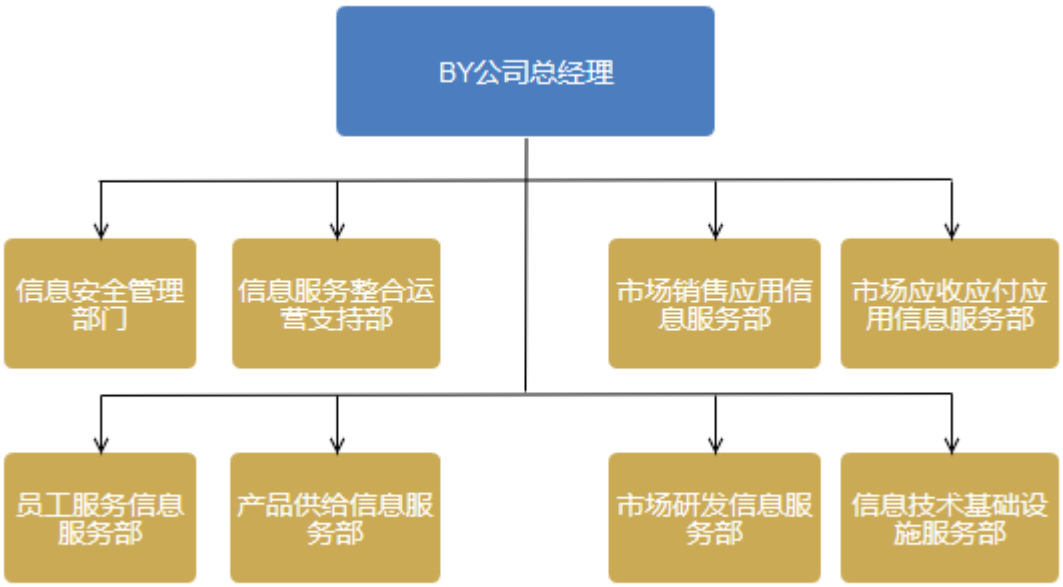

图 5.1 BY 公司新组织架构图

Fig. 5.1 New organization chart of BY company

在新的组织架构中，BY 公司将给予新建立的信息安全管理部门充分授权。该部门主管人员将直接汇报给 BY 公司总经理，并参与 BY 公司高层领导会议。在会议当中，信息安管部门主管需要将新版信息安全管理制度的制定和执行计划呈现给全体高层管理人员，并在各部门领导综合讨论后，由 BY 公司总经理对新版信息安全管理制度做出最终决策，BY 公司总经理将倡议各部门领导全力配合和支持信息安管部门的工作。

同时，BY 公司还将明确信息安全管理部门组织结构和职责范围。该部门将主要划分为三个职责分支结构，具体组织汇报关系如下图 5.2 所示：

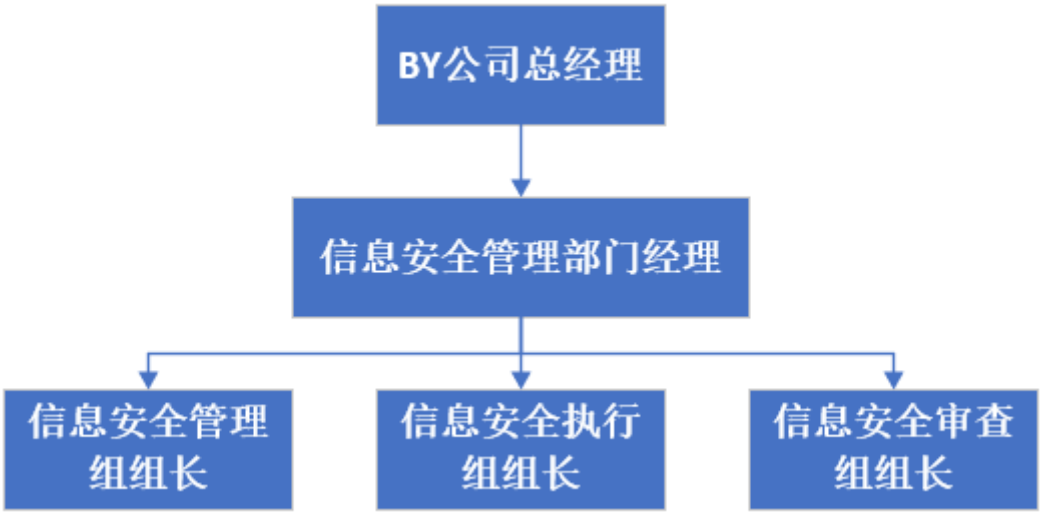

图 5.2　BY 公司信息安全管理部门组织关系图

Fig. 5.2　Organization chart of BY company information security department

其中信息安全管理组，将主要负责信息安全管理制度的规划和制定，风险评估方法和接受标准的制定以及信息安全工作落实情况监督等；信息安全执行组，将主要负责落实信息资产识别，风险评估工作。负责落实、协调和实施信息安全管理工作。与其他部门同事保持良好沟通，确保信息安全管理目标统一。同时，定期将信息安全管理实践效果和相关问题汇报给信息安全部门主管；信息安全审计组，将定期和不定期实施公司内部信息安全审核和检查，向信息安全部门主管汇报审核中发现的问题，并跟踪内审过程中发现不合规问题的整改进度。

5.3　充分发挥各部门领导的管理职能

（1）　在信息安全管理计划和信息安全管理制度的指导下，各部门领导明确了解信息安全管理工作目标，明确自身在管理流程中的职责和义务，并将员工在信息安全管理工作中的职责和义务清晰的传达给员工。

（2）　作为部门领导，在信息安全管理活动中要以身作则，积极遵守信息安全管理相关制度，在部门日常工作管理当中起到表率作用。

（3） 各部门领导与员工就公司信息安全管理相关信息，要及时充分沟通。要了解员工在工作中常见的信息安全管理相关问题，及时反馈，并定期检查员工信息安全管理工作执行情况。

（4） 各部门领导要认可员工的首创精神。对积极参与信息安全管理活动，并给予具有建设性建议的员工，要提出表扬，并将相关意见积极反馈给信息安全管理部门。

5.4 倡导各部门信息安全管理工作协调统一

BY 公司信息安全管理工作是否能够有效开展，很大程度上取决于信息安全管理部门和其他职能部门之间的合作。为了保证信息安全管理计划和制度的顺利实施，首先要积极促进组织内部沟通，加强组织内部合作。BY 公司的信息安全管理部门，将统一协调各部门间在信息安全管理流程方面的合作，并为各部门在信息系统设计、构建、开发、部署、测试、应用和运维等层面，提供信息安全管理综合指导，立足成为 BY 公司信息安全管理的“大本营”；其他各职能部门经理，通过各项线上线下例会、交流活动、经验分享会等形式，增进沟通，加强合作，保证管理公开、透明、流程统一、明确人员分工，共同达到公司内部管理职能协调统一的目的，进而能够更好的为业务的可持续发展提供动力，保障业务使用 BY 公司信息系统的安全；BY 公司的各位员工，在组织信息安全管理制度和方针的指导下，认真落实并按照规章制度工作。对组织做到诚实守信，对部门领导要体现出自己的才能。在遵守企业信息安全管理制度的同时，也要积极根据 BY 公司实际运营状况，提供信息安全管理实践的反馈和建议。

其次，为了将信息安全管理的理念渗透到日常工作当中，还要构建企业信息安全风险防范文化。以“信息安管部门指导为主，各部门领导配合为辅”的内部合作方针，在公司内部宣传和强化信息安全风险防范的重要性。由信息安管部门发起，公司创办《BY 公司信息安全月报》，宣传近期发生的信息安全事件，员工在信息安全管理过程中的重要贡献，以及对近期信息安全管理新政颁布的展望；同时，公司通过微信公众号的形式，每两周定期发布有关提高员工信息安全防范意识的文章，提高了员工的信息安全风险防范意识和风险防控意愿。

再次，为了保证公司内部信息安全管理相关信息的透明性，还将设立多种沟通会议，以达到相关工作协调统一的目的。

（1） 信息安全管理工作周会：该周会时长为 20 分钟，参与人员为信息安全管理部门经理和其他职能部门经理，旨在针对近期存在的紧急信息安全管理问题交换意见，简要探讨风险控制方向和措施。

（2） 信息安全管理工作月会：该月会时长为 40 分钟，除 BY 公司总经理外，其他全员都要参加。该会议的主要议程是：回顾近期存在的信息安全管理问题；如有总部传达来的信息安全管理策略变更，要在该会议当中提及；如有信息安全管理问题事件，将依据该事件进行管理分析，找出问题所在并指出问题解决方向。

（3） 信息安全管理工作年会：该年会时长为 60 分钟，BY 公司全员参加。该会议的主要议程是：回顾信息安全管理团队全年工作重点及完成度；回顾公司内部信息安全管理问题类型汇总并指出改进方向；对为信息安全管理工作积极提出建设性意见，并且意见被信息安管部门采纳的员工，给予奖状表彰并授予奖金；展望下一年度 BY 公司信息安全管理工作的重点发展方向。

（4） 信息安全管理紧急会议：该会议时间不定，参会人员取决于信息安全管理事件的严重程度。对于信息安全管理部门召开的紧急会议，各部门领导应积极予以配合。

5.5 信息安全管理工作成效管控

由信息安全管理部门审计组主导公司内部信息安全管理审计工作。该部门每年将依照公司信息安全管理制度框架，审查 BY 公司在信息安全管理层面存在的隐患和漏洞，根据 BY 公司业务实际情况，针对这些问题提出改善意见和方案。

同时，该部门将联合外部专门的审查机构，对 BY 公司定期进行外部审查，评价公司当前的信息安全管理水平。如有重大问题发现，将需要联合问题相关管理团队经理，基于外部审计专家提供的专业性意见和建议，共同协商并制定整改措施。

结　论

为了更好的面对日益激烈的国内和国际市场竞争，BY 集团和 BY 公司变革步伐的频率只会不断加快，而产业信息化的进程也将不断加速，这将给企业的运营发展和信息安全管理不断带来新的挑战。只有将行之有效的信息安全管理措施和指导思想引入到 BY 公司的企业运营管理当中，才能保证 BY 公司持续稳定的运营和发展。

本文首先基于信息安全管理体系、信息安全等级保护等管理模型，使用案例分析、调研访谈及定性定量风险分析等方法，分析出 BY 公司信息系统的几个主要信息安全风险问题，即“信息安全管理制度不健全”，“员工职责范围不明确”以及“缺少成型的员工信息安全培训”，同时总结出这些信息安全风险问题的成因。其次，针对 BY 公司这些主要信息安全风险问题，阐述了具体的风险控制措施，以及部门建设、制度建设、人员管理等方面的信息安全体系建设方案。最后，针对阐述的风险控制方案和体系建设方案，提出 BY 公司信息安全管理的保障措施。

本人在论文研究实践的过程中得到了一点启示，即采取匿名调查，私人访谈的形式，深入了解 BY 公司现存信息安全问题的实际情况。整理到的数据和信息较多，因此，总结出的重点问题具有鲜明的代表性。

然而本人在信息安全领域相关的经验和水平有限，有待在后续的研究过程中进一步完善，同时也将通过对工作经验的积累和理论知识的巩固，对实施过程中的不足之处进行不断的完善和改进。

参 考 文 献

[1] 张焕国.信息安全工程师教程[M]. 北京:清华大学出版社,2016.
[2] 杨启飞. 大数据时代国内信息安全研究：现状、趋势与反思[J]. 情报科学.
[3] 宋晓龙, 李鹤田.国内外信息安全评测认证的发展现状和趋势[J]. 信息安全与通信保密, 2001(1)：17-21.
[4] 陈光.信息系统信息安全风险管理方法研究[D]. 长沙：国防科学技术大学,2006.
[5] Saleh M S, Alfantookh A. A new comprehensive framework for enterprise information security risk management[J]. Applied computing and informatics, 2011, 9(2): 107-118.
[6] Fenz S, Ekelhart A. Verification, validation, and evaluation in information security risk management[J]. IEEE Security & Privacy, 2010, 9(2): 58-65.
[7] Broderick, J. Stuart. "Information security risk management—when should it be managed?." *Information Security Technical Report* 6.3 (2001): 12-18.
[8] 任伟. 钢铁企业信息安全风险系统管理研究[J]. 山西冶金, 2008 (4): 21-23.
[9] 毛纪辉. 烟草行业信息安全风险及防控[J]. 信息与电脑, 2017 (7): 201-202.
[10] 李超.信息系统安全等级保护实务[M]. 北京：科学出版社, 2013
[11] 万通, 曹木恒.基于 ISO27001 的 IDC 信息安全管理体系[J]. 信息安全与通信保密, 2009(1):41-46.
[12] 唐拥政, 王春风.基于 PPDR 的动态无线网络安全模型的改进研究[J]. 盐城工学院学报(自然科学版), 2013(3): 105-108.
[13] 吴军, 李桃红, and 邵定宏. "P2DR2 闭环动态安全模型的企业网应用研究." [J]. 电子商务 6 (2009).
[14] 吴亚非, 李新友, 禄凯.信息安全风险评估[M]. 北京：清华大学出版社.2007.
[15] 李硕.5G 时代的通信安全问题分析[J]. 通讯世界, 2019(9)：215-216.
[16] 向宏, 傅鹏, 詹榜华.信息安全测评与风险评估[M]. 北京：电子工业出版社.2009.
[17] 赵庆聪. 基于业务战略的信息资产识别方法[J]. 北京信息科技大学学报, 2014(2):72-73.
[18] 宫亚峰, 赵波, 徐金伟.再论信息安全资产的识别与评估[J]. 国家信息技术安全研究中心, 2010(2):5-7.
[19] 余立新. 关于资产风险度赋值中的一些概念问题的探讨[J]. 信息安全与通信保密,2007(01):46-47.
[20] Rainer.Jr R K.et. Risk Analysis for Information Technology[J]. Journal of Management Information Systems.1991.8(1).129-147.
[21] 程建华.信息安全风险管理、评估与控制研究[D]. 长春：吉林大学,2008.

[22] 沈浩,杜彦辉,孙言.信息安全风险评估标准研究[J]. 网络安全技术与应用,2009(05):91-93.
[23] Bilge Karabacak, Ibrahim Sogukpinar.ISRAM:infbrmation security risk analysis method[J]. Computers&Security Journal, 2005,24: 147-159.
[24] Bernd Blobel, Francis Rogar-France. A systematic approach for analysis and design of secure health information systems[J]. Medical Informatics, 2001,62: 51-78.
[25] 张乐鑫.B 公司基于 ISO27000 信息安全管理体系的风险评估和控制[D]. 上海：华东理工大学,2015.
[26] 易昱烨. 法约尔理论在企业管理中的应用[J]. 科教导刊, 2016 (2016 年 12):157-159.

附录 A　调查问卷

第一部分 调查背景介绍

近年来，公司内部频繁发生信息安全事件，我们对口的业务部门深受影响，效益损失严重。为了更好的了解当前我们公司信息安全管理现状，针对性的解决近年来频繁出现的信息安全问题，希望通过此问卷调查，来进一步了解公司内部当前主要在哪些层面存在信息安全管理问题。

本问卷采取匿名调查的形式，在问卷调查中会需要大家填写所在的部门信息、岗位信息以及工作年限等。这些个人信息将主要用来做后续问题分析参考使用，不会向其他不相关部门及人员泄露。希望同事们能通过该问卷反馈出最真实的声音，以便我们可以通过该问卷了解到当前公司信息安全管理问题最真实的情况。

问卷填写要求：

1. 问卷内容需全部填写，如超过 80%题目未作答，本问卷视为无效；
2. 封闭式问题均为单选题；
3. 开放式问题请您在问题下方的横线上填写。

第二部分 调查主体（请在您认为正确的选项上打勾）

您所在的部门为：□信息服务整合运营支持部　□市场销售应用信息服务部
□ 市场应收应付应用信息服务部 □ 员工服务信息服务部
□市场研发信息服务部　□ 产品供给信息服务部
□ 信息技术基础设施服务部

请简要描述您所在的岗位信息:

_____

请提供您的工作年限信息：

○1 年以内　○1 - 2 年　○2 - 3 年
○3 - 5 年　○5 - 8 年　○8 年以上

第三部分 调查问题

1. BY 公司的信息安全管理理念先进，制度明确，规范完整，具有质量保障。

○非常同意

○同意

○不一定

○不同意(如选择该选项，请简要说明原因) _____

○非常不同意(如选择该选项，请简要说明原因) _____

2. BY 公司技术人员对信息安全检测和报警有明确的安全分析报告及响应措施。

□非常同意

□同意

□不一定

□不同意(如选择该选项，请简要说明原因) _____

□非常不同意(如选择该选项，请简要说明原因) _____

3. BY 公司有明确的信息安全管理部门及相关人员。

○非常同意

○同意

○不一定

○不同意(如选择该选项，请简要说明原因) _____

○非常不同意(如选择该选项，请简要说明原因) _____

4. BY 公司经常组织具有时效性的信息安全管理相关培训。

○非常同意

○同意

○不一定

○不同意(如选择该选项，请简要说明原因) _____

○非常不同意(如选择该选项，请简要说明原因) _____

5. BY 公司信息系统补丁实施更新。

○非常同意

○同意

○不一定

○不同意(如选择该选项，请简要说明原因) _____

○非常不同意(如选择该选项，请简要说明原因) _____

6. BY 公司具有完整明确的网络分析报告。

○非常同意

○同意

○不一定

○不同意(如选择该选项，请简要说明原因) _____

○非常不同意(如选择该选项，请简要说明原因) _____

7. 我对 BY 公司其他部门的工作职责内容十分了解，处理信息安全事件时得心应手。

○非常同意

○同意

○不一定

○不同意(如选择该选项，请简要说明原因) _____

○非常不同意(如选择该选项，请简要说明原因) _____

8. 我对 BY 公司的物理设备安全十分放心。

○非常同意

○同意

○不一定

○不同意(如选择该选项，请简要说明原因) _____

○非常不同意(如选择该选项，请简要说明原因) _____

9. BY 公司几乎没有发生过网络安全事件。

○非常同意

○同意

○不一定

○不同意(如选择该选项，请简要说明原因) _____

○非常不同意(如选择该选项，请简要说明原因) _____

10. BY 公司的信息安全核心技术手段十分健全。

○非常同意

○同意

○不一定

○不同意(如选择该选项，请简要说明原因) _____

○非常不同意(如选择该选项，请简要说明原因) _____

11. 您对 BY 公司信息安全的总体评价是怎样的？

_____

12. 您认为 BY 公司在信息安全管理方面存在哪些不足？

_____

13. 您对 BY 公司信息安全管理有哪些意见和建议？

_____

致　　谢

本文从开题选题，到中期答辩，再到全文的定稿，导师李瀛副教授一直能够细心指导，为全文的研究结构和行文细节提供了宝贵的意见和建议。李瀛副教授治学严谨，学识渊博，不仅在信息安全领域颇有建树，而且还能够潜心为导生的研究论文无私奉献，我希望借此对导师李瀛副教授表达我诚挚的谢意！

与此同时，我还要感谢大连理工大学全体给予我们课程教学的任课老师。你们幽默风趣的课程设计，严谨的课程结构，理论结合实践的教学形式，让我体会到了“教学实为本，实践乃为先”的学习理念。这样的学习理念，也正是本文成文的精神基础和研究纲领；感谢和我一起并肩学习的同学和朋友们，你们精益求精的学习态度和严谨的逻辑分析思路，是我 MBA 学习生涯中一道亮丽的风景线，也是我潜心进行论文研究的学习榜样。

最后，我要感谢进行论文审阅的各位老师，你们中肯的意见指导着一届又一届的 MBA 学子在论文研究的道路上前行，衷心感谢你们能在百忙之中为我的论文研究提供宝贵的意见！

大连理工大学学位论文版权使用授权书

本人完全了解学校有关学位论文知识产权的规定，在校攻读学位期间论文工作的知识产权属于大连理工大学，允许论文被查阅和借阅。学校有权保留论文并向国家有关部门或机构送交论文的复印件和电子版，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，可以采用影印、缩印、或扫描等复制手段保存和汇编本学位论文。

学位论文题目：BY 公司信息安全风险管理研究

作 者 签 名 ： 日期： 2021 年 6 月 6 日

导 师 签 名 ： 日期： 2021 年 6 月 6 日

大连理工大学学位论文独创性声明

作者郑重声明：所呈交的学位论文，是本人在导师的指导下进行研究工作所取得的成果。尽我所知，除文中已经注明引用内容和致谢的地方外，本论文不包含其他个人或集体已经发表的研究成果，也不包含其他已申请学位或其他用途使用过的成果。与我一同工作的同志对本研究所做的贡献均已在论文中做了明确的说明并表示了谢意。

若有不实之处，本人愿意承担相关法律责任。

学位论文题目：BY公司信息安全风险管理研究

作 者 签 名 ：  日期：2021 年 6 月 6 日