中小企业信息安全管理体系最佳实践

刘小茵　主编

中国标准出版社

中小企业信息安全管理体系

最佳实践

主　编　刘小茵

编　委　（按汉语拼音字母顺序）

孔祥林　李尧　林强　柳荣梦　田刚　肖锟

中国标准出版社

北　京

图书在版编目(CIP)数据

中小企业信息安全管理体系最佳实践/刘小茵主编.
—北京:中国标准出版社,2010
ISBN 978-7-5066-5904-8

Ⅰ.①中… Ⅱ.①刘… Ⅲ.①中小企业-信息系统-安全管理-最佳化 Ⅳ.①F276.3

中国版本图书馆 CIP 数据核字(2010)第 136032 号

中国标准出版社出版发行
北京复兴门外三里河北街 16 号
邮政编码:100045

网址 www.spc.net.cn
电话:68523946 68517548
中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销

*

开本 787×1092 1/16 印张 11 字数 253 千字
2010 年 8 月第一版 2010 年 8 月第一次印刷

*

定价 **30.00** 元

序言

随着信息技术的高速发展，特别是Internet的问世及网上交易的启用，许多信息安全的问题也纷纷出现：系统瘫痪、黑客入侵、病毒感染、网络钓鱼、网页改写、客户资料的流失及公司内部资料的泄露等等。这些已给组织的经营管理、业务发展甚至生存带来严重的影响。

在我们周围，信息安全威胁无处不在。有人认为，信息安全“不就是安装杀毒软件，在电脑上设设密码吗？”如果我们这样想，就和全世界95%的人一样，都错估、低估了信息对公司的致命影响。下面看看几个日常工作中我们可能都会碰到但往往被忽视的例子：

打印纸双面打印——好习惯换取的大损失。节约用纸是很多公司的好习惯，公司往往提倡纸张要充分利用，要尽量使用“废纸”的背面进行打印。其实，将拥有这种习惯公司的“废纸”收集在一起，我们会发现打印、复印造成的废纸有时候包含着公司的机密。

白板——公司研发信息泄露。公司在研发过程中，研发小组往往要经过多轮的研究、分析和评审。研发小组讨论的时候会在白板上列出一些产品的核心参数、使用的模型或方法等。在离开会议室的时候往往没有将白板上的信息擦掉，“有心人”非常轻易地就窥探到产品的机密。

电脑易手——新员工真正的入职导师。很多员工可能都有过这样的经历：如果自己新到一家公司工作，在自己前任的电脑里漫游是了解新公司最好的渠道。在一种近似“窥探”的状态下，公司里曾经发生过的事情“尽收眼底”，例如公司以往的客户记录、奖惩制度等。如果有幸拿到原来是人力资源部

员工使用的电脑，或许能看到全公司的薪资表。

光盘刻录——资料在备份过程中流失。如果想要拿走公司的资料，最好的办法是申请光盘备份，把文件做成特定的格式，交给网络管理员备份，然后声称不能正常打开，要求重新备份。大多情况下，留在光驱里的“废盘”就可以在下班后大大方方带出公司。

邮箱——信息窃取的中转站。利用电子邮件转移窃取的公司资料占所有信息窃取的八成以上。很多企业不装软驱、光驱、USB接口，却忽视如何避免员工通过电子邮件窃取信息。

大容量存储——大量窃取资料常用手段。压缩软件的作用毕竟是有限的，如果把自己的大容量存储设备如U盘、移动硬盘，甚至智能手机等拿到单位来，连上局域网，只要半小时，就是有1Gbyte大小的文件也可以轻松带走。

以上只是众多信息安全问题中的几个常见案例。人们利用这些手段能轻易获得公司的秘密，如果给别有用心的人利用就可能给公司带来严重的损失。从这些例子看，信息的泄漏很多时候并不需要高超的技术手段，往往是由于公司没有规定相关的信息安全规章制度或人们还没有较高的信息安全意识。

越来越多的公司意识到信息安全对企业持续健康发展的重要性，希望在组织中依据ISO/IEC 27001:2005(GB/T 22080—2008)标准建立全面系统的信息安全管理体系，并通过认证获得证书。众所周知，建立一个体系前期需要花费公司较多的资源，对于中小企业，在资源比较紧张的情况下，如何有效地建立和实施信息安全管理体系(ISMS)是普遍希望解决的问题。

本书正是基于这样的背景情况，通过一个虚拟组织——创新科技发展有限公司——如何在组织内建立和实施信息安全管理体系的过程，为中小企业建立和实施信息安全管理体系提供一个有益的思路及力所能及的帮助。

需要说明的是，本书给出的范例只是一个案例，是针对“创新科技发展有限公司”的情况而编写的。对于其他企业需要根据企业的业务特点、企业规模、资源、员工素质、所处的环境等来建立适合各自的信息安全管理体系。

编 者

2010年4月

目录

第1章 实施企业背景

1.1 公司简介

创新科技发展有限公司(以下简称“创新”)是一家创新企业,公司成立2年,生产电子阅读器,公司员工100人左右,拥有完整的开发、生产和销售体系,具有独立开发能力,拥有自主知识产权,获得了多项专利和软件著作权登记。

1.2 组织结构及各部门职责

1.2.1 组织结构

创新公司的组织结构如图1-1所示。

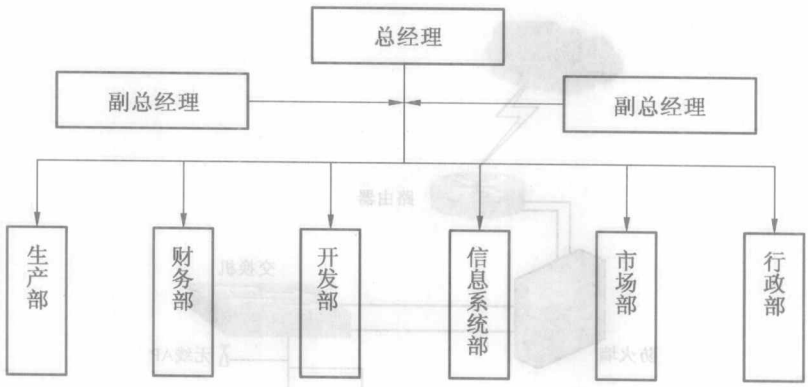

图1-1 组织结构图

1.2.2 各部门职责

1.2.2.1 生产部

人数30,主要负责将开发部定型的产品转产,并根据市场部对市场需求的分析来确定生产计划,同时确保产品的质量达标和及时交货。具体负责电子阅读器的(PDA)生产。

1.2.2.2 财务部

人数4,负责公司的预决算并根据情况调整计划,编写公司财务分析报告,执行国家的财务会计政策、税收政策和相关法规,对公司内部的运营资金和利润分配进行管理。

1.2.2.3 开发部

人数20,按照公司的研发流程完成新产品的设计和开发工作,对返修较多的产品进行跟踪分析和问题处理。同时跟踪业界最新技术和方法,积极与外部研发机构联系合作事宜。

1.2.2.4 信息系统部

人数2，主要负责公司内部信息系统的建设和维护，保证公司业务的正常运作。挂靠在开发部下由开发部经理负责管理。

1.2.2.5 市场部

人数46，包括了售前和售后服务人员，以及市场及销售人员。主要职责是建立完善的市场信息收集和分析团队，对消费者的心理和行为进行调查并作出市场预测，收集竞争对手的信息，实施通路计划和促销活动。

1.2.2.6 行政部

人数5，负责合同的保管，公司员工的教育培训，公司的工资、资产、档案管理，负责公司网页的信息收集、整理、更新及刊物的编辑、印刷，以及印章管理等工作。

1.3 主要设备及拓扑结构

1.3.1 公司网络拓扑结构

见图1-2。

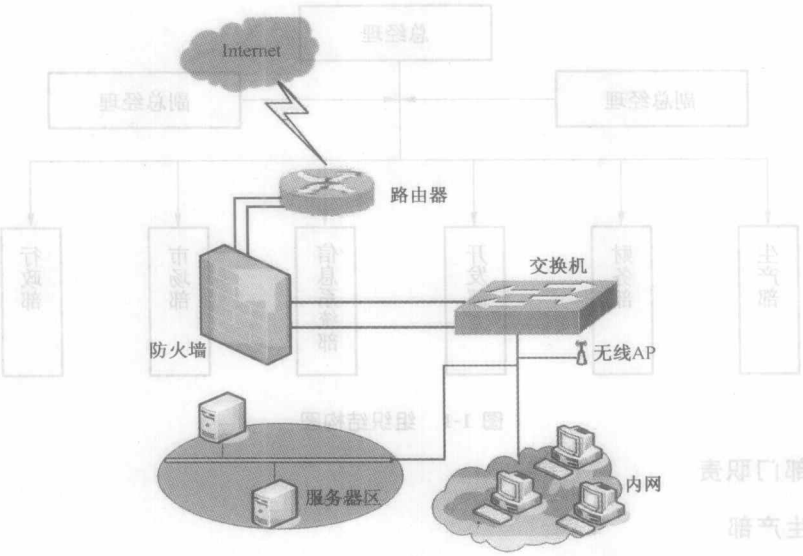

图1-2 创新公司网络拓扑结构图

1.3.2 主要设备

(1) 服务器2台——一台处理财务信息，另一台负责其他事项。

(2) PC终端49台——总经理1台、副总经理2台、生产部5台、财务部4台、开发部21台、信息系统部1台、市场部10台、行政部5台。

(3) 应用系统——OA办公系统，邮件系统，金蝶财务管理系统，ERP管理平台。

(4) 无线AP 1台。

(5) 防火墙 1 台。
(6) 交换机 1 台。
(7) 路由器 1 台。
(8) 笔记本电脑 98 台。
(9) 综合打印/传真机 1 台。

1.4 公司物理环境

见图 1-3。

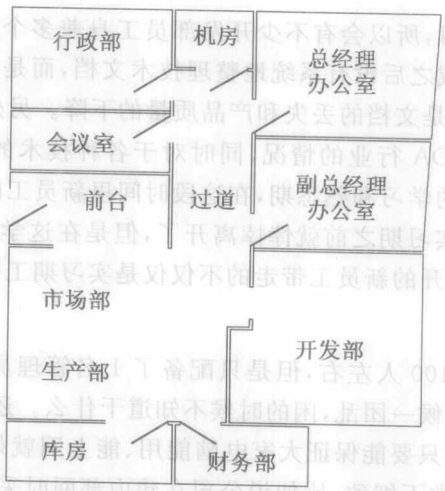

图 1-3 办公场所平面图

1.5 安全要求

1.5.1 信息安全现状

随着电子阅读器生产企业越来越多，电子阅读器的利润逐年下降，不少企业出现了“低端产品赚吆喝，高端产品赚收入”的局面。创新公司的优势就在于自己的研发能力和对高端市场透彻的分析。在最初的 2 年，公司凭借这两方面的优势抢占了不小的市场份额，但是随着人才频繁的流动和公司之间的信息窃取越来越频繁，公司的新技术在很短时间内就被竞争对手获得。此外，公司内部的运作管理也出现了一些问题，比如技术文档丢失后第二天发现其在别人的桌面上，电脑病毒导致的大面积网络瘫痪，公司内部出现物品丢失的情况却不知是谁人所为等。同时，公司还发现员工对于报废的终端设备随意丢弃或者干脆拿回家使用的情况，而网络管理员由于权限有限也无法采取有效的措施来制止。针对以上情况，公司高层管理人员决定对公司展开一次信息安全方面的情况调查，发现各个部门都有不少的问题存在，具体如下。

1. 生产部

随着市场需求的逐步加大，生产部发现供应商的供货时间越来越久，而且还出现某些批次的器件存在被退货的问题，工厂的工人常私自将损坏或不可用的器件丢弃而没有上报。

另外，生产部有一台公用的电话可以拨打全国长途，工人可以随意使用，包括下班时间。

2. 财务部

财务部的主要业务都是在内网展开，只有经理的电脑是同时连接内网和外网的，但是由于经理对电脑不熟悉，所以不少业务是由他的助理在他的电脑上完成的。财务系统使用的是金蝶专业版系统，数据库是单独使用一台服务器，由网络管理员负责维护，对财务系统的维护和备份是外包商承担的，每半年进行一次系统升级维护和数据备份。部门共4人，有2名出纳均可独立操作对外转账业务。

3. 开发部

由于时常会有紧急项目，所以会有不少开发部员工身兼多个项目的任务。项目多而急的状况导致了不少项目完成之后没有系统地整理技术文档，而是直接将开发文档交给了生产部门，随之而来的问题就是文档的丢失和产品质量的下降。另外，开发部由于对本部门的员工要求较高，需要了解PDA行业的情况，同时对于各种技术的使用有特殊的要求，所以新员工上岗之后有6个月的学习和熟悉期，在这段时间里新员工的待遇比较低，导致了不少员工在还没通过6个月的实习期之前就悻悻离开了，但是在这学习的几个月里也接触了不少的公司秘密文件，所以离开的新员工带走的不仅仅是实习期工资，还有公司的心血。

4. 信息系统部

虽然公司全职员工有100人左右，但是只配备了1名管理员，也就是自己管自己的部门，常出现的问题是忙的时候一团乱，闲的时候不知道干什么。还有就是公司领导对于这个部门并不是十分重视，觉得只要能保证大家电脑能用、能上网就好了，其他的投入都是多余的。一个人自然管理得非常不细致，比如说公司在建内部网时采取了几个措施：与Internet的连接有防火墙，但防火墙没有进行很好的配置；服务器上安装了防病毒软件，但防病毒资料库没有及时更新，用户端没有严格地安装防病毒软件；服务器操作系统和用户PC操作系统没有及时更新软件补丁等问题。

5. 市场部

虽然市场部有近50人，但是由于大部分人员长时间在外，所以他们只有10张办公桌，有时候会发生回办公室没位置坐的情况，而且由于没有固定的座位，时不时会将客户的资料遗忘在座位上。另外就是市场部每人都配备了笔记本电脑，但是对于这些电脑的情况网络管理员并不是十分清楚，因为公司的政策并没有清楚说明到底是公司负责购买还是可以使用个人自己的，所有权到底是公司的还是个人的，所以网管也没办法统一登记和管理，那么问题就是如果这些笔记本丢失了怎么办，里面又有多少数据？

6. 行政部

人力资源只有1个人在负责，所以划归行政部了。行政部由于不太涉及公司的核心技术秘密，所以对员工的安全意识培训不到位，不少人都把打印错误的技术文档直接就丢进废纸篓；行政部不少员工上班时间使用聊天工具，并且随意点开朋友发来的网页链接，导致不少机器都有木马或病毒；部分员工的显示屏下贴着电脑的开机密码，并且密码只有3～5位。

1.5.2 信息安全需求

首先，为了改善公司核心技术被窃取和流失的状况，以及给客户充分的信心，公司领导

决定要治理信息安全，通过对核心技术的保护来找回正在失去的高端市场；其次，也希望通过改善公司的工作氛围和管理体制来留住人才；最后是公司准备 2 年之内在美国 NASDAQ 金融市场上市。

以上这些因素让领导们充分地意识到了信息安全的重要性，但是由于手头事务繁忙，一直无暇考虑何时开始正式地建立信息安全管理体系(ISMS)，以下接二连三发生的事件让总经理下定决心要真真正正地实施 ISMS 了。

事情开始于某工作日的早晨，负责人力资源的副总刚到办公室就看见开发部元老级的陈工拿着一份不知从哪里得来的公司员工上年度待遇清单，上面清晰地列出了总经理级别以外的所有员工去年收入情况。面对这份表格上准确的数字以及陈工的收入还不及新来的欧阳博士 2/3 的实际情况，人力副总真是有口难辩。这边在使尽各种办法劝说、开出许多优惠条件的情况下才好不容易把陈工留在了公司，那边又见市场部的同事怒气冲冲地从投标现场回来，头一句话就是“为什么竞争对手拿着跟我们几乎一样的标书在我之前将我们的思想展示给客户了?”这还没算完，最近不少员工反应公司的电脑非常不稳定，不是文件丢失就是开机没多久就死机了；市场部的同事都不敢把笔记本拿回公司用了，说是接上公司的网络没多久就中毒。针对这些情况，公司算了一笔账，原来这些看似并不大的问题每年导致公司损失上百万甚至几百万。这下老总真的是坐不住了，决心尽早在公司内部建立 ISMS。

1.6 ISMS 实施需求

通过多方打听，请教专家，发现要全面解决公司的问题，并且有效改善现在的运营状况，最经济实用的方式就是建立一套 ISMS 体系，这比聘请几个 CISSP 专家、购买功能强大的各种安全产品彻底有效多了。公司成立信息安全管理小组，开始信息安全管理体系的建立和实施。

第2章 ISMS的建立及实施

2.1 建立及实施ISMS主要过程

建立ISMS是一项艰苦而细致的工作，创新公司的领导层要对ISMS的建立做出承诺，同时配备必要的人力、物力和财力资源，公司的全体员工也在体系建立过程中给予充分的配合。创新公司成立ISMS项目组，对ISMS的建立和实施进行了充分的策划和管理。通过策划，创新公司把整个过程分为5个阶段，其实施流程如图2-1所示。从项目启动到认证，整个项目实施周期为6个月。

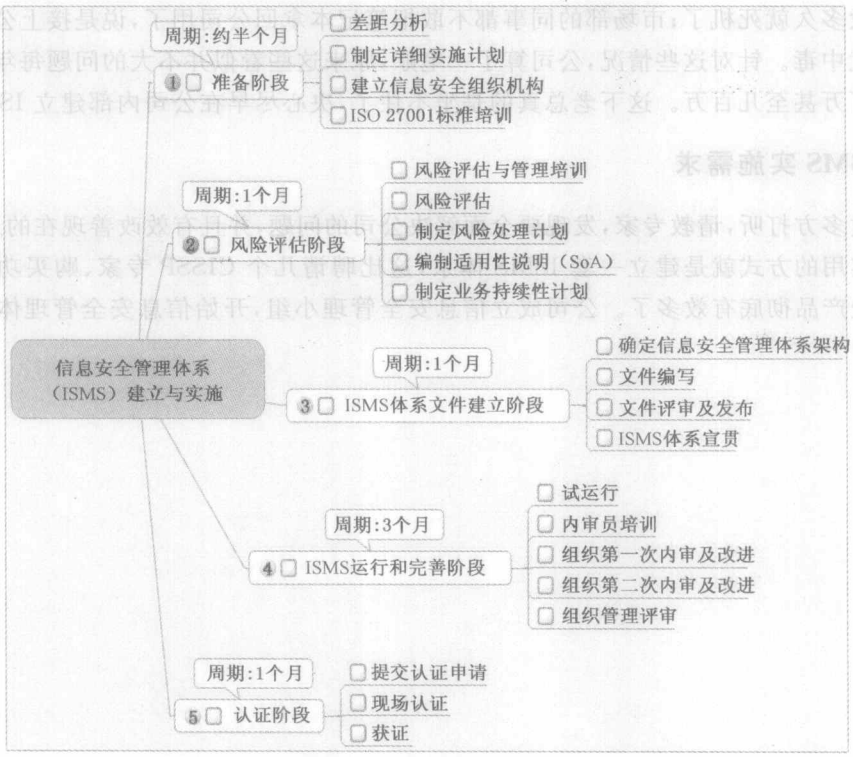

图2-1 ISMS建立与实施阶段图

2.2 各过程说明

2.2.1 准备阶段

2.2.1.1 成立信息安全管理小组

在项目启动初期，创新公司成立了信息安全管理小组，小组由各个部门的负责人和部门

指定的信息安全员组成，组长由公司 CIO 担任。信息安全管理小组组长同时被任命为公司 ISMS 的管理者代表。

整个信息安全管理小组共 14 个人，负责公司 ISMS 的建立和推广实施。信息安全管理小组在公司组织架构中的地位如图 2-2。另外每个部门还配备了至少一名的信息安全员。

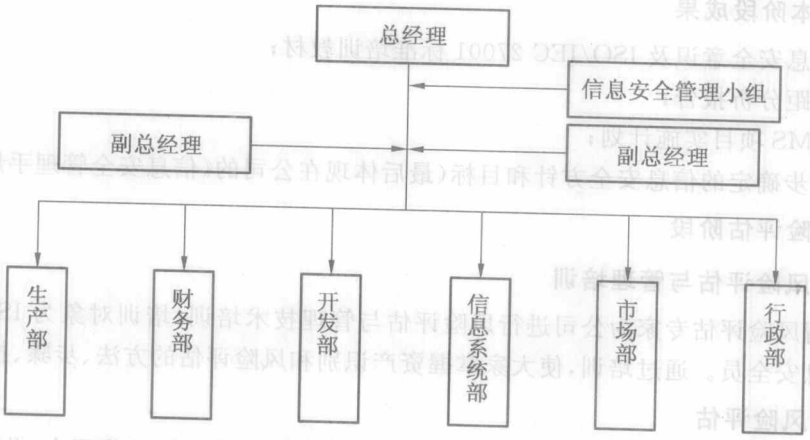

图 2-2 公司信息安全组织架构

信息安全管理小组的职责如下：

(1) 制定信息安全管理工作的方针、政策；

(2) 策划建立信息安全管理体系；

(3) 组织进行风险评估，评审和批准风险评估报告；

(4) 制定风险处理计划，监督风险处理措施的执行情况；

(5) 编制残余风险报告并提交给总经理批准；

(6) 负责处理重大信息安全事件；

(7) 负责监控 ISMS 实施情况；

(8) 负责 ISMS 持续改进。

部门信息安全员职责如下：

(1) 负责部门的资产登记及评价；

(2) 负责部门资产的风险评估；

(3) 负责传达公司的信息安全要求；

(4) 负责收集部门的信息安全需求并定期向 ISMG 汇报；

(5) 负责收集部门信息安全事件并定期向 ISMG 汇报。

2.2.1.2 开展 ISO/IEC 27001:2005 标准培训

创新公司请专家对公司内部员工进行为期 3 天的信息安全意识培训和标准详细解读培训，以提高公司员工的信息安全意识，熟悉 ISO/IEC 27001 标准要求，初步了解企业实施 ISMS 的过程、步骤、方法和资源要求等。

2.2.1.3 差距分析

创新公司请咨询公司的专家会同公司有关人员对公司现行的信息安全管理体系与

ISO/IEC 27001:2005信息安全管理体系标准要求进行比照性诊断，找出存在的问题和可以在新体系中继续采用的管理体制，作为下一步开展工作的依据。

差距分析后，公司ISMG根据差距情况，制定详细的项目实施计划，并确定体系覆盖范围、信息安全方针和目标。

2.2.1.4 本阶段成果

(1) 信息安全意识及ISO/IEC 27001标准培训教材；

(2) 差距分析报告；

(3) ISMS项目实施计划；

(4) 初步确定的信息安全方针和目标(最后体现在公司的《信息安全管理手册》中)。

2.2.2 风险评估阶段

2.2.2.1 风险评估与管理培训

公司请风险评估专家为公司进行风险评估与管理技术培训，培训对象为ISMG成员及部门的信息安全员。通过培训，使大家掌握资产识别和风险评估的方法、步骤、技巧。

2.2.2.2 风险评估

公司ISMG会同部门信息安全员在所确定的信息安全管理体系范围内，分析组织内与信息安全有关的资产，对资产进行识别与评价，识别和评价所面临的信息安全威胁、薄弱点及其对信息安全的影响，确认已有的信息安全控制措施，实施风险评估。详见第3章内容。

另外创新公司还请专业信息安全公司对公司的网络、服务器、信息系统等做了渗透性测试，从技术角度找出存在的系统弱点、漏洞及错误，并给予纠正。

2.2.2.3 制定风险处理计划

根据风险评估结果制定风险处理计划，计划主要列出对目前存在的风险应采取的安全控制措施、职责和优先级。详见3.10。

2.2.2.4 编制适用性声明(SoA)

适用性声明是组织为满足需要而选择的目标和控制方法的评论性文件。公司根据风险评估过程中所选择到的控制措施及公司业务需求编制适用性声明，在SoA中阐述了安全控制措施选择或不选择的理由。SoA发布前应经过管理层的批准。详见第5章内容。

2.2.2.5 制定业务持续性计划

公司根据风险评估结果，对公司的研发成果，也就是具有公司知识产权的资产采取灾难备份的措施，并制定了业务持续性计划。计划包括计划启动的条件、应急程序、备用程序、计划维护时间要求等。详见7.9.1。

2.2.2.6 本阶段成果

(1) 资产登记表；

(2) 渗透性测试报告；

(3) 风险评估报告；

(4) 风险处理计划；

(5) 残余风险报告；

(6) 适用性声明(SoA);

(7) 业务持续性计划。

2.2.3 ISMS 文件建立阶段

2.2.3.1 确定信息安全管理体系架构

文件化管理模式为当前管理体系普遍所采用。ISO/IEC 27001:2005 也对体系文件做出要求。ISO/IEC 27001:2005 作为建立和维持信息安全管理体系的标准,要求组织通过确定信息安全管理体系范围、制定信息安全方针、明确管理职责、以风险评估为基础,选择控制目标与控制方式等活动建立信息安全管理体系。

创新公司根据公司业务流程及差距分析、风险评估结果,依据 ISO/IEC 27001:2005 条文要素流程及控制要求,建立起自己的 ISMS 的架构,列出信息安全手册和必须编制的程序文件清单。公司将 ISMS 文件分为三个层次,如表 2-1。创新公司根据需求定义出具体文件列表,如表 2-2。

表 2-1 ISMS 体系文件层次架构

层次	文 件	备 注
第一层	信息安全管理手册、策略、适应性声明	
第二层	程序文件及规章制度	根据公司业务、组织结构及标准要求制定出相关的程序文件,定义各必要过程的文件和规章制度
第三层	记录	程序文件、指南或规章制度所产生的记录

表 2-2 ISMS 体系文件列表

文件编号	文件名称	记录编号	记录名称
ISMS-01	信息安全管理体系手册		
ISMS-02	信息安全适用性声明		
ISMS-03	信息安全策略		
ISMSP-001	文件控制程序	ISMSP-001-R01	《文件更改申请(通知)单》
		ISMSP-001-R02	《文件发送(回收)单》
		ISMSP-001-R03	《文件记录一览表》
ISMSP-002	记录控制程序	ISMSP-002-R01	《文件/记录作废(销毁)申请(通知)单》
ISMSP-003	内部审核控制程序	ISMSP-003-R01	《内部审核计划》
		ISMSP-003-R02	《内部审核检查清单》
		ISMSP-003-R03	《内部审核员名单》
		ISMSP-003-R04	《纠正/预防措施表》
		ISMSP-003-R05	《管理评审/内部审核报告》