信息安全管理体系
实施案例及文件集

谢宗晓　刘琦　主编

中国标准出版社

信息安全管理体系实施案例及文件集

谢宗晓　刘琦　主编

中国标准出版社

北京

内容提要

本书以虚拟的网上售书企业 e-BookStore 为具体案例介绍了部署信息安全管理体系(ISMS)的完整过程,包括项目启动、定义 ISMS 范围、确立 ISMS 方针、业务分析、评估与处置安全风险、风险管理设计、文件设计与编写、记录设计,以及内部审核和管理评审,其经验涵盖信息安全的共性问题,不只适用于 IT 及相关行业,还适用于包括金融、电力、石油石化、通信、政府、教育等在内的各领域。

图书在版编目(CIP)数据

信息安全管理体系实施案例及文件集/谢宗晓,刘琦主编.
—北京:中国标准出版社,2010(2010.6 重印)
ISBN 978-7-5066-5713-6

Ⅰ.①信… Ⅱ.①谢…②刘… Ⅲ.①信息系统-安全管理-体系-中国 Ⅳ.①TP309

中国版本图书馆 CIP 数据核字(2010)第 043967 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 15.25 字数 362 千字
2010 年 4 月第一版 2010 年 6 月第二次印刷
*
定价 **40.00** 元

编委会

主　编：

谢宗晓　刘　琦

副主编：

邓阿群　郑　榕　贺　焱

吴海燕　王海棠

编　委：

朱金娥　刘　燕　张　胜　肖泽昌

易勇强　徐孝忠　周延婷　康钧伟

曹　晶　王昭顺　程瑜琦　陈新来

魏　勇　毛俪颖　尹世强

前言

本书的主要目的是通过完整的案例向读者介绍信息安全管理体系(Information Security Management System, ISMS)是如何在一个组织中进行应用的。

GB/T 22080—2008《信息技术　安全技术　信息安全管理体系　要求》(ISO/IEC 27001:2005, IDT)的正式发布,毫无疑问会使ISMS在国内的推广应用上一个新的台阶。该标准的第4、5、6、7、8章建立了信息安全管理体系的框架,附录A直接引用GB/T 22081—2008《信息技术　安全技术　信息安全管理实用规则》(ISO/IEC 27002:2005, IDT)并与其保持一致,其中给出了11个安全域、39个控制目标、133项控制措施。正如标准所述:本标准为实施OECD指南中规定的风险评估、安全设计和实施、安全管理和再评估提供了一个强健的模型。事实上,ISMS目前已是业界所公认的信息安全最佳实践之一。

作为"最佳实践"之一,高深的理论基础并不是标准所关注的,推广、应用、实践、落地才是ISMS的关键之处。因此,本书中的篇幅也一样淡化理论上的讨论,而是直指"实践"本身。

如何才能使读者更好地理解ISMS呢?显然,用理论解释理论肯定无益于事。最好的办法就是举例子,用例子为读者描述一个活生生的ISMS,因此,本书从案例介绍开始,然后用很短的篇幅介绍了实施的过程,剩余篇幅为读者

描述了 e-BookStore 建立起来的 ISMS，这其中包括大部分的文件和记录模板。

e-BookStore 的案例是虚拟的，在《信息安全风险评估　概念、方法和实践》及《信息安全管理体系应用手册——ISO/IEC 27001 标准解读及应用模板》等书中已被引用，在本书中也保持了一贯的连续性。我们在设计过程中，尽量使 e-BookStore 行业特征弱化，从而能够保证案例和 GB/T 22080—2008 标准本身一样：适用于所有类型的组织（例如，商业企业、政府机构、非赢利组织）。

本书在成文过程中经历数次改动，这不仅使本书更为结构化，更重要的是使读者更容易理解 ISMS 文件体系。

感谢中国标准出版社的张宁主任，张主任从读者角度提出了很多宝贵的意见，其中包括减少空洞理论的讨论、提供更多实用的模板。感谢王西林和曹剑锋编辑在审稿过程中给出的有益建议。

本书成文仓促，错误在所难免，恳请读者批评指正。

编　　者

2010 年 4 月于北京

目 录

0 案例介绍

e-BookStore是虚拟的网上售书企业，在本书中以其为案例介绍部署ISMS(Information Security Management System，信息安全管理体系)的完整过程。

当然，不同类型的组织部署ISO/IEC 27001:2005必然存在不同之处。就行业来分析，目前比较典型的行业应用如表0-1所示。

表0-1 应用ISO/IEC 27001:2005的典型行业

序号	行 业	应 用 分 析
1	金融行业	金融行业包含大量的数据，对信息化的依赖程度也比较高，可以参考更细致的标准ISO 13569
2	电力(电网及发电企业)	应用广泛，电力行业是标准化的示范行业，其中对于质量管理体系、环境管理体系和职业健康管理体系的应用非常深入和规范。具体可见本书的文献[4]
3	IT企业	应用广泛，IT企业一般会最早认识到信息安全的重要性
4	BPO(业务流程外包)	此类企业对于认证的需求量最大，但是存在应用不规范的问题
5	石油石化(包括炼化企业)	石油石化企业集中度较高，因此数量很少，虽然应用ISO/IEC 27001，但是认证需求不大
6	通信企业	通信行业对数据的安全性要求也非常高，但是目前数量较少，认证的范围基本以省级分公司为主
7	政府组织	应用，但是认证需求不大
8	教育系统(包括各类学校)	同政府组织
9	国税、烟草、工商等	同政府组织
10	卫生组织(包括各类医院)	各类医院中有大量的人员隐私信息，会是应用的重点，但是一般应用中可以参考更细致的标准ISO/IEC 27799

但是，正如ISO/IEC 27001:2005中1.1总则所指出的：本标准适用于所有类型的组织(例如，商业企业、政府机构、非赢利组织)。也就是说ISO/IEC 27001:2005是抛开了行业的差异性，对信息安全共性进行讨论的标准。事实上，在实际部署过程中，各个组织的共性也非常多。

e-BookStore正是总结了这些组织的共性而得到的一个完整案例，其经验不是只适用于IT行业或相关行业，而是适用于所有的行业。

在本书中不再对ISMS作入门性的介绍，读者可以参考文献[1]或文献[2]。

文献[1]中对目前ISMS系列标准的概况进行了介绍，并对ISO/IEC 27001:2005(GB/T 22080—2008)及ISO/IEC 27002:2005(GB/T 22081—2008)做了详细的解读，并在后续章节中对ISMS在一个组织中的部署进行了指导。

文献[2]对于信息安全、信息安全管理体系、信息安全风险评估等相关的概念给出了定义和解读，并在后续章节中介绍了信息安全管理体系审核的相关概念和方法。

0.1 概述

e-BookStore 创建于 1999 年 8 月，是目前最具竞争力的网上中文图书城之一，每天通过互联网向全球中文读者提供超过 100 多万种的中文图书和音像制品。e-BookStore 的使命是：让全球中文读者做到“鼠标轻松一点，好书即到眼前”。目前已有超过 1 000 万的注册用户在 e-BookStore 上订购过自己喜爱的图书和音像制品，e-BookStore 每月的营业额已超过 1 000 万元人民币。

*e-BookStore*是公司目前使用的 logo，公司网址为 www. e-bookstore. com。

e-BookStore 的办公地点在北京上地科技园区融安大厦 8 层，办公场地面积 1 200 m^2。该大厦刚刚启用一年，有比较完备的防火与供电设施。

0.2 组织架构

e-BookStore 现有员工 219 人，CEO(首席执行官)柴璐。

公司下设七个职能部门，基本情况如表 0-2 所示。

表 0-2 公司基本情况

部 门	主 要 功 能	负责人	人数
客户服务部	用户相关的工作，包括发货、退换货、投诉处理、客户联络、疑问解答	刘琦俪	67
采购部	图书、音像制品采购，合作伙伴、供应商等选择	程瑜	15
技术部	EBS 系统、OA 系统的设计、开发和运维；IT 基础设施的建设和运维	张毅凯	98
营销部	制定和实施营销策略，包括广告、宣传、营销政策制定等	李旭	29
财务部	财务计划的制定和实施，收款、支付、记账、报税等财务相关工作	韩龙龙	3
行政部	后勤保障和日常事务，办公设备采购，固定资产管理，商业秘密保护等	毛颖	3
人力资源部	制定和实施人力资源计划，包括人员招聘、绩效考核、岗位职责定义	张志宏	4

公司管理层组织架构如图 0-1 所示。

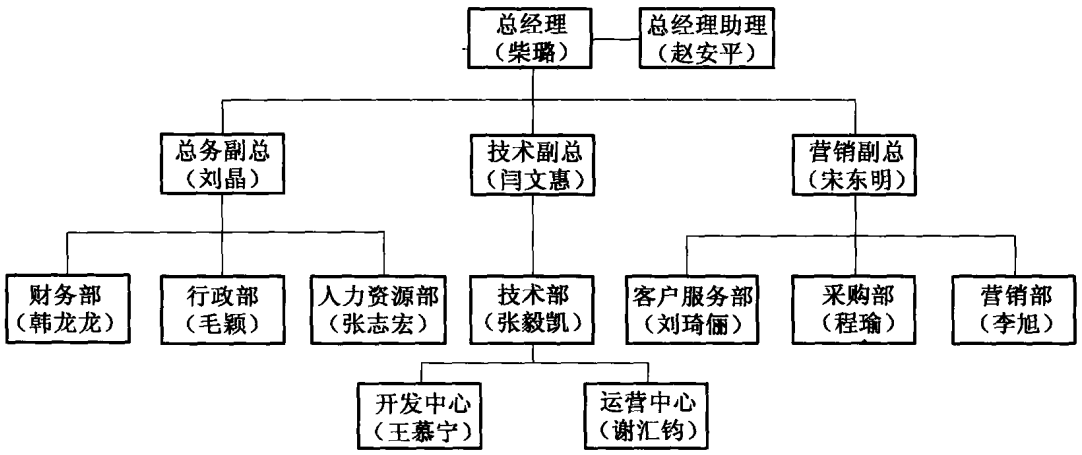

图 0-1 组织架构图

0.3 业务介绍

e-BookStore 建立了庞大的物流支持系统，包括在北京建立了 2 万 m^2 的仓库。通过庞大而先进的物流支持系统，e-BookStore 员工每天把大量的图书和音像制品通过航空、铁路、公路、水运等快捷运输手段送往全球各地，然后由本地的快递公司为 e-BookStore 读者提供“送货上门”服务。

e-BookStore 为用户提供了灵活的支付方式，如网上支付、邮局汇款及货到付款等。e-BookStore 在自己发展的同时，也促进了网上支付、邮政快递、图书音像出版等不同行业的快速发展。

为了更直观地了解 e-BookStore 的业务特点，本书首先介绍用户购书的过程，更详细的业务介绍将在之后的章节中陆续给出。

0.4 信息系统

为了实现使命，e-BookStore 主要运行以下四个主要信息系统：

a) 网上售书系统(“EBS”系统)；

b) 办公自动化系统(“OA”系统)；

c) 财务软件系统(“U8”系统)；

d) 仓储及物流管理系统。

这些系统运行在 e-BookStore 搭建的基于 TCP/IP 技术的局域网上，为了保证网络速度，e-BookStore 将核心服务器均托管在专业 IDC(Internet Data Center，数据中心)机房。

关于这些信息系统的详细情况会在风险评估的相关章节中进行介绍。

网络拓扑如图 0-2 所示。

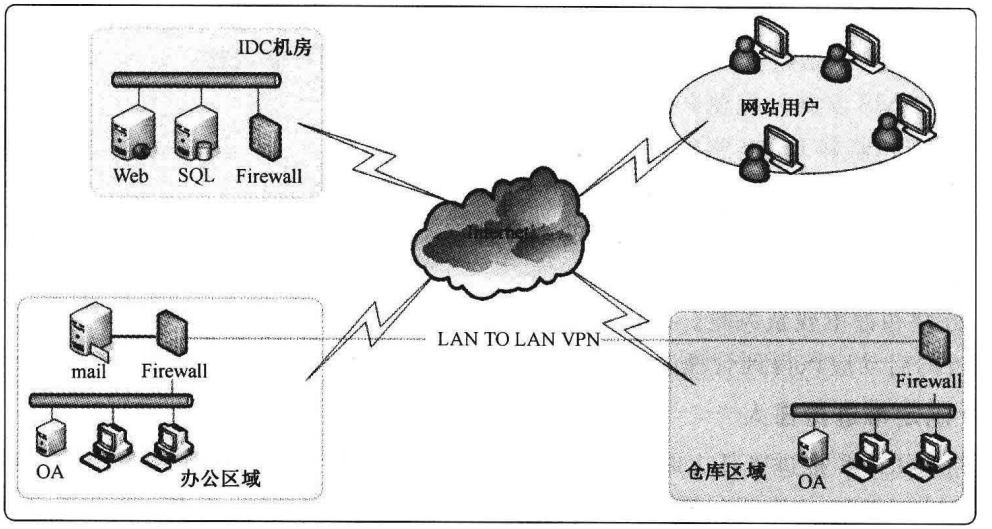

图 0-2 网络拓扑图

1 实施流程

1.1 启动项目

采用 ISMS 是 e-BookStore 的一项战略性决策，这不仅能提升信息安全管理水平，对组织的整个管理水平也会有很大的提升。

1.1.1 定义初始目标与范围

ISMS 的目标直接影响着 ISMS 的设计和实施，这些目标可能包括：

a) 保证 e-BookStore 网上售书主营业务的业务连续性；

b) 提高 e-BookStore 网上售书系统等重要业务系统的灾难恢复能力；

c) 提高信息安全事件的防范和处理能力；

d) 促进与法律、法规、标准和政策的符合性；

e) 保护信息资产；

f) 使信息安全能够进行测量与度量；

g) 降低信息安全控制措施的成本；

h) 提高信息安全风险管理的水平。

由于实施 ISMS 的复杂度与范围大小紧密相关，因此在定义了初始目标之后，应圈定初始的范围，以请示领导。

1.1.2 获得管理者正式批准

管理者的支持是项目成败的最关键要素之一，这些支持可能包括：

a) 为 ISMS 实施分配独立的预算；

b) 批准和监督 ISMS 实施；

c) 安排充分的 ISMS 的实施资源；

d) 把 ISMS 实施和业务进行充分的结合；

e) 促进各部门对信息安全问题的沟通；

f) 处理和评审残余风险。

项目的启动应该得到管理者正式的书面认可。

1.1.3 确定推进责任人

在指定 ISMS 推进责任人时，最重要的考虑是：

a) 保证 ISMS 的协调和最终责任人在高层(通常是主管信息化工作的单位领导)；

b) 指定 ISMS 推进的直接责任人为中层领导(通常是信息化主管部门领导)；

c) 由信息安全主管人员具体负责 ISMS 的推进过程；

d) 每一个员工/借调员工都要在其工作场所和环境下，承担相应的责任。

在推进过程中，不但要涉及相关的责任人，还可能涉及其他角色。

具体角色的安排请参见 4.1.3“信息安全管理体系职责”。

1.1.4 召开项目启动会议

管理者的支持还应包括对员工思想上的动员，思想上的动员可以采取召开项目启动会议的方式完成。

会议应清晰的向员工阐述：

a) ISMS 对本组织而言的重要性(通过举例子的方式)；

b) 项目所涉及的初始范围及相关部门。

1.2 定义 ISMS 范围

实施 ISMS 的工作量与 ISMS 界定的范围大小密切相关，因此，ISMS 的范围和边界必须合理地加以定义。

1.2.1 定义责任范围

可以通过调研组织的管理结构、部门设置和岗位责任等，界定 ISMS 的责任边界。实施这个步骤时，需要考虑：

a) 受到影响的不止内部相关部门，还可能有外部相关方；

b) 负责 ISMS 的领导应基本上与受影响范围的负责人是一致的，如果信息系统的责任部门不止一个，那么则应该由更高一层的领导来负责协调；

c) 定义的范围，必须能够在该范围内实现 ISMS 的 PDCA 循环。

1.2.2 定义物理范围

物理边界的定义包括识别应属于 ISMS 范围的组织内的建筑物、场所或设施等。

处理跨越物理边界的信息系统是很复杂的，这可能包含：

a) 移动访问；

b) 远程设施；

c) 签署的第三方服务；

d) 无线网络。

这些问题应通过定义适当的界面和服务层次加以解决。

1.2.3 完成范围概要文件

在定义 ISMS 范围的时候，这些范围和边界可以以不同的方法合并在一起。例如：物理场所(如建筑物、数据中心或办公室)和这个物理场所的关键流程应并入该范围内。信息系统的移动访问就是一个例子。

描述 ISMS 范围和边界的文件，应包括以下信息：

a) 业务特性；

b) 关键业务过程列表；

c) 组织结构文件；

d) 场所和楼层位置图；

e) 网络拓扑；

f) 设备部署；

g) 处理的信息资产；

h) 对 ISMS 范围的删减的合理性说明。

范围概要文件请参见4.1.1“信息安全管理体系方针”(或4.1.2“信息安全管理手册”)。

1.3 确立ISMS方针

信息安全方针是组织总体方针的一部分,是保护敏感、重要或有价值的信息所应该遵守的基本原则。

1.3.1 制定ISMS方针

制定ISMS方针的过程如下:

a) 根据电子商务的业务要求,建立ISMS的目标;

b) 确定实现ISMS目标的工作重点;

c) 考虑业务要求、法律、法规和政策要求的安全义务;

d) 确定风险评价的准则;

e) 建立风险评估的框架;

f) 阐明高层领导的责任,以确保信息安全管理的需要;

g) 获得管理者的批准。

1.3.2 准备ISMS方针文件

ISMS方针文件应至少包括下面这些内容:

a) 信息安全的总体目标、方向和原则。

b) 明确的ISMS的目标,该目标应在初始目标的基础上确定。

c) 为实现ISMS的目标所建立的框架,包括组织框架和各种信息安全活动的框架。

d) 风险评估和风险处理的框架。

e) 风险评价的准则以及接受风险的准则。

f) 特别重要的安全方针策略、原则、标准和符合性要求的简要说明,可包括:

- 符合法律、法规和政策要求;
- 安全教育、培训和意识要求;
- 业务连续性管理;
- 信息安全事件处理。

ISMS方针文件应该易于理解,并及时传达给ISMS范围内的所有用户。

详细的文件示例,请参见4.1.1“信息安全管理体系方针”。

1.4 进行业务分析

在管理者已经批准实施ISMS,并定义了ISMS的范围和ISMS方针之后,需要进行业务分析,以确定组织的安全要求。

1.4.1 定义基本安全要求

在本步骤中,为了阐明ISMS信息安全要求,应:

a) 确认组织的信息安全目标,并识别所确认的目标对未来信息处理要求的影响;

b) 识别ISMS范围内的主要业务、流程和功能;

c) 识别当前应用系统、通信网络、活动场所和IT资源等;

d) 识别关键信息资产及其在保密性、完整性和可用性方面的保护;

e) 识别所有基本要求(例如法律、法规、政策、标准、业务要求、行业标准、供应商协议,