# 剖析 ISO27001:2005

Information technology — Security techniques —
Information security Management systems — Requirements

信息技术—安全技术—信息安全管理体系要求

Version 1.0

2008 年 3 月

# 文档说明

在翻译时，我尽力揣摩每条英文的含义以及标准制定者的意图，希望用深入浅出的方式表达出来。虽然翻译的整个过程从 2008 年 1 月一直持续到 2008 年 3 月，但是由于本人学识浅薄，水平有限，很难做到完美。希望看过本文者，给我提出修改意见和建议，在下感激不尽；期望借助大家的力量，把她完美起来。



熊甲林

2008 年 3 月 26 日

联系方式：

Blog: http://hi.baidu.com/xiongjialin

MSN: cobitcissp@hotmail.com

# 我与 ISO2700X 的亲密关系

在众多信息安全标准中，令我最动情的要数 ISO2700X。其中的原由，还得从过去说起。话说 1999 年，我刚刚迈出大学校门，放弃了留在上海的机会，毅然来到改革春风吹拂的深圳。当时，我充满了豪情壮志，妄想着成为中国的比尔盖兹。第一份工作自然是软件开发，编起程序来劲头十足，往往是废寝忘食。不出 3 个月，已经是公司的开发主力了。随着工作内容的不断重复，创造性的乐趣越来越少，软件开发的兴趣日渐消亡，原来的理想也随之暗淡。1 年后，转做 DBA 和小型机管理方面的工作，还在同一家公司。应用程序属于信息系统最上层的部分，在做软件开发时不清楚操作系统、数据库、网络等底层的运作，一直很好奇。做 DBA 和小型机的管理给了我解开疑惑，满足好奇的机会。仗着刨根问底和不懈钻研的精神，很快就成为系统管理的骨干。这时，我把理想定位在做中国最出色的 DBA。就在我 DBA 之梦如日中天的时候，公司从海外空降了一位 CIO。就是这位 CIO 把我推进了信息安全的大门。

CIO 到位之后，做了一系列调整，选中我做信息安全。那时是 2002 年的 8 月份，对信息安全，公司是一穷二白，我也是一穷二白。CIO 说，“ 没事，你能行的 ”。就仗着 CIO 的这句话和 “ 车到山前必有路 ” 的座右铭，我扛起了信息安全的大旗。跨进信息安全大门，第一件事就是找漏洞补漏洞，第二件事就是学习信息安全方面的道道。就在这个时候，我认识了 BS7799 ，ISO13335，ISO15408 等标准。我觉得 BS7799 对工作最有指导意义，在她身上花的时间最多。从 1999 版、2000 版、2002 版到 2005 版，都有学习过，看着 BS7799 成长为 ISO2700X 标准。总结起来，我对 BS7799 的认识分为三个阶段。第一个为 “ 天书 ” 阶段，看不懂。当时网上流传一个 1999 版的中文版，翻译的质量不敢恭维，只得啃英文。第二个阶段为 “ 废话 ” 阶段，看完以后，觉得都是一堆废物，就像领导做的指示，没有具体操作的办法。第三个阶段为 “ 宝物 ” 阶段，经过不断摸索实践之后，从心底里由衷地感到 BS7799 是一件宝物。她就像一位智者在指引着我如何做信息安全。从那时起，我就有一个愿望：翻译 BS7799，以一个实践者的视角揣测每条标准背后的意图，让信息安全的来者们走得更轻快。可惜，由于工作太忙，没有付诸实践。一晃就是好几年。2006 年 4 月底，我离开工作了近 7 年的第一家公司；出来给自己打工，专做信息安全咨询和培训方面的工作。经过一年多为客户咨询和培训的经历，那个愿望又在心底的某个角落跳了出来，变得越来越大，不停地催促着我。从 2002 年到现在，参照 BS7799/ISO2700X 标准做信息安全的公司越来越多，通过认证的数量呈指数式增长。但是对 ISO2700X 标准的认识是不是到位，还有待探讨。因此，在 2007 年即将结束的几天里，我下定决心：“ 剖析 ISO27001 ”、“ 剖析 ISO27002 ”；把此作为一家之言，抛砖引玉。

译者　2007.12.30

# 0 介绍

## 0.1 概述

本国际标准提供一个为建立、实施、运行、监控、评审、维护和改进信息安全管理体系（ISMS）的模型。采用ISMS应该是组织的战略性决策。组织的ISMS设计和实施会受到组织的要求、目标、安全需求、采用的方法、组织规模和组织结构的影响。上述因素及其支持原由会随着时间发生改变。因此，实施ISMS应根据组织的需要进行调整。例如，简单的环境只需要一个简单的ISMS解决方案。

内外部相关方可将本标准用于评估ISMS的符合性。

## 0.2 过程方法

本国际标准采用“过程方法”指导组织建立、实施、运行、监控、评审、维护和改进ISMS。

组织为了有效运行，需要明确和管理众多活动。任何利用资源并经过处理把输入转化为输出的活动都可视作一个过程。通常，一个过程的输出直接构成下一个过程的输入。

组织系统化地应用各个过程，连同这些过程的识别、相互作用及过程的处理，可称之为“过程方法”。

本国际标准为ISMS阐述的过程方法在应用时要关注以下几个方面的重要性：
a) 深刻了解组织的信息安全要求，以及建立信息安全策略和信息安全目标的需求；
b) 实施和运行控制措施以管理组织的信息安全风险，要在整体业务风险框架下进行；
c) 监控和评审ISMS的效果和有效性；
d) 基于客观测量进行持续改进。

本国际标准采用“策划-实施-检查-改进”（PDCA）模型。该模型适用于ISMS的所有过程。图1描述了ISMS如何输入相关方的信息安全要求和期望，经过必要的活动和过程，产生满足这些需求和期望的信息安全输出。图1也展示了第4、5、6、7和8章中阐述的过程之间的联系。

采用PDCA模型也反映了OECD指南—《信息系统和网络的安全指南》（2002）中的准则。本国际标准在风险评估、安全设计和实施、安全管理和再评估方面，为实施这些指南中的准则提供了一个健壮模型。

举例1（安全要求的例子）：
出现信息安全问题不会给组织带来严重经济损失或干扰。

举例2（安全期望的例子）：
如果发生严重的安全事故（例如组织的电子商务网站被黑客攻击），会有经过充分培训的人员按照适当的程序使影响最小化。

图1 – 应用于ISMS过程的PDCA模型

策划（Plan，建立ISMS）
根据组织风险管控和提高信息安全的整体策略和目标，建立安全策略、目标、对象、过程和程序。

实施（Do，实施&运行ISMS）
实施和运行安全策略、控制、过程和程序。

检查（Check，检查&评审ISMS）
根据安全策略、目标和实践经验评估和测量（可适用时）ISMS的效果，并向管理层报告结果，进行评审。

改进（Act，维护&改进ISMS）
根据管理评审的结果，采取纠正和预防措施，以实现ISMS 的持续改进。

### 0.3 与其他管理体系的兼容性

本国际标准与ISO 9001:2000和ISO 14001:2004相一致，以支持与相关管理标准的相兼容、以及整合的实施和运行。表C.1描述了本国际标准与ISO 9001:2000和ISO 14001:2004之间章节的对应关系 。

本国际标准的设计使组织能将ISMS集成到相关管理体系中或与相关管理体系相兼容。

**信息技术-安全技术-信息安全管理体系-要求**

注意 — 本文献不保证包括所有需要的条款。用户自己为应用本文献的正确性负责。符合本国际标准并不能说明符合了法律的要求。

# 1 范围

### 1.1 总则

本国际标准覆盖所有类型的组织（如商业企业、政府机构和非盈利组织）。本国际标准为组织根据整体业务风险建立、实施、运行、监控、评审、维护和改进文件化的信息安全管理体系规定了要求；为组织依据自身全部或部分要求实施适合自己的安全控制规定了要求。

ISMS要设计成能够采取充分、适当的安全控制保护信息资产，并让相关方充满信心。

注1：本国际标准中提及的“ 业务 ”是广义的，泛指涉及组织生存的所有活动。

注2：ISO/IEC 17799 为设计控制提供了实施指南。

### 1.2 应用

本国际标准规定的所有要求都是通用的，旨在适用于各种类型、各种规模、各种性质的组织。组织如果对第4、5、6、7 和8 条款的内容进行了删减，就不得宣称符合本国际标准。

任何控制的删减必须满足风险可接受标准，并且要有相关责任人接受相应风险的证据。另外，任何控制的删减不得对组织满足风险评估和法律法规提出的安全要求造成影响，否则不得宣称符合本国际标准。

注：组织如果已经存在一个有效运转的业务管理体系（例如ISO 90001 或ISO 14001），将能在现有管理体系的范围内更好地满足本国际标准的要求。

# 2 参考标准

下列是应用本国际标准必须参考使用的文件。对于标注日期的，使用日期对应的版本；对于未标准日期的，使用最新

的版本（包括所有的修订）。

ISO/IEC 17799：2005 *信息技术－安全技术－信息安全管理实施规范*

# 3 术语及定义

本国际标准采用以下术语及定义

### 3.1 资产

任何对组织有价值的事物。
[ISO/IEC 13335-1:2004]

### 3.2 可用性

获得授权的实体可以访问和使用的特性。
[ISO/IEC 13335-1:2004]

### 3.3 保密性

信息不被未授权的个人、实体和过程获取，或者不泄漏给未授权的个人、实体和过程的特性。
[ISO/IEC 13335-1:2004]

### 3.4 信息安全

保护信息的保密性、完整性和可用性，另外也可以包括其他特性，例如真实性、可审查性、抗抵赖性、可靠性。
[ISO/IEC 17799:2005]

### 3.5 信息安全情况（Event）

识别出从系统、服务或网络状况中表明可能违反信息安全策略、防护措施失效、或以前未知的与安全相关的情况。
[ISO/IEC TR 18044:2004]

*笔者笔记：“Event ”在这里指的是情况而非事件，属于事件之前的状态*

### 3.6 信息安全事件（Incident）

出现单个或一系列非期望或非预期的信息安全情况（Event），很可能危及业务运营和威胁信息安全。
[ISO/IEC TR 18044:2004]

### 3.7 信息安全管理体系（ISMS）

属于整体管理体系的一部分，根据整体业务风险建立、实施、运行、监控、评审、维护和改进信息安全。
注：本管理体系包括组织结构、策略、计划活动、职责、惯例、程序、过程和资源。

### 3.8 完整性

保护资产的准确和完全的特性
[ISO/IEC 13335-1:2004]

### 3.9 残余风险

实施风险处置后残留的风险。

[ISO/IEC Guide 73:2002]

### 3.10 风险接受

接受风险的决策。
[ISO/IEC Guide 73:2002]

### 3.11 风险分析

系统地使用信息以识别来源和估计风险。
[ISO/IEC Guide 73:2002]

### 3.12 风险评估

风险分析和风险评价的全过程
[ISO/IEC Guide 73:2002]

### 3.13 风险评价

将估计的风险与既定的风险准则进行比较以确定风险重要程度的过程。
[ISO/IEC Guide 73:2002]

### 3.14 风险管理

指导和控制组织应对风险的一系列相互配合的活动。
[ISO/IEC Guide 73:2002]

*笔者笔记：*风险管理一般包括风险评估、风险处置、风险接受和风险沟通。

### 3.15 风险处置

选择和实施措施以改变风险的过程。
[ISO/IEC Guide 73:2002]
注：本国际标准中的术语“ 控制 ”等同于“ 措施 ”。

### 3.16 适用性声明

与组织ISMS 相关并适用于组织ISMS 的控制目标和控制措施的文件化的声明。
注 :控制目标和控制是基于风险评估和风险处置过程的结果和结论、法律法规要求、合同责任和组织对信息安全的业务要求。

# 4 信息安全管理体系

### 4.1 总体要求

组织必须根据整体业务活动和面临的风险，建立、实施、运行、监控、评审、维护和改进文件化的信息安全管理体系。本国际标准采用图1所示的PDCA模型。

### 4.2 建立并管理ISMS

#### 4.2.1 建立ISMS

组织必须做下列事项：

a) 根据业务、组织结构、地理位置、资产和技术，用其特征术语定义ISMS的范围和边界，以及排除在外 的详细说明及其理由。

b) 根据业务、组织结构、地理位置、资产和技术，用其特征术语定义ISMS策略：
1) 包括设定信息安全目标的框架，和建立信息安全活动的总体方向和原则；
2) 考虑业务和法律法规的要求，以及合同的安全责任；
3) 在组织整体风险管理的框架之下，建立和维护ISMS；
4) 建立风险评价的准则[见4.2.1c]；
5) 要得到管理层的批准。
注：本文件将ISMS策略作为信息安全策略的一个扩展集。这些策略可以在同一个文件中描述。

c) 定义组织的风险评估方法：
1) 确定适用于ISMS、已识别的业务信息安全要求和法律法规要求的风险评估方法；
2) 开发风险接受的准则，并确定风险的可接受水平[见5.1f]。

选取的风险评估方法必须确保风险评估产生可比较的、可重复的结果。

注：风险评估存在多种不同的方法。例如，ISO/IEC TR13335-3《信息技术－IT安全管理指南－IT安全管理技术》中论述的风险评估方法。

d) 识别风险：
1) 识别ISMS范围内的资产及其所有者（备注1）；
2) 识别资产面临的威胁；
3) 识别可能被威胁利用的弱点；
4) 识别资产的保密性、完整性和可用性受到损失的影响。

备注1：术语“ 所有者 ”是指被授予资产管理职责（资产的产生、发展、维护、使用和安全）的个人或实体。“ 所有者 ”并不是意味着拥有这个资产的财产所有权。

e) 分析并评价风险：
1) 考虑资产的保密性、完整性或可用性受到损失的后果，评价安全失效可能会对组织造成的业务影响；
2) 根据资产的主要威胁、弱点、有关的影响以及已经实施的安全控制，评估安全失效发生的可能性；
3) 估计风险的级别；
4) 根据4.2.1 c）中建立的风险接受准则，判断风险是否可以接受或需要处置。

f) 识别和评价风险处置的选择。可行的选择包括：
1) 应用适当的控制；
2) 在确切满足组织策略和风险接受准则的前提下，有意识地、客观地接受风险[见4.2.1 c] ；
3) 规避风险；
4) 将相关业务风险转嫁给其他方，如保险公司、供应商。

g) 选择风险处置的控制目标和控制。
应选择并实施控制目标和控制，以满足风险评估和风险处置过程所识别的要求。控制目标和控制的选择，应考虑风险接受准则（见4.2.1 C)2)）以及法律法规和合同要求。

从附录A中选择合适的控制目标和控制，应作为这一过程的一部分，并满足识别出来的要求。

注：附录A包含了与组织相关的一系列广泛通用的控制目标和控制。本国际标准的附录A为选择控制提供了一个起点，以避免遗漏重要的控制。

h) 获得管理层对残留风险建议的批准；
i) 获得管理层对实施和运行ISMS的授权；

j) 准备适用性声明
应准备适用性声明，该声明应包括以下内容：
1) 4.2.1 g)中选择的控制目标和控制，以及选择的原因；
2) 目前实施的控制目标和控制（见4.2.2 e) 2)）
3) 附录A中被删减的控制目标和控制，及删减的理由。

注：适用性声明提供了一个风险处置决策的总结。通过判断删减的合理性，再次确认没有控制目标被无意遗漏。

### 4.2.2 实施和运行ISMS

组织必须做下列事项：

a) 制定风险处置计划，为管理信息安全风险安排合适的管理措施、资源、职责和优先级（见5）；
b) 实施风险处置计划以达到确定的控制目标，包括资金的投入以及角色和职责的分配；
c) 实施 4.2.1 g）中选择的控制以达到控制目标；
d) 确定如何测量所选择的控制或一组控制的有效性，并详细说明这些测量措施如何评估控制的有效性以得出可比较的、可重复的结果；

注：测量控制的有效性可以让管理者和相关人员确定这些控制对原计划控制目标的实现程度。

e) 实施培训和意识计划（见5.2.2）；
f) 管理ISMS的运行；
g) 管理ISMS资源（见5.2）；
h) 实施能够及时检测安全情况（event）和响应安全事件的程序和其它控制（见4.2.3）。

### 4.2.3 监视和评审ISMS

组织必须做下列事项：
a) 执行监控、评审程序和其它控制：
   1) 及时检测过程结果中的错误；
   2) 及时识别失败、成功的安全违规和安全事件；
   3) 使管理层能确定，为安全活动委派的人员或实施的信息技术是否实现了预期；
   4) 通过使用指标，帮助检测安全情况（event），进而预防安全事件；
   5) 确定所采取的措施是否有效解决安全违规。

b) 定期评审ISMS的有效性（包括安全策略和目标的实现情况，安全控制的评审），综合考虑安全审核、安全事件、控制的有效性测量结果以及所有相关方的建议和反馈；
c) 测量控制的有效性，以证实安全要求是否得到满足；
d) 考虑以下方面的变化，按计划的时间间隔，复审风险评估并评审残余风险和已确定的风险可接受水平：
   1) 组织；
   2) 技术；
   3) 业务目标和过程；
   4) 已识别的威胁；
   5) 已实施控制措施的有效性；
   6) 外部事件，如法律法规、合同要求和社会风气的变化。
e) 按计划的时间间隔进行ISMS内部审核（见6）；
   注：内部审核，有时也称为第一方审核，是为了组织内部的目的，由组织自己或以组织的名义进行的审核。
f) 定期进行ISMS管理评审，确保ISMS范围是足够的，确保ISMS过程的改进机会得到识别（见7.1）；
g) 根据监控和评审活动的发现，更新安全计划；
h) 记录可能影响ISMS有效性或表现的动作和事件（见4.3.3）。

### 4.2.4 保持和改进ISMS

组织必须定期做下列事项：
a) 实施ISMS已识别的改进；
b) 按照8.2和8.3的要求采取适当的纠正和预防措施。总结从其它组织或组织自身的安全经验得到的教训；
c) 与所有相关方沟通措施和改进。沟通的详细程度应与环境相适宜，必要是，应约定如何进行；
d) 确保改进活动达到了预期的目的。

## 4.3 文件资料要求

### 4.3.1 总则

文件资料必须包括管理决策的记录，以确保所有措施可回溯到管理决策和策略，并且要确保记载的结果应该是可重复的。

重要的是，文件资料要能够证明选择的控制能够回溯到风险评估和风险处置过程的结果，最终回溯到ISMS 策略和目标。

ISMS文件资料必须包括：
a) ISMS 策略（见4.2.1 b)）和目标；
b) ISMS 的范围（见4.2.1 a)）；
c) ISMS 的支持性程序和控制；
d) 风险评估方法的描述（见4.2.1 c)）；
e) 风险评估报告（见4.2.1 c)到4.2.1 g)）；
f) 风险处置计划（见4.2.2 b)）；
g) 组织为确保信息安全过程被有效的策划、运行和控制而文件化的程序（注1），以及描述如何测量控制措施有效性而文件化的程序（见4.2.3 c)）；
h) 本国际标准所要求的记录（见4.3.3)。
i) 适用性声明。

ISMS策略要求的所有文件必须是可用的。

注1：本国际标准出现的术语“ 文件化的程序 ”，是指建立该程序，并形成文件、进行实施和维护。

注2：不同组织的ISMS文件的数量、详略程度不同，取决于：
——组织的规模和组织活动的类型；
——安全要求的范围和复杂度，以及被管理系统的范围和复杂度。

注3：文件和记录可以采取任何形式、任何媒体。

### 4.3.2 文件的控制

ISMS所要求的文件必须予以保护和控制。必须制定文件化的程序，规定以下方面所需的管理措施：
a) 在发布之前，文件要得到批准；
b) 必要时，对文件进行评审、更新并再次批准；
c) 确保文件的变更和目前的修订状态保持一致；
d) 确保在使用时可以获得所需版本的文件；
e) 确保文件保持清晰易读、容易辨认；
f) 确保文件能被需要者获取，并按照文件分级级别对应的程序进行传递、存储、至最终销毁；
g) 确保外来文件得到识别；
h) 确保文件的分发是受控的；
i) 防止作废文件被无意使用；
j) 若因某种原因而保留作废文件时，要对这些文件进行适当的标识。

### 4.3.3 记录的控制

必须建立并保持记录，以提供要求得到符合和表明ISMS有效运行的证据。记录必须得到保护和控制。ISMS必须考虑相关法律法规要求和合同责任。记录应保持清晰易读、容易辨认和检索。必须形成文件化的程序并进行实施，对记录的标识、储存、保护、检索、保存期限和处置进行控制。

必须对4.2所列过程的执行进行记录，对ISMS相关的安全事件进行记录。

举例（记录的例子）：
访问者登记表、审核记录和填写完的访问授权表。

# 5 管理层职责

## 5.1 管理层承诺

管理层应通过以下行动证实其建立、实施、运行、监控、评审、维护和改进ISMS的承诺：
a) 建立ISMS策略；
b) 确保ISMS目标和计划得到建立；
c) 为信息安全设立角色和职责；
d) 向组织传达实现信息安全目标和符合信息安全策略的重要性、法律的责任以及持续改进的需要；
e) 为建立、实施、运行、监控、评审、维护和改进ISMS,提供充足的资源（见5.2.1）；
f) 确定接受风险的准则和风险可接受水平；
g) 确保ISMS内部审核得到实施（见6）
h) 实施ISMS管理评审（见7）。

## 5.2 资源管理

### 5.2.1 资源提供

组织必须确定并提供以下方面所需的资源：
a) 建立、实施、运行、监控、评审、维护和改进ISMS；
b) 确保业务要求得到信息安全程序的支持；
c) 识别并指出法律法规的要求和合同的安全责任；
d) 通过正确应用所采取的控制来保持足够的安全；
e) 需要时，进行评审并对评审的结果采取适当行动；
f) 如果需要，改进ISMS的有效性。

### 5.2.2 培训、意识和能力

组织必须确保在ISMS中担当职责的人员有能力执行分配的任务，可以通过以下措施做到：
a) 确定从事影响ISMS工作的人员需要具备的能力；
b) 提供培训或采取其他措施（如雇佣能胜任的人员）来满足上述能力要求；
c) 对人员行动的有效性进行评价；
d) 维护教育、培训、技能、经验和资质的记录（见4.3.3）。

组织也必须确保所有相关人员认识到，他们的信息安全活动的相关性和重要性，以及如何为实现ISMS目标作出自己的贡献。

# 6 ISMS 内部审核

组织必须按计划的时间间隔进行ISMS内部审核，以确定ISMS的控制目标、控制措施、过程和程序是否：
a) 符合本国际标准及相关法律法规的要求；
b) 符合已识别的信息安全要求；
c) 得到有效地实施和维护；
d) 符合期望。

必须对审核方案进行策划，综合考虑受审核过程和区域的状况和重要性，以及上次审核的结果。必须对审核准则、范围、频次和方法进行规定。审核员的选择和审核的实施必须保证审核过程的客观性和公正性。审核员不能审核自己的工作。

必须形成文件化的程序，对策划和实施审核、报告结果以及保持记录（见4.3.3）的职责和要求进行规定。

受审核区域的负责人必须立即采取措施以消除发现的不符合项及其原因。后续活动应包括对所采取的措施进行验证并报告验证结果（见8）。

注：ISO19011:2002《质量/环境管理体系审核指南》，可以为ISMS内部审核提供指导。

# 7 ISMS管理评审

## 7.1 总则

管理层必须按计划的时间间隔（至少一年一次）评审ISMS，以确保其持续的合适性、充分性和有效性。评审必须包括评估ISMS的改进机会和变更需要，包括信息安全策略和信息安全目标。评审结果必须清楚地记入文件，并维护好。（见4.3.3）。

## 7.2 评审输入

管理评审的输入必须包括：
a) ISMS审核和评审的结果；
b) 相关方的反馈；
c) 在组织中可以用来改善ISMS绩效和有效性的技术、产品或程序；
d) 预防和纠正措施的实施情况；
e) 上次风险评估未充分指出的弱点或威胁；
f) 有效性测量的结果；
g) 对上次管理评审后所采取措施进行验证的结果；
h) 任何可能影响ISMS的变化；
i) 改进建议。

## 7.3 评审输出

管理评审的输出必须包括与以下方面有关的任何决定和措施：
a) ISMS有效性的改进；
b) 更新风险评估和风险处置计划；
c) 必要时，针对以下方面的变化和可能影响ISMS的内外部事件，修订促进信息安全的程序和控制：
   1) 业务要求；
   2) 安全要求；
   3) 实现现有业务要求的业务过程；
   4) 法律法规；
   5) 合同责任；
   6) 风险接受准则/风险接受水平。
d) 资源需求；
e) 改进测量控制措施有效性的方法。

# 8 ISMS 改进

## 8.1 持续改进

组织必须通过应用信息安全策略、信息安全目标、审核结果、监视事件的分析、纠正预防措施和管理评审（见7）持续改进ISMS的有效性。

## 8.2 纠正措施

组织必须采取措施消除不符合ISMS要求的原因，以防重复发生。为纠正措施形成的文件化的程序必须规定以下方面的

要求：

a) 识别不符合项；
b) 确定不符合的原因；
c) 对采取措施（确保不符合不再发生）的必要性进行评价；
d) 确定和实施所需的纠正措施；
e) 对采取纠正措施的结果进行记录（见4.3.3）；
f) 对采取的纠正措施进行评审。

### 8.3 预防措施

组织必须确定措施消除潜在不符合ISMS要求的原因，以防止发生。预防措施必须与潜在问题的影响相适宜。为预防措施形成的文件化的程序必须规定以下方面的要求：

a) 识别潜在的不符合项及其原因；
b) 对采取措施（确保不符合不发生）的必要性进行评价；
c) 确定并实施所需的预防措施；
d) 对采取预防措施的结果进行记录（见4.3.3）；
e) 对采取的预防措施进行评审。

组织必须识别风险的变化，并通过关注变化显著的风险识别需要的预防措施。必须根据风险评估的结果来确定预防措施的优先级。

注：预防不符合的措施通常比纠正措施有更好的成本效益比（更划算）。

## 附录A（规范） 控制目标和控制

表A.1 中所列出的控制目标与控制直接引用于BS ISO/IEC 17799:2005 第5 到15 章。表A.1中列出的控制目标与控制并不详尽，如果需要，组织可考虑增加另外的控制目标与控制。必须把选择此表中的控制目标和控制作为4.2.1 规定的ISMS 过程的一部分。

ISO/IEC 17799:2005 第5 到15 章为支持A.5 到A.15 规定的控制，提供了（最佳实践）实施建议和指南。