信息安全管理体系应用手册

——ISO/IEC 27001标准解读及应用模板

谢宗晓　郭立生　主编

中国标准出版社

信息安全管理体系应用手册

——ISO/IEC 27001标准解读及应用模板

谢宗晓　郭立生　主编

中国标准出版社

北京

内 容 提 要

本书从论述信息安全管理体系基础入手，分析了 ISO/IEC 27001:2005、ISO/IEC 27002:2005 等 ISMS 相关重要标准，结合 PDCA 循环模型，对如何设立和建立 ISMS、实施和运行 ISMS、保持和改进 ISMS 进行了详细的论述并辅以大量的应用模板，是一个实用的信息安全管理体系应用手册。

本书适用于从事信息安全管理工作的技术人员、管理者以及进行相关培训、认证的人员。

图书在版编目(CIP)数据

信息安全管理体系应用手册：ISO/IEC 27001 标准解读及应用模板/谢宗晓，郭立生主编. —北京：中国标准出版社，2008

ISBN 978-7-5066-5040-3

Ⅰ. 信… Ⅱ. ①谢…②郭… Ⅲ. 信息系统-安全管理-国际标准，ISO/IEC 27001-手册 Ⅳ. TP309-65

中国版本图书馆 CIP 数据核字(2008)第 146784 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 16.25 字数 379 千字

2008 年 10 月第一版 2008 年 10 月第一次印刷

*

定价 **45.00** 元

编委会

序

这本手册，是从事信息安全管理体系(ISMS)咨询服务的同志根据自己对国际标准化组织制定的ISMS标准(ISO/IEC 27000系列)的学习体会和实践经验编写的。书中重点解读了建立信息安全管理体系的要求和管理控制措施选择(ISO/IEC 27001《信息安全管理体系　要求》，ISO/IEC 27002《信息安全管理实用规则》)；并用自己的实践经验，从一个组织如何建立信息安全管理体系的角度阐述了标准相关的过程和活动，以及过程活动中需要完成的输入输出结果，此外还提供了相关的文件模板和表单，有助于我们加深对建立ISMS的理解。

我国正在根据《国家信息化领导小组关于加强信息安全保障工作的意见》(中办发[2003]27号)开展一系列有关信息安全保障的基础性工作。文件提出的“立足国情，以我为主，坚持技术管理并重”的要求已经成为大家共识的工作方向。信息系统安全等级保护制度的贯彻落实正在深入进行，重要信息系统和基础信息网络的信息系统安全等级保护定级工作大体在2007年完成，符合等级保护要求的信息系统安全建设工作将成为新的工作重点。能否在等级保护建设中落实“技管并重”将是对我们的一次考验。

信息安全管理已经从零散的重结果的管理，发展到系统的重过程的建立信息安全管理体系的阶段。ISO/IEC 27000系列标准体现了这种转变。我国积极参与了ISO/IEC SC27信息安全管理体系标准的制定工作，并把ISO/IEC 27000系列标准采纳为我国国家标准。ISO/IEC SC27已经正式颁布的相关最新国际标准(ISO/IEC 27001，ISO/IEC 27002，ISO/IEC 27006)正处在转化为国标的工作过程中，不久即将公布。

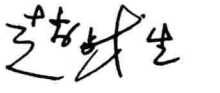
在转化过程中，国信办组织了ISMS标准的试点工作，参与试点的单位根据自己的体会认为，这套标准总体上适合需要，有助于加强信息安全保障的管理工作。

“要我做”和“我要做”是面对ISMS的两种不同心态。一些对信息化依赖程度高的单位，已经领悟到ISMS的建立绝非是给别人看的，它涉及一个单位信息化成败的核心利益。领导重视和全员参与是建立和运行ISMS的关键成功因素。只有领导重视才能把ISMS的建立放到单位繁忙工作的应有位置；才能保证制定出结合单位使命和业务的正确的方针、目标、策略；才能承诺和保证建立和运行ISMS的必要的人、财、物资源；才能指导和指令全员责任的落实；才能持续关注ISMS，使之得以持续的发展和改进提高。只有全员参与才能把复杂的ISMS责任分解到应有的责任人；才能在信息安全保证工作中形成人人有事做，事事有人做，做事有依据的氛围和局面；才能把通常高喊的“齐抓共管”的口号落到实处。

风险管理的思想和方法应该贯穿于ISMS的全过程。识别风险、分析风险、处置风险，通过选择适合单位信息安全保障的安全控制措施把等保定级的系统面对的风险保持在可接受的程度内是决定我们投资效益的基本依据。

技术需要管理，管理需要技术。国际上通过开发自动化工具的手段加强信息安全保障工作的执行力，形成信息安全管理的常态化的动态值得我们关注。我们需要加速自主的研究和开发，拿出我们自己的支持ISMS的自动化工具和手段。

祝愿我国的信息安全保障工作者，结合国情，努力工作，创造出更多的ISMS的实践经验，对ISMS的科学持续发展做出应有的贡献。



2008年7月15日于北京

前言

在全球信息技术高度发达的今天，随着计算机及网络技术的发展和普及、社会信息化进程的快速推进，电子政务、电子商务、网上银行、网络游戏、ERP等已成为当前IT技术的应用热点。网络技术和其他信息技术正在改变传统的生产、经营和生活方式，并逐渐成为新的经济增长点。我国国民经济和社会发展对网络和信息系统的依赖性不断加强，整个人类社会对计算机网络和信息系统的依赖程度也越来越大，网络对许多人来说已成为工作和生活中必不可少的一部分。但网络在给我们带来极大便利的同时，也带来了一些棘手的问题，其中的突出问题就是网络信息安全。

信息网络国际化、社会化、开放化、个人化的特点，使国家的信息领域不断延伸。国际上围绕信息的获取、分析、使用和控制的竞争越来越激烈，网络信息安全正成为维护国家安全、保持社会稳定、影响长远利益的一个关键组成部分，备受各国政府的关注和重视。近年来，僵尸网络(Botnet)、网络仿冒(Phishing)、木马、间谍软件、零时间威胁等新威胁的不断恶化，更使得网络安全问题成为大家关注的焦点，也使人们充分认识到了网络信息安全综合防护系统建设的重要性和紧迫性。作为一个亟待解决的关键问题，网络信息安全不但是发挥信息革命带来的高效率、高效益的有力保证，而且是对抗信息霸权主义、抵御信息侵略的重要保障。网络信息安全保障能力建设成为21世纪各国综合国力、经济竞争实力和生存能力的重要组成部分。

随着整个业务环境的变化，企业是否意识到飞速发展中的信息技术所蕴涵的风险？无论是意外宕机、数据丢失、系统

崩溃、网络攻击，还是自然灾害、市场变幻、政策调整、流量峰值……，各种突如其来的信息安全风险就像暗礁，潜伏在企业周围，风险无处不在。由于IT的失败给商业带来影响的例子比比皆是，诸如：美国、瑞典大量信用卡的数据失窃；因为一个零售商IT系统出现问题导致大量客户信用卡的数据被盗窃，从而造成巨额的损失等。

所有这些教训都应该使我们认识到：加强企业信息安全管理能力已迫在眉睫。企业需要一个完整的业务不间断性计划，从评估一直到实施，为业务运行保驾护航。组织的业务目标和信息安全要求紧密相关，任何组织或企业，其成功经营的能力在很大程度上取决于其有效地管理其信息安全风险的能力。因此，如何确保信息安全已是各种组织改进其竞争能力的一个新的挑战任务。

企业不但面临着信息安全方面的问题，同时还面临合规方面的问题、系统可用性问题以及业务可持续性问题等越来越多的问题。面对繁杂的监管法规（如：萨班斯—奥克斯利法案）和管理理论，应如何选择建立最适合自己企业的信息安全管理体系？一个组织建立了规范的信息安全管理体系，如何解决日常经营管理的灵活性和规范性的矛盾？在风险与效率之间如何才能达到一个理想的平衡点？随着市场的不断发展和变化，一个企业的业务范围、流程也需要随之调整，如何才能保持企业的ISMS持续合规？这些问题已经摆在了我们的面前，本书内容对您理解和解决这些问题将会大有裨益。

组织建立一个基于ISO/IEC 27001:2005的ISMS，已成为信息化发展的需要。本书作者从论述信息安全管理体系基础入手，分析了ISO/IEC 27001:2005、ISO/IEC 27002:2005等ISMS相关重要标准，结合PDCA循环模型，对如何设计和建立ISMS、实施和运行ISMS、监视和评审ISMS、保持和改进ISMS进行了详细的论述，是一个实用的信息安全管理体系应用手册。相信本书的推出定会对我国从事ISMS工作的相关人员更好地理解和实施信息安全管理体系起到很好的帮助和借鉴作用，同时，也可为我国信息安全管理体系的实施工作起到积极的推动作用。

刘宝旭

2008年7月18日

目 录

第 1 章 信息安全管理体系基础

1.1 什么是信息安全

1.1.1 信息及信息系统

1. 信息的定义

信息(information)的定义多种多样。人们从哲学、信息论、控制论和社会学等各个角度对信息进行了定义。从哲学的角度来看,信息是物质的一种普遍属性,本质属性。事物在运动中发出一定的信号,这些能够被其他事物所感知的表征该事物特征的信号的内容即为该事物向其他事物所传递的信息。更为明确的定义,例如 GB/T 4894—1985《情报与文献工作词汇 基本术语》将信息定义为:物质存在的一种方式、形态或运动状态,也是事物的一种普遍属性,一般指数据、消息中包含的含义,可以使消息中描述的不确定性减少。

事实上,Merriam-Webster Collegiate Dictionary(韦氏大辞典)对于信息的解释更为全面。下面一段是其对于 information(信息)词条的解释,其中释义 2 中对于常见的信息已经做了大致的分类。

1: *the communication or reception of knowledge or intelligence*;

2: ***a*** *(1): knowledge obtained from investigation, study, or instruction (2): intelligence, news (3): facts, data* ***b***: *the attribute inherent in and communicated by one of two or more alternative sequences or arrangements of something (as nucleotides in DNA or binary digits in a computer program) that produce specific effects* ***c*** *(1): a signal or character (as in a communication system or computer) representing data (2): something (as a message, experimental data, or a picture) which justifies change in a construct (as a plan or theory) that represents physical or mental experience or another construct* ***d***: *a quantitative measure of the content of information; specifically: a numerical quantity that measures the uncertainty in the outcome of an experiment to be performed*;

3: *the act of informing against a person*;

4: *a formal accusation of a crime made by a prosecuting officer as distinguished from an indictment presented by a grand jury*.

从上面的定义中可以看出,信息、消息(message)和信号(signal)之间有密切联系,信息常以消息形式表现出来,并通过信号来传递,但是三者之间是有区别的。消息可能包含丰富的内容,也可能根本就不包含任何信息。消息是外壳,而信息则是消息的内核。信号是信息的载体,同一种信息可以用不同的信号表示,而一种信号也可能传递了不同的信息。

同理，信息和数据(data)也是不同的，在GB/T 4894—1985的定义中将数据和信息划为相同的范畴。一般认为，数据是对某种情况的记录，包括数值数据(例如各种统计资料数据)以及非数值数据(例如各种图像、表格、文字和特殊符号等)两种；而信息则一般理解为经过加工处理后具有参考价值的数据。因此，数据也可以认为是信息的外壳，与消息相比只是表现形式不同。

可以把信息简单地定义为：信息就是经过加工的数据或消息，信息是对决策者有价值的数据。

2. 信息系统的定义

“系统”(system，在标准中一般被翻译为体系)来源于拉丁语 systēma。ISO 9000：2000《质量管理体系　基础和术语》中将体系定义为：相互关联或相互作用的一组要素。系统有两个以上要素，各要素和整体之间，整体和环境之间存在一定的有机联系。

系统由输入、处理、输出、反馈、控制五个基本要素组成。

一般而言，信息系统(information system)指的是输入数据，经过处理后，输出信息的特殊系统。

更详细的信息系统的定义为：一个以人为主导，利用计算机硬件、软件、网络通讯设备以及其他办公设备，进行信息的收集、传输、加工、存储、更新和维护的人机系统。

虽然信息系统与计算机并没有必然的联系，但是毫无疑问，计算机的出现使信息技术出现了前所未有的革命，也使信息量急剧的膨胀。本书所讨论的信息系统都是以计算机作为核心的。

3. 信息系统的发展

19世纪末 Herman Hollerith 发明了第一台电子穿孔卡(punched card)用于处理数据，这种系统于1890年被美国人口普查局(US Bureau of the Census)广泛地用于统计报告。1946年第一台电子计算机的产生，将新的设备用作数据输入的手段，在其后的五六十年，信息系统技术手段的发展更是日新月异。

现将信息系统的发展经历大致总结如下：

(1) 20世纪50年代：

- 穿孔卡系统(punched card systems)；
- 大型机(large-scale computers)；
- 中型机(medium-size computers)；

(2) 20世纪60年代：

- 小型机(small-scale computers)；
- 晶体管(transistor)与主存(core-memory)；
- 并发系统；
- 实时与在线系统；

(3) 20世纪70年代：

- 微处理器、网络与病毒(worm)；
- 个人计算机出现；
- 网络(network)出现；

- 进一步的安全考虑；
- 病毒出现；

(4) 20 世纪 80 年代：

- 工业化时代；
- 个人计算机(personal computer)普及；
- 局域网(local area network)；

(5) 20 世纪 90 年代：

- 全面互联(interconnection)；
- 因特网(Internet)与 www(world wide web)。

1.1.2　信息安全及其定义

1. 信息安全在各个阶段的重点

由信息的定义可知：信息安全(information seurity)的历史远远早于信息系统。实际上，加解密的应用最早可以追溯到公元前 1800 年以前的古代埃及，对于密码学的历史，可以参阅文献[5]，其中叙述了密码学从古埃及时代一直到 1963 年 4 000 多年的发展历史。但是由于本书所讨论的信息安全着重于以计算机为核心的信息系统，因此本章节中所讨论的信息安全发展历程从 20 世纪 40 年代开始。

早在二十世纪四五十年代，人们认为信息安全就是通信保密，采用的保障措施就是加密和基于计算机规则的访问控制，这个时期被称为“通信保密(COMSEC)”时代，其时代标志是 1949 年 Shannon 发表的《保密通信的信息理论》；在 70 年代，人们关心的是计算机系统不被他人所非授权使用，这时学术界称之为“计算机安全(INFOSEC)”时代，其时代特色是美国 80 年代初发布的橘皮书——《可信计算机评估准则》(TCSEC)；90 年代，人们关心的是如何防止通过网络对联网计算机进行攻击，这时学术界称之为“网络安全(NETSEC)”，其时代特征是美国 80 年代末出现的“莫里斯”蠕虫事件；进入了 21 世纪，人们关心的是信息及信息系统的保障，如何建立完整的保障体系，以便保障信息及信息系统的正常运行，这时学术界称之为“信息保障(IA)”。

对照信息系统的发展阶段，很容易理解信息安全侧重点的发展过程，如表 1-1 所示。

表 1-1　信息系统及信息安全发展的对比

信息系统的发展阶段	信息安全的侧重点及分析
20 世纪 50 年代： • 穿孔卡系统(punched card systems)； • 大型机(large-scale computers)； • 中型机(medium-size computers)	通信保密(COMSEC)。在这个时代及这个时代之前，密码学一直是信息安全的核心甚至是全部(当然，目前仍然是信息安全的重要基础)。由于计算机尚未全面发展，因此基于加解密的通信安全是主要的关注点
20 世纪 60 年代： • 小型机(small-scale computers)； • 晶体管(transistor)与主存(core-memory)； • 并发系统； • 实时与在线系统	

续表 1-1

信息系统的发展阶段	信息安全的侧重点及分析
20 世纪 70 年代： • 微处理器、网络与病毒(worm)； • 个人计算机出现； • 网络(network)出现； • 进一步的安全考虑； • 病毒出现	计算机安全(INFOSEC)。二十世纪六七十年代是计算机迅猛发展的 20 年，尤其集中计算、未授权使用等问题是关注的焦点
20 世纪 80 年代： • 工业化时代； • 个人计算机(personal computer)普及； • 局域网(local area network)	
20 世纪 90 年代： • 全面互联(interconnection)； • 因特网(Internet)与 www(world wide web)	网络安全(NETSEC)。网络的全面普及使得逻辑位置变得比物理位置更重要，因此网络安全成为重中之重。目前网络安全依然是很多组织面临的重要问题

中国科学院信息安全国家重点实验室吕述望教授认为，未来信息安全的发展方向是知识安全。按照这个理论，在信息资源中，数据是事实与数字组成的原始的素材；信息是对原始素材进行整理后形成的消息与情报；知识是对消息与情报进行理性分析与综合后形成的系统的认识和思想及清晰表述的论断。那么，知识安全是数据安全和信息安全的扩展与延伸，又是信息资源安全一个新的发展阶段。

2. 信息安全的定义

从其发展的历史看，信息安全同信息本身的定义一样是一个很宽泛的概念，很难精确地加以定义。目前，国内外对信息安全的定义主要分为两类：从安全内容进行定义和从安全属性进行定义。

1) 从安全内容进行定义

从安全内容进行定义强调安全涉及的方面。

一种是在定义中历数信息安全涉及的保护区域。例如：信息安全是与保护相关的概念，其目的是保护组织的资产，至少要包括下面这些方面：管理实践、物理安全、人员安全、主机安全、网络安全、通信安全和操作安全等。

另一种是从信息系统的纵向防御结构进行定义。这种定义一般把“信息安全”局限在狭义概念。例如，在 GA 163—1997《计算机信息系统安全专用产品分类原则》中：本标准适用于保护计算机信息系统安全专用产品，涉及实体安全、运行安全和信息安全三个方面。实体安全包括环境安全、设备安全和媒体安全三个方面。运行安全包括风险分析、审计跟踪、备份与恢复、应急四个方面。信息安全包括操作系统安全、数据库安全、网络安全、病毒防护、访问控制、加密与鉴别七个方面。

2) 从安全属性进行定义

从安全属性进行定义强调安全的目标。

例如：ISO/IEC 27002:2005 中定义信息安全：保证信息的保密性(confidentiality)、完整性(integrity)和可用性(availability)；另外也可包括诸如真实性(authenticity)、可核查性(accountability)、不可否认性(non-repudiation)和可靠性(reliability)等。

在 ISO/IEC 27002:2005 引言中提出信息安全是保护信息免受各种威胁的损害，以确保业务连续性、业务风险最小化、投资回报和商业机遇最大化。这里也强调了信息安全的目标，并且把其看作是组织的有机组成的一部分，最终目的是确保“投资回报和商业机遇最大化”。

从上面的定义中可以看出：信息安全的目标是保证信息的一系列安全属性，从而达到对组织业务盈利能力的支撑作用；这个目标是通过一系列的控制措施来实现的，这些措施应该覆盖信息安全相关的各个方面，包括信息、信息处理设施、信息处理者和衍生出来的信息的安全利用等。

注：ISO/IEC 27002:2005《信息安全管理体系 实用规则》原来编号为 ISO/IEC 17799:2005。该标准于 2005 年被修改转化为 GB/T 19716—2005。

1.1.3　信息资产的安全属性

在 ISO/IEC 27002:2005 的信息安全定义中涉及了信息资产的安全属性，其中 ISO/IEC 13335-1:2004 定义：保密性是信息不能被未授权的个人、实体或者过程利用或知悉的特性；完整性是保护资产的准确和完整的特性；可用性是根据授权实体的要求可访问和利用的特性；真实性是保证主体或资源确系其所声称的身份的特性。真实性应用于诸如用户、过程、系统和信息等的实体；可核查性是确保实体行为能被有效跟踪的特性；可靠性是与预想的行为和结果相一致的特性。

注：ISO/IEC 13335-1:2004《IT 安全概念和模型》将会被 ISO/IEC 27005 代替，ISO/IEC 27005 目前尚没有正式版本发布。

1. 信息资产的属性

保密性、完整性和可用性是信息资产最重要的三个属性，国际上称之为信息的 CIA 属性或者信息安全金三角。其缩写恰好与美国中央情报局(Central Intelligence Agency，简称 CIA)一致。

信息安全的三个属性的关系如图 1-1 所示。

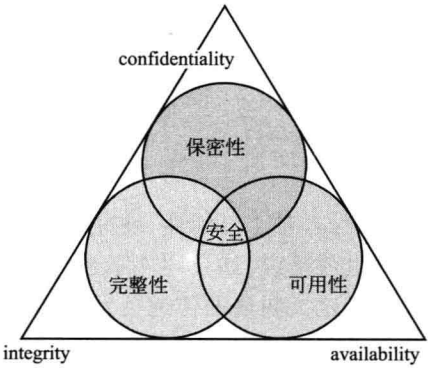


图 1-1　安全属性

对保密性而言，信息不能泄露给未授权者，这些未授权者可能包括个人、实体或者是过程。泄露的途径有很多，例如口头泄露，通过网络、打印机、复印机、USB 存储设备等泄露。可以这样通俗地理解保密性：只有授权个人、实体或者是过程才能访问受保护的信息。保密性是在日常的信息安全工作中强调的比较多的方面，也是最容易理解的一个属性。因为保密性没有其他两个属性的含义那么宽泛，而且用户很容易与现实世界中的保密的概念进行类比。

完整性通常被理解为“防止未授权的更改”和“防篡改”等，在不同的环境往往被赋予不同的含义。在信息安全领域，信息资产的完整性往往还要意味着：