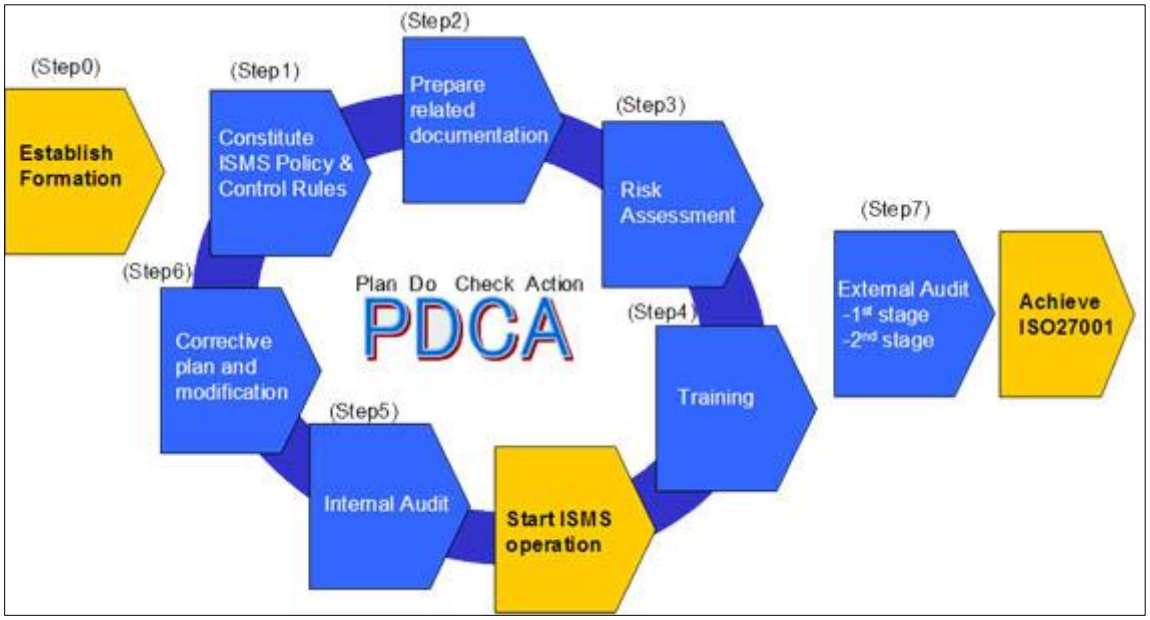
信息安全管理体系

随身小册子

Pocket Book of

Information Security Management Systems



最佳实践

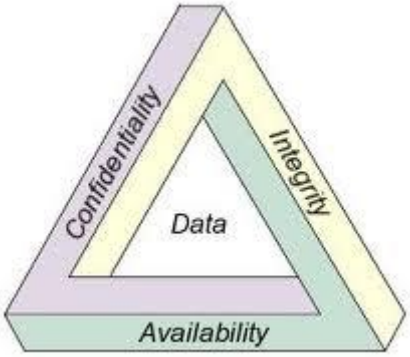
Best Practice

信息安全视频点播中心 | Information Security Video On demand Center
HTTP://ISVOC.COM

目 录

目录

ISO 27001定义信息安全



毋庸置疑，信息是信息时代的货币。在通常情况下，信息是一个组织拥有的最宝贵的资产，即使该信息没有受到正式和全面的估价。
IT 治理是董事会和管理团队用来引导和控制企业各种结构、标准和流程，旨在有效地管理，保护和利用其组织的信息资产。
信息安全管理是 IT 治理的一个子集，它的重点是保护一个组织的信息资产安全。

信息资产面临的风险

资产在 ISO 27001中的定义为“对组织具有价值的任何东西”。信息资产面临着各种各样的威胁，这些威胁包括来自外部的和内部的，威胁的范围包含有随机产生的和非常 具体的。风险包括自然灾害，欺诈和其他犯罪活动，也包括用户错误和系统故障。信息风险可以影响信息资产的一个或多个信息安全基本三要素或信息安全三属性， 它们是：可用性、机密性和完整性。

ISO 27001中将这些三要素或者三个属性定义为：
1.可用性(AVAILABILITY)- ‘经授权的实体在正常需求下可以访问和使用的属性’，信息允许由人类用户访问，以及软件程序访问；
2.保密性(CONFIDENTIALITY)- ‘信息不提供或披露给未经授权的个人、实体或程序的属性‘；
3.完整性(INTEGRITY)- ‘维护资产的准确性和完整性的属性’。

信息安全

ISO 27001将信息安全定义为“对信息的机密性，完整性和可用性的保持”。此外，如真实性（防伪确认），可跟踪性，不可抵赖性和可靠性等属性也可以参与进来。

信息安全管理体系

ISO 27001定义了 ISMS，即 Information Security Management System，亦即信息安全管理体系，是整个管理系统的一部分，以业务风险方法为基础，其目的是建立、实施、运行、监督、评审、保持和改进信息安全。该管 理体系包括“组织的结构、方针政策、规划活动、职责、实践（惯例）、程序、过程和资源。ISMS 的存在是为了维持机密性，完整性和可用性。如图所 示，ISMS 确保组织的信息和信息资产的机密性，完整性和可用性，最关键的信息资产在所有三个属性都是重要的。

ISO27001信息安全标准背景

信息安全标准，BS7799最初是在1999年4月份作为两个部分进行发布。

第一部分，《信息安全管理实施细则》，Code Of Practice for Information Security Management，它提供了一套综合的、由信息安全最佳惯例组成的实施规则，其目的是作为确定各类信息系统通用控制范围的唯一参考基准，并且适用于 大、中、小组织。

第二部分，《信息安全管理体系规范》，Specification for Information Security Management Systems.，它规定信息安全管理体系要求与信息安全控制要求，它是一个组织的全面或部分信息安全管理体系评估的基础，它可以作为一个正式认证方案的 根据。

两部分标准的关联是第二部分的附件 A 中列出了所有的信息安全控制措施，以供组织考虑和加以选择。这些控管措施和标准的第一部分中的控管措施是一致的，并且第二部分要求用户到第一部分中寻找详细的关于实施和部署的指导意见。

由于 BS7799第一部分开始被其它国家的标准化组织吸收和采用，并发布类似的标准。所以2000年12月，BS7799-1：1999《信息安全 管理实施细则》通过了国际标准化组织 ISO/IEC 的认可，正式成为国际标准——ISO/IEC17799：2000《信息技术—信息安全管理实施细 则》。

2002年，BSI 对 BS7799-2：2000《信息安全管理体系规范》进行了改版，发布了 BS7799-2：2002《信息安全管理体系规范》。这次的重大修订包括：
统一了标准两个部分章节的排序；
引入并应用 PDCA 过程模式到标准中；
添加了 ISMS 的持续改进；
改进标准及附属章节，以便与其他管理标准协调一致，这些标准如 ISO9001：2000以及 ISO14001：1996

2005年6月，ISO 组织对 ISO/IEC 17799进行了改版，新版标准为 ISO/IEC 17799：2005《信息技术—安全技术—信息安全管理实施细则》。不少发达的国家如捷克、丹麦、荷兰、芬兰、法国、德国、冰岛、日本、韩国、挪威、葡 萄牙和瑞典等等对这一标准进行了本地语言的翻译，中国也对此做了翻译。

2005年10月，BS7799-2：2002通过了国际标准化组织 ISO 的认可，正式成为国际标准 ISO/IEC 27001：2005《信息技术—安全技术—信息安全管理体系—要求》。

ISO27001用于为建立、实施、运行、监视、评审、保持和改进信息安全管理体系提供模型。（Information Security Management System，简称 ISMS）采用 ISMS 应当是一个组织的一项战略性决策。一个组织的 ISMS 的设计和实施受业务需求和目标、安全需求、所采用的过程以 及组织的规模和结构的影响。上述因素及其支持过程会不断发生变化。期望信息安全管理体系可以根据组织的需求而测量，例如简单的情形可采用简单的 ISMS 解 决方案。

ISO27001标准可以作为评估组织满足顾客、组织本身及法律法规的信息安全要求的能力的依据，无论是组织自我评估还是评估供方能力，都可以采用，也可以用作独立第三方认证的依据。

2007年4月 ISO /IEC 17799：2005标准直接更改标准编号为 ISO/IEC 27002。

ISO 27000系列标准介绍

ISO 已为信息安全管理体系标准预留了 ISO/IEC 27000系列编号，类似于质量管理体系的 ISO 9000系列和环境管理体系的 ISO 14000系列标准。
规划的 ISO 27000系列包含下列标准:

ISO 27000——《信息安全管理体系原理和术语》
《Information security management system fundamentals and vocabulary》
该标准主要用于阐述 ISMS 的基本原理和术语，预计2008年发布。

ISO/IEC 27001:2005
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
该标准源于 BS7799-2，主要提出 ISMS 的基本要求，已于2005年10月正式发布。
标准介绍：
ISO27001用于为建立、实施、运行、监视、评审、保持和改进信息安全管理体系（Information Security Management System，简称 ISMS）提供模型。采用 ISMS 应当是一个组织的一项战略性决策。一个组织的 ISMS 的设计和实施受业务需求和目标、安全需求、所采 用的过程以及组织的规模和结构的影响。上述因素及其支持过程会不断发生变化。期望信息安全管理体系可以根据组织的需求而测量，例如简单的情形可采用简单的 ISMS 解决方案。
ISO27001标准可以作为评估组织满足顾客、组织本身及法律法规的信息安全要求的能力的依据，无论是组织自我评估还是评估供方能力，都可以采用，也可以用作独立第三方认证的依据。

ISO/IEC 27002:2005
Information technology — Security techniques — Code of practice for information security management
信息技术—安全技术—信息安全管理实用规则
该标准取代了 ISO /IEC 17799：2005，直接由 ISO/IEC 17799：2005更改标准编号为 ISO/IEC 27002，已于2007年4月实施。
标准介绍：
本标准为在组织内启动、实施、保持和改进信息安全管理提供指南和通用的原则。本标准概述的目标提供了有关信息安全管理通常公认的目标的通用指南。

本标准的控制目标和控制措施预期被实施以满足由风险评估所识别的要求。本标准可以作为一个实践指南服务于开发组织的安全标准和有效的安全管理实践，帮助构建组织间活动的信心。
本标准包含的实施规则可以认为是开发组织具体指南的起点。本实施规则中的控制和指导并不全都是适用的。而且，可能需要本标准中未包括的附加控制和指南。当 开发包括附加控制和指南的文件时，包括对本标准适用的条款进行交叉引用可能是有用的，该交叉引用便于审核员和商业伙伴进行符合性核查。

ISO/IEC 27003:2010
Information technology — Security techniques — Information security management system implementation guidance
信息技术—安全技术—信息安全管理体系实施指南
该标准已于2010年2月正式发布。
该标准为按照 ISO/IEC 27001建立信息安全管理体系（ISMS）实施计划提供应用指南。通常将 ISMS 作为一个项目实施。

ISO/IEC 27004:2009
Information technology — Security techniques — Information security management — Measurements
信息技术—安全技术—信息安全管理—测量
该标准已于2009年12月正式发布。
该标准旨在帮助组织测量、报告和系统性的改进其信息安全管理体系的有效性。
该标准为制订测量项和实施测量提供指南，以评估信息安全管理体系和 ISO/IEC 27001规定的控制措施的实施效果。

ISO/IEC 27005:2008
Information technology — Security techniques –Information security risk management
信息技术—安全技术—信息安全风险管理
该标准以 BS7799-3和 ISO13335为基础，已于2008年6月正式发布。
本标准描述了信息安全风险管理的要求，可以用于风险评估，识别安全要求，支撑信息安全管理体系的建立和维持。

ISO/IEC 27006:2007
Information technology — Security techniques — Requirements for bodies providing audit and certification of information security management systems
信息技术—安全技术—信息安全管理体系审核认证机构要求
该标准已于2007年2月正式发布。
该标准对提供 ISMS 认证的机构提出要求，所有提供 ISMS 认证服务的机构需要按照该标准的要求证明其能力和可靠性。

ISO/IEC 27007和 ISO/IEC 27008
这两个审核指南标准目前正在开发之中。这两个标准的制定工作正在与开展 ISO 19011最新修订和制定 ISO 17021-2的有关人士合作。ISO/IEC 27007是专门为 ISMS 的范围和复杂程度、风险管理、控制方法的选择和 ISMS 审核员的能力等方面提供审核指南的标准。另一方面，ISO/IEC 27008对 ISO/IEC 27001附录 A 中规定的安全控制提出了技术要求。这两个标准预计将在2011年出版。

行业标准
人们正在制定一系列 ISO/IEC 27001行业应用新标准。当然，这些标准将不会取代 ISO/IEC 27001，但他们引入了行业附加的特殊要求。目前的工作方案包括：

ISO/IEC 27010 – 用于行业间的沟通

这个标准主要涉及那些国家基础设施的行业和组织的各类安全要求。这包括指令安全及控制应用措施，如监督控制和数据采集。

ISO/IEC 27011 – 适用于电信组织
该标准基于 ISO/IEC 27002，这个标准已于2008年出版，电信标准号为 X.1051。

ISO/IEC 27013 – 将 ISO/IEC 20000 –1和 ISO/IEC 27001整合
该标准为那些希望将服务管理和信息安全管理体系的共性整合成为一体的机构提供指南。如：他们可将文件化体系、事故处理体系和安全服务提供、监督和审查程序整合起来。

ISO/IEC 27014 – 信息安全管理框架
该标准支持公司管理框架的信息安全。ISO/IEC 27001是一个理想的信息安全框架，因为它包含三个关键管理要素，即：风险管理，控制体系和审核职能。

ISO/IEC 27015 – 金融和保险服务业
该标准是 ISO/IEC 27001标准在金融和保险业的特殊运用。

已经发布：
ISO/IEC 27000——信息安全管理体系原理和术语
ISO/IEC 27001——信息安全管理体系要求
ISO/IEC 27002——信息安全管理实践规则
ISO/IEC 27003——信息安全管理体系实施指南
ISO/IEC 27004——信息安全管理测量与指标
ISO/IEC 27005——信息安全风险管理
ISO/IEC 27006——信息安全管理体系审核认证机构要求
ISO/IEC 27011——适用于电信组织

准备中(草案)：
ISO/IEC 27007——信息安全管理体系审核指南
ISO/IEC 27008——信息安全管理体系审核指南（控管措施）
ISO/IEC 27010——用于行业间的沟通
ISO/IEC 27013——将 ISO/IEC 20000 –1和 ISO/IEC 27001整合
ISO/IEC 27014——信息安全治理框架
ISO/IEC 27015——金融和保险服务业
ISO/IEC 27031——电信就绪之业务持续性指南
ISO/IEC 27032——互联网安全指南
ISO/IEC 27033——网络安全指南
ISO/IEC 27034——应用安全指南
ISO/IEC 27035——安全事件管理
ISO/IEC 27036——安全外包指南
ISO/IEC 27037——数字证据的鉴定，收集和保持

ISO/IEC 27001概述

该标准的标题是“信息技术—安全技术—信息安全管理体系—要求”

该标准源于 BS7799-2，主要提出 ISMS 的基本要求，已于2005年10月正式发布。

让我们看一下纸质的标准，加上首尾的零头，标准总共有44页。但是标准的核心部分只包含在其中的9页里，这9页列出了设计和部署信息安全管理体系的技术规范或要求。另外，标准有17页的内容是附录 A，它其中包含133项独立的控制措施，这些控制措施的适用性必须得到考虑。

标准快速介绍

ISO27001用于为建立、实施、运行、监视、评审、保持和改进信息安全管理体系（Information Security Management System，简称 ISMS）提供模型。采用 ISMS 应当是一个组织的一项战略性决策。一个组织的 ISMS 的设计和实施受业务需求和目标、安全需求、所采 用的过程以及组织的规模和结构的影响。上述因素及其支持过程会不断发生变化。期望信息安全管理体系可以根据组织的需求而测量，例如简单的情形可采用简单的 ISMS 解决方案。

ISO27001标准可以作为评估组织满足顾客、组织本身及法律法规的信息安全要求的能力的依据，无论是组织自我评估还是评估供方能力，都可以采用，也可以用作独立第三方认证的依据。

信息安全体系管理规范包含在 ISO 27001的第四至第八章，晚些我们会逐一进行学习和讨论。

标准的主要内容包括：

0 简介

0.1总则

0.2过程方法

0.3与其它管理体系的兼容性

1 范围

2 引用标准

3 术语和定义

4 信息安全管理体系

4.1总体要求

4.2 建立和管理 ISMS

接着讨论 ISMS 的组成部分：ISO 27001第4-8章，ISO 27001的附录 A 和 ISO 27002的关系

ISO 27001第4章列出了总体要求，它被后面的第5-8章的详细规范要求支撑。附录 A 所列的控制清单直接同 ISO 27002中的具体指导相关联，正是这些控制措施，形成了信息安全管理体系的大部分内容。

总体要求
尽管所有这些章节都很重要，发起章节才是成效性中最重要的，即章节4.2.1：建立信息安全管理体系：
章节4.2.1包含如下6个重要事项：

1.范围——ISMS 在组织中适用性的定义

2.策略——董事会的信息安全政策，其中规定了整个 ISMS 的指导方针

3.资产清单——所有类型的信息资产(包括有形的及无形的)，这些是 ISMS 工作的主题对象

4.风险评估——鉴别出每项资产涉及的风险

5.风险应对计划——识别出每项风险要如何处理，当然是在董事会关于风险应对方法的整体指导下进行

6.适用性申明——描述 ISO 27001附录 A 中哪些控制措施已经被采用，如何被采用的；哪些控制措施没有被采用，以及没有采用它们的理由。

ISO/IEC 27002概述

信息技术—安全技术—信息安全管理实用规则

该标准取代了早前的 ISO/IEC 17799及 BS 7799，它为在组织内启动、实施、保持和改进信息安全管理提供指南和通用的原则。本标准概述的目标提供了有关信息安全管理通常公认目标的通用指南。

本标准的控制目标和控制措施预期被实施以满足由风险评估所识别的要求。本标准可以作为一个实践指南服务于开发组织的安全标准和有效的安全管理实践，帮助构建组织间活动的信心。

本标准包含的实施规则可以认为是开发组织具体指南的起点。本实施规则中的控制和指导并不全都是适用的。而且，可能需要本标准中未包括的附加控制和指 南。当开发附加控制和指南的文件时，包括对本标准适用的条款进行交叉引用可能是有的，该交叉引用便于审核员和商业伙伴进行符合性核查。

标准含有16个章节，其中5至15共11个章节包含 ISO 27001附录 A 中所含的所有控制措施。这些章节包含39个安全分类，两个标准中控制措施的编号是完全相同的。章节的编号并没有排序意义，根据实际情况的需要，所有的章节都可能是很重要的。

安全分类，所有的安全类别都包含有：
1.控制目标，声明需要达成的结果
2.要达到控制目标所要部署的一个或多个控制措施

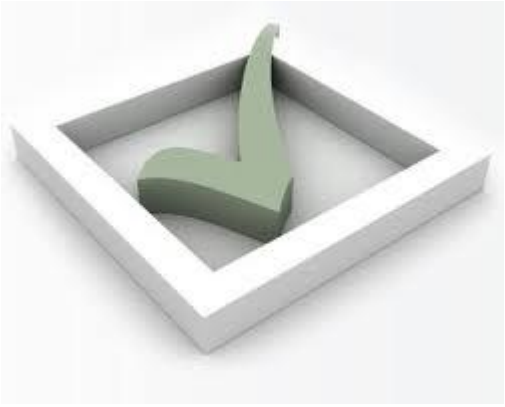
每个安全分类中的控制措施都以如下相同的方式进行排序：
1.控制申明，它描述控制的目标
2.部署指南，它是关于组织如何部署这个控制措施的详细指南
3.其它需要考虑的信息，包括对其它标准的参考

标准的16个章节目录如下：

前言

0 引言
1 范围
2 术语和定义
3 标准的结构
4 风险评估和处理
5 安全方针
6 信息安全组织
7 资产管理
8 人员安全
9 物理和环境安全
10 通信和运维管理
11 访问控制
12 信息系统的信息获取、开发以及维护
13 信息安全事故管理
14 业务持续性管理
15 符合性

ISO27001与27002的关系



ISO27001和 ISO27002之间的工作关系需要理解的非常明确，因为 ISO27001对 ISO27002有相当程度的依赖，实际上它必需要用到 ISO27002。

开发信息安全管理的国际标准 ISO 27002的原因最初在 BSI 的网站上的描述如下：
许多组织都表示需要有一个共同的关于信息安全管理最佳实践的标准，他们希望能够部署信息安全控制措施，以满足他们自己的业务需求以及与他们有业务关系的其 它机构。这些组织认为有必要分享通用最佳实践的好处，并以此作为一个真正的国际水平，以确保它们能够保护他们的业务流程和活动，以满足业务的需要。

它并没有提供一个用于获得国际认证的基本方案。认证方案只有 BS7799的第二部分和现在的 ISO 27001可以做到。

两个标准之间的对应关系

ISO27001:2005的附件 A 中列出了 ISO17799:2005也就是新编号 ISO27002中的133个控件，并且遵循相同的编号系统，和使用同样的关于控制措施的语言用词。
ISO27001的前言中指出：控制目标和控制措施直接来自 ISO17799:2005，并且和它保持一致。
ISO27001规定：应该从附件 A 中选择控制目标和控制措施，以满足“风险评估和风险处理过程中确定的控管要求”。
ISO27002还提供了有关如何实现特定的控制措施的实质性指导。任何一个 ISO27001 ISMS 的实施都将需要获取和研究 ISO27001和 ISO27002两份标准。
尽管 ISO27001强制指定 ISO27002作为一个控制措施选择和部署的指导来源，它并不限制该组织对控制措施的选择。序言接着指出：“ISO 标准中的控制目标和控制措施可能并不是很详尽，组织可能需要考虑和采取更多的控制目标和控制措施。”

ISO27001与27002的比较

ISO 27001是一个信息安全管理体系规范。它使用的词汇像“应该”和“必须”。它规定我们的需求。它是对其中第一、第二和第三方的审计进行规范的。

第一方的审计是一个组织对该组织自己的行为进行审核，即自审。第二方审计的工作由一个合作组织进行，这个合作组织通常是有一些商业关系的合作伙伴。第三方审计是由独立的第三方进行，如认证机构或外部审计师。

实施细则或一套指引，使用的字眼例如“可以”和“建议”，它允许单个的组织机构选择执行哪些标准元素，和不执行哪些。这种内在的元素可选择性意味着 ISO 27002并不适合为审计提供坚实的标准。而在这方面，ISO27001就不提供任何回旋余地。

任何实施 ISMS 的并且希望得到 ISO 27001评审的组织，将必需遵守这个标准中的规格。

作为一个通用的规则，实施了以 ISO 27001为基础的 ISMS 的组织需要密切注意该标准本身的措辞，并要密切注意它的任何修改。与官方修改的任何不符，通常发生在3年和5年的认证周期内，将会影响到现有的认证。

恰当的第一步是获取和阅读 ISO 27001的副本。副本可从 ISO 网站或国家标准机构购买。

信息安全管理体系认证机构和认证流程

ISO 27001提供了由一个认证机构对一个组织的信息安全管理体系进行独立审计和认证的规范。如果信息安全管理体系被认为符合规范要求，组织可以被发放正式的证书以确认之。

认证机构

认证是由独立的，可信的认证机构进行的。它们在不同的国家有不同的叫法，包括'注册机构'，'评估和登记机关'，'认证/注册中心'和'登记司'等等。无论他们被如何称呼，他们都在做同样的事情，并接受同样的要求。

经认可的认证机构是一个已经证明完全符合任何国际和国家标准规定的认证机构。

认证流程

对于已经通过 ISO 9000或任何其他管理体系标准认证的任何组织，该认证流程将会非常熟悉。

认证机构将分两个阶段发起审核流程。第一阶段将进行文件的审查（可能包括也可能不包括预认证的访问），这将使审计人员进行首次实际的正式访问以便能：
熟悉该组织机构；
对文件进行审查；
确保 ISMS 得到了足够的开发，已经能够接受正式的审计；
获取足够的关于该组织的信息，以及认证的目的和范围，以便有效地准备他们的审计。

这次访问是通常时间比较短，取决于组织的规模，可能只需要一两天。在作出访问之前，一些组织将开展远程文件审查。

正式审计

正式的审计，通常被称为'初审'，将花上数天时间。审计过程包括测试组织的（信息安全管理体系 ISMS）文档流程以和标准的要求进行比较，以确认该组织已制订出符合标准要求的文档体系，然后再测试组织对 ISMS 的实际遵从情况。

审计工作将遵循一个预先设定的计划。审计人员将与他们进行沟通，包括和组织中的哪些人以及用什么顺序与他们面谈。

审计报告

认证审核将使用负面报道（也就是说，它会找出不足之处，而不是光辉点），以评估 ISMS 确保该组织的程序和流程，该组织的实际活动和执行的记录符合 ISO 27001的要求，并且给出申报的系统的范围。审计的结果将是：
*书面审计报告（通常可在审计完成时交付）
*不符合项纠正措施和意见
*商定的纠正措施和时限

不符合项可以是轻微的或严重的;轻微的不符合项将被作为主要的改进机会，严重的不符合项将意味着该组织并不会（在这个阶段）成功地获得认证。通常， 当一个严重的不符合项被发现出来时，审计人员会建议，审计过程暂停，以便该组织使用足够的时间解决这个严重问题之后再重新开始。

审计输出结果

访问的预期结果应当是组织的 ISMS 通过了 ISO 27001的认证和证书的效果问题。该证书应得到适当的展示，组织应该开始准备应对它的第一次监督访问，它将在约6个月后进行。

任何轻微的不符合项应该得到解决，并由邮件告知，所有证书的发放将依赖在事前商定的时间表内的整改情况。

审计监督将在审计后进行，既要确保他们不会发展成为不符合项，也要作为该组织持续改进活动的一部分。

正式批准的认证标志可以被组织用来当做营销材料。

信息安全标准与其他管理系统的兼容性及可集成性

BS 7799第二部分在2002年第一次尝试着在信息安全管理体系标准同 ISO 9001:2000质量管理体系和 ISO 14001:1996环境管理体系之间建立和谐关系。这一步骤反映了一些组织将信息安全同其管理系统进行整合和一致性调整的尝试。

ISO 27001 附录 C 以及整合

ISO 27001 附录 C 只是参考性的，而非强制性的——并没有组织被要求来设法整合进它的管理系统。附录 C 列出了其中个别条文如何对应 ISO 9001:2000和 ISO 14001:2004中的条文。对于大多数，但不是所有的组织来讲，关键的对应关系将是 ISO 27001与 ISO 9001的。如下的 ISO 27001条文是管理系统集成的出发点：

1) 第4.3条，其中涉及文档需求
2) 第5.1条，其中涉及管理层承诺
3) 第7条，其中涉及管理审查
4) 第6条，其中涉及内部审计。

他们之间这些相同的条文，使两个管理系统可能部署共同的文件体系、管理以及审核流程。

综合管理系统

一套综合管理系统只需要：

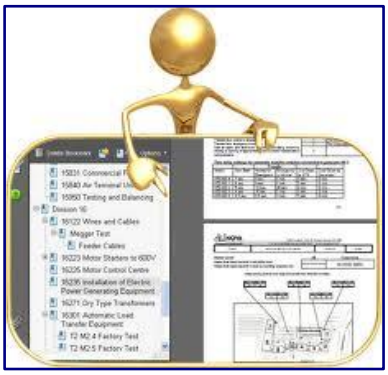
1) 一份程序手册，其中包含质量和信息安全的程序
2) 一套全面和综合的审计程序，内容包括审查过程所有方面的活动
3) 标准的管理授权、批准、监测和审查流程，它将处理所有落在这些适用范围内的活动，这些范围包括信息安全管理体系，质量管理体系或环境管理体系。

ISO 9001

已经拥有同 ISO 9001标准相兼容的系统的组织可以很简单地添加一些，就可获得 ISO27001认证认可的信息安全管理体系。条文1.2已经提到这一点：

“如果一个组织已经有一个可操作性的业务流程管理系统，在大多数情况下，它可以用来满足本国际标准在这个现有的管理体系之上的要求。”

文档要求和记录控制



设计和实施管理系统的关键原因之一是使组织能够认识自己的现状，在能力成熟度模型方面，它被称为一个“混沌”的组织。“混沌”组织没有一个固定的程 序，或流程，结果很大程度上取决于人们的表现，而人们却花了很多时间在“消防救火”上，比如不停地修复软件错误和解决突发事件。

ISO 9001:2000是一个众所周知的获得广泛实施的质量保证或业务流程管理系统。如果该组织没有和 ISO 9001认证管理体系兼容的文件控制体系，组织则应当获得 ISO 27001的4.3条中涵盖的关于文档控制和记录问题的指导手册。

文档控制要求

ISO27001明确要求管理制度要记录在案。控制 A.10.1.1明确要求的安全程序要被记录、维护、并提供给所有需要它们的用户。

其他在附件 A 中有明确的文件要求的包括：

* A.7.1.3可接受的资产使用
* A.8.1.1记录在案的人力资源安全的角色和责任
* A.11.1.1访问控制策略
* A.15.1.1鉴别适用的法律法规

许多其他的控制需要“正式”程序或者“明确”的沟通，而这些可以在技术上不被记录而实现，期望是所有的流程和程序都被记录。

ISMS 文件的内容

文件必须是完整的、全面的、符合标准的要求并且适应每个组织不同的需求。符合要求的 ISMS 将有充分的记录。ISO 27001描述了 ISMS 所需的最小的文档体系，表明该组织保持了足够的记录，用以证明其遵守规定与标准。这些文件包括：

* 信息安全政策，ISMS 的适用范围声明，风险评估，各种控制目标和适用性声明。总之，这些构成了 ISMS 的政策手册。
* 组织和它的管理层在 ISMS 的指定范围内采取的行动的证据（包括董事会会议和指导委员会会议的记录，以及其它的特别报告）。该标准规定，应记录管理层的决定，这样所有的行动都应追溯到这些决定和政策，任何已记录的结果应可以重复记录。
* 一个管理架构说明（包括指导委员会等等）。这和组织结构图可能是有相关的，非常有用。
* 风险处置计划和实施每一个指定的控制措施的基础文件程序（其中应包括责任和需要采取的行动）。一个程序描述包括，谁必须做什么，在什么条件下，或什么时候 以及如何做。这些程序将是政策手册的一部分，本身可以是纸张或电子的。标准还规定，选择的控制之间的关系，风险评估的结果和风险处理过程，以及 ISMS 的 政策和目标，都应该得到展示。
* 有关 ISMS 的管理和审查的治理流程应包括责任和必要的行动。

并不是所有组织都要实现一个同样复杂的文件结构。标准指出“由于组织的不同，ISMS 文档深度可以有所不同，这些不同包括组织规模和活动的类型；安全需求和被管理系统的范围和复杂度。

记录控制

标准关于记录控制的要求对那些已经实施 ISO 9001的人们来讲非常相似。因为4.3.3条规定，记录的保留是为了提供证据表明 ISMS 的符合标准的要求。在正常的期限中，组织也有法律法规监管所要 求的其它记录需要保存。这些记录是为了展示 ISMS 的有效性，这些记录必需得到良好控制，记录的内容要真实、准确、清晰和易于识别和检索；这就意味着，特 别是对电子记录，即使硬件和软件已经升级，对它们的访问必须得到保留。

附件 A 文件控制

附件 A 中有进一步的 ISMS 文档相关的控制要求。它们也是很重要的，这些控制包括：

* A.7.2.1分类指导原则，它处理保密分级
* A.7.2.2处理信息的标签，其中涉及不同保密级别的信息和信息媒介如何被标记
* A.15.1.3保护记录，其中涉及保存组织文件
* A.15.1.4数据保护和个人隐私信息。

文件层级

按照一般管理体系的惯例，通常是由四个层次构成的，不过也有小型组织将第二层和第三层综合一起以简化文档管理的：

第一级–安全政策手册

它是管理架构的摘要，其中包括了信息安全方针政策和控制措施目标，以及适用性声明中所提及已实施的控制措施。

第二级–各类程序文件

程序用来实施所要求的控制措施，描述由谁，做什么，在什么条件下或什么时候，以及如何做等的安全流程。

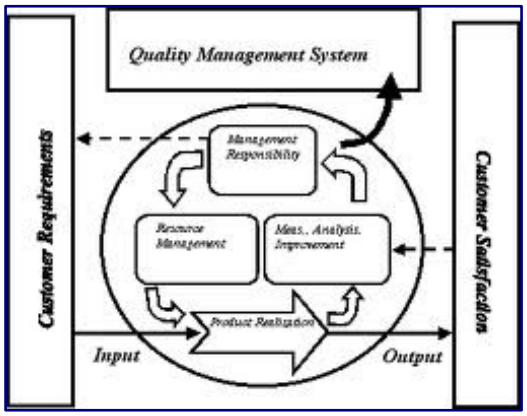
第三级–具体的作业指导书、检查清单等

解释特殊工作和活动的细节，以及如何完成特定的工作。包括详细的工作指导书、表单、流程图、服务标准和系统手册等。

第四级–记录文件

实施各项流程的执行记录成果，以符合上述1、2和3等级文件要求的客观证据。

管理责任



实施 ISO 27001认可的 ISMS 是影响整个组织的事情。范围和政策声明的清晰划分是到明确要求了的。对范围内的例外情况需要记录下辩护的理由，而政策应适用于整个组织。

该标准还明确表示，ISMS 的设计应以满足组织的需要，并应以满足并不断满足这些需要的方式进行实施和管理。

管理指导

本标准要求管理层应“必要传达给组织符合信息安全目标与遵守信息安全政策的重要性。”这些要求在 ISMS 标准的后续版本越来越得到加强，因为事实越来越清楚地表明：没有这些管理方面的支持和指导，设计并建立 ISMS 是很难的。

ISMS 的战略性质，在标准4.1章节中有明确的规定要求，它声明“组织应建立、实施、运作、监督、审查、维持和改善一个可记录的 ISMS，以应对该组织在整体商业活动环境中所面临的风险。”组织针对风险处理的总体方针设定应同本标准的风险评估策略相一致。

管理层的责任是非常重要的，第5条全专门设置了详细的规定，要求管理层“应当提供其承诺的建立、实施、运作、监督、审查、维持和改进 ISMS 的证据。”

提供管理层承诺的证据

ISO 27001认证审核员希望看到表明这一条款的要求得到了满足的证据。通常的做法是通过和首席执行官或其他对整体业务负责的执行人员进行面谈，以及审查记录 （这些记录如会议记录，议程表等，其中就包含管理层对政策进行了辩论、达成了一致协议、进行了检查和并且测定了改进目标）。至关重要的是，管理层必须决定 可接受风险的准则和水平，这是一个关键步骤，没有它的话，从整个 ISMS 的制定到部署控制所依据的风险评估过程不能得到进行。

管理相关的控制措施

附录 A 特定指出管理参与的一些控制措施。它们的详细编号如下：

* A.5.1.1 信息安全策略文档，必需得到管理层的批准
* A.6.1.1 对信息安全的管理承诺; 管理部门必须通过“指明方向，明确承诺，明确任务，以及承担信息安全责任”来积极地支持。承诺的主要表现包括：信息安全政策，建立和扩展 ISO 27001项目组，协调信息安全的活动，以及分配信息安全的责任。
* A.6.1.4 授权信息处理设施的流程；其中一定要有一个管理程序，以授权新的信息处理设施
* A.8.2.1 管理责任；这项控制规定管理层 “应要求员工，承包商和第三方用户遵守和应用组织既定的安全政策和程序。”

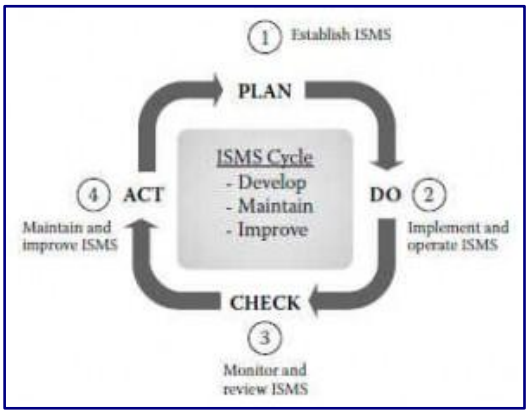
* A.10.1.3 职责分离；在考虑责任的分配时必须考虑这项重要的要求
* A.11.2.4 进行用户访问权限审查；这个控制要求管理层应当使用正式的程序定期审查用户的访问权限
* A.15.1.2 对信息安全策略和标准的遵从；这项控制明确从各个管理层级延伸管理职责，要求管理人员“确保在其责任区内的所有安全程序得到正确地执行，以实现对安全政策和标准的遵从。”

管理评审的要求

除了控制要求，标准在第7条（ISMS 的管理审查）中提到，“管理层应该在计划的时间间隔内，审查组织的 ISMS，以确保其持续活动的适宜性，充分性和有效性。”这一节清楚地界定了所需的（至少每年一次的）输入审查过程；以及包括从所有组织的监督和审查活动中得到的产出。

管理审查的输出应形成文件，并应得到贯彻执行，它应带来稳定和持续不断的 ISMS 改善。一个经过 ISO 27001认证的 ISMS 在认证有效期内将定期得到审查，这些审查将集中考察组织和它的管理层如何推动了持续改进的过程。

信息安全过程方法和 PDCA 循环



2002版的 BS7799第2部分在 ISMS 的设计和部署上第一次促进了“过程方法”的采用。这种方法就是广为人知的“Plan-Do- Check-Act(PDCA)，PDCA 是英语单词 Plan(计划)、Do(执行)、Check(检查)和 Act(行动)的第一个字母，译成中文为：计 划、实施、检查和改进”，对于进行质量和经营管理的人们来讲很熟悉。

PDCA 循环是由美国统计学家戴明博士在1950年代提出来的，所以也俗称“戴明环”。它指出，业务流程应该处理一个连续的反馈回路，使管理人员能 够识别和改变这一进程中需要改进的部分。这个过程，或者对过程的改进，首先要进行规划，然后实施，再衡量绩效，并将绩效同计划进行比较，以发现偏差或确定 潜在的改进点，并且汇报给管理层以便做出采取实际行动的决定。

PDCA 和 ISO 27001

ISO 27001在第0.2章节认可了这种模式，并且描述了如何将其应用于信息安全环境中。ISO 27001的附件 B 交叉引用了经合组织关于 PDCA 模型的准则。ISO 27001采用了 PDCA 的过程模型，并将其应用于架构所有 ISMS 的过程。

将 PDCA 循环应用在过程方法中意味着，按照流程设计的基本准则，流程中应该有输入和输出。ISMS 的需求作为其输入“有兴趣的各方对信息安全的需求和期望，通过各种必要的行动和过程，产生满足这些要求和期望的信息安全结果”。

在战术层面应用 PDCA 循环

这意味着，PDCA 循环模型有两个层面上的应用：在战略层面上，对 ISMS 自身的整体开发；在战术层面上，对每一个 ISMS 的过程的开发。

ISO 27001条文中的 PDCA 四个循环阶段

标准的简介中描述了在战略层面上，将 PDCA 循环应用到 ISMS 的开发。PDCA 循环和标准中确定了的 ISMS 的开发阶段之间的对应关系如下：

计划阶段（建立 ISMS，章节4.2.1)：

* 定义 ISMS 的范围和信息安全方针；
* 定义风险评估的系统性方 法；
* 识别风险；
* 应用组织确定的系统性方法评估风险；
* 识别并评估可选的风险处理方式；
* 选择控制目标与控制方式；
* 准备适用性申明 SOA。

实施阶段(实施和运作 ISMS，章节4.2.2)：
* 实施特定的管理程序；
* 实施所选择的控制，执行风险应对计划；
* 为受影响的员工提供必要的培训和提升安全意识
* 运作管理；
* 实施能够促进安全事件检测和响应的程序和其他控制。

检查阶段(监督和审查 ISMS，章节4.2.3)：
* 执行程序，检测错误和违背方针的行为；
* 定期评审 ISMS 的有效性；
* 评审剩余风险和可接受风险的等级；
* 执行管理程序以确定规定的安全程序是否适当，是否符合标准，以及是否按照预期的目的进行工作；
* 定期对 ISMS 进行正式评审，以确保范围保持充分性，以及 ISMS 过程的持续改进得到识别并实施；
* 记录并报告所有活动和事件。

改进阶段(维护和改进 ISMS，章节4.2.4)：
* 测量 ISMS 绩效；
* 识别 ISMS 的改进措施，并有效实施；
* 采取适当的纠正和预防措施；
* 必要时修改 ISMS，确保修改达到既定的目标；
* 持续检查、测试和改进的“持续改进”过程。

定义信息安全管理体系的范围

计划工作的第一部就是设定工作范围。
划定范围的要求在标准的条文4.2.1.a 中。具体的要求是，该组织将“依据在商业方面的特点、组织、位置、资产和技术，定义 ISMS 的范围和界限，并包括从范围中排除的所有细节和理由。”
标准的第1章节（范围）中也明确提到这点。它强调，标准中“商业”的广义解释是以该组织的生存为目的的主要活动。

第1章节给出决定 ISMS 项目范围的四个准则如下：
1.哪个法律或管理机构将为 ISMS 负责？
2.上述机构将拥有、经营和依赖哪些信息资产？
3.生成、存储和共享信息相关的流程都有哪些？
4.有什么法律和规章的规定要求适用于该信息？

范围界定实践

范围界定实践应当确定什么在 ISMS 的范围内，什么是范围之外。ISMS 于是在内外之间设定了一个边界。ISMS 的开发要求内、外部之间有一个联系点，这个联系点将被当做一个潜在的风险点，需要具体和适当的应对处理。

小型组织

在小组织里，所有的东西都应该在 ISMS 的范围内。这符合标准规定的期望，简单的情形适用简单的方案。ISO 27001特别强调从范围内排除的要求，并特别指出，所有的信息资产，或者和信息资产有关的任何东西，都应在信息安全管理体系的范围内。

大型组织

在较大的组织里，特别是那些有多个部门、多个经营场所和单位的组织里，范围的划定将更为复杂。上述的四个准则将有助于我们做出适当的决定。通常情况下，简 单地列出所有的信息资产和信息流的行为有助于明确确定 ISMS 的范围。要对在范围内的资产分别进行风险评估，所以尽早地识别出来它们有利于整个项目的进 展。
要注意，如流程一类的信息资产，不能一半在 ISMS 中，一半不在；它们要么整个全在范围内，要么就全部都不在。

法律和监管框架

对较大组织来讲，法律和监管框架对 ISMS 的范围有具体的要求。很显然，属于任何一个单一的法规或其他法律要求的范围内的信息和信息管理流程，必需在 ISMS 的范围内。

信息安全策略的制定

ISO 27001要求在计划阶段的第二步定义信息安全策略。

标准的章节4.2.1.b 要求组织制定信息安全政策。这项规定也包含在附录 A 的控制编号5.1.1中，它也是 ISO 27001众多章节的最前面一章，并且受到 ISO 27002最佳实践指南的支持。ISO 27002章节5.1.1条文扩充了 ISO 27001附录 A 中同样编号的要求，并且符合 ISO 27001第 4.2.1.b 的规范。它解释说，将政策文件作为控制目标的一项的原因是，它提供“为信息安全对业务需求和有关法律法规的依从提供管理指导和 支持。”

政策和业务目标

条文5.1.1接着指出，政策文件应设置为“符合经营目标的明确的政策方向”。该标准的观点是，一个成功的和有益的 ISMS 将不会破坏或阻止商业活动。实施阻碍业务活动的系统来应对风险，这并不与商业目标相一致，这样的话业务内部的人们将会忽略或绕过 ISMS 的控制。

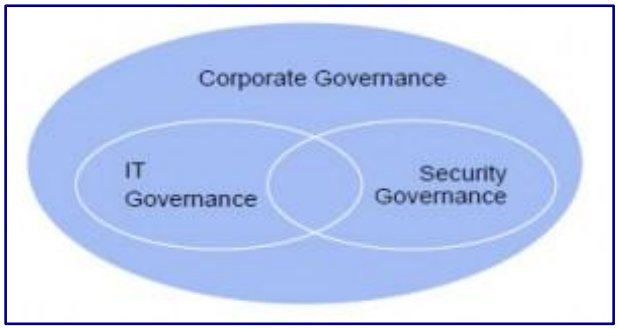
信息安全政策是重要的，必须制定到使每个字都是清楚的、明确的和有意义的（即提供一个“明确的方向”）。最后的政策确定是根据该项目范围的完成而定。范围的划定，即成功实施 ISO 27001的九大关键要素之一，对政策的定义有着举足轻重的贡献。

信息安全政策必须由董事会签署通过，并通过恰当的方式发布给那些需要用到它的人们。

信息安全治理和信息安全管理体系

关于信息治理，ICT 治理委员会绘制了一幅架构图，它展示了管理层如何响应来自业务和其他方面的直接压力来指导、评估和监测 ISMS 的有效性。

管理层将评价新的或变更了的业务和 IT 流程，并考虑当时的风险和业务需要，通过信息安全政策，提供组织以风险控制为基础的指导，将控制措施作为其作业流程的一部分，然后监测和评估这些控制的有效性。



信息安全管理之风险评估

信息安全管理体系实施的第三步是进行风险评估。风险评估在 ISO 27001的条文第4.2.1.c,d,f,g 中，在 ISO 27002的章节4中也有相关的支持性指导。这是这两个标准直接互补的第二个领域。只是 ISO 27001指定的风险评估步骤是必需遵守的，而 ISO 27002则在其第4章提供了更多的风险评估流程指南，但是它特意并未提供如何进行单独评估的详细指导。这是因为每个组织都被鼓励自行选择最适合自己行 业、复杂性和风险环境的方法。

风险处理计划的目标

ISO 27002声明风险处置计划有四个相互关联的目标。它们是：
1.消除风险（中止它们）；
2.降低不可消除的风险至“可接受的”水平；
3.容忍风险，亦即接受那些“可接受”的风险；
4.转移风险，通过合约或保险，将风险转嫁给其它组织。

关于什么是“可接受的”的定义对于风险应对计划来说至关重要，并且标准要求管理层“制定接受风险和可接受风险的准则”。它们应该成为管理层来做决定的程序的证据，并且一定要符合“在组织整体业务活动和他们面对的风险的背景下”。

风险处理计划只能在风险得到识别、分析和评估之后才能制定。风险评估过程的设计应该在组织内部的风险处置框架之下运作，并应遵照标准的具体要求。

风险评估流程

目前，定性风险评估是风险分析最常用的方法，也是标准条文4.2.1.d 中特别指定的风险识别方法。精确的数字概率数据并不是必要，要用到的是估计潜在损 失的可能性。大多数定性风险分析方法使用一系列相关的元素，这些元素也是标准要求需要识别出来的，它们包括：每项资产，它的所有者，对保密性，完整性和可 用性的威胁，它的脆弱性（即弱点）及影响。

标准设定了进行风险评估必需遵守的六个步骤：
1.在 ISMS 范围内识别出相应的资产
2.识别出这些资产的保密性，完整性和可用性所面临的威胁
3.识别出可能利用这些威胁的漏洞
4.评估这些威胁可能造成的影响
5.评估这些事件发生的可能性
6.综合评估风险

识别出范围内的资产

第一步是找出 ISMS 范围内的所有信息资产，同时记录下“拥有”这些资产的个人和部门。这项工作基于、并且也可以成为范围划定工作的一部分。这项工作中的主要组成部分包括：
1.从物理和逻辑的层面确定受保护的边界
2.找出边界内所有需要接收、存储、处理和发送信息或数据的系统，以及这些系统内的信息资产。
3.确定这些系统、信息资产和组织的目标及任务之间的关系
4.识别出对组织达成目标和任务至关重要的系统和信息资产，可能的话，将它们按优先顺序排列。附件 A.7.1是关于资产清单的控管措施，在这一点，可采纳 ISO 27002的章节7.1的指南。它明确提出，要将信息资产的属性和级别纳入考量，并且建议此时对资产进行信息安全

的等级划分，这和附件 A.7.2中关于信息应该得到适当划分是一致的。

资产所有者

在确认信息资产的同时需要识别出这些资产的“所有人”。ISO 27001定义“所有人”为“负有被认可管理责任的个人或个体，其控制资产的生成、开发、维护、使用及安全。”这里的定义并非法律认知或一般认知的财产拥 有者。每项资产必需拥有一个所有人，这是附录 A.7.1.2 中关于资产所有权中的要求。资产的所有者是个人，或者组织的一部分，它应该对资产的分级和保护 负责。

威胁

它们是那些可以让识别出来的资产出现故障或“攻击”资产的事情。它们可能来自外部，也可能来自内部。标准强制要求下一步对每项资产进行潜在威胁的识别。当 然，像单个威胁可以影响多个资产一样，标准要求 ISMS 可以拥有相当的灵活性，对于落在同一级别同一类型的资产，当它们面临的威胁也一样时，可将这些资产 当做一类，在后续的工作中进行相同的对待。

漏洞（弱点）

它们让系统容易受到某种攻击，是可以被威胁利用的系统缺陷，能够增加系统被攻击的可能性。举例讲，“火灾”是来自外部的威胁，而服务器机房堆有可燃物即是 漏洞。在标准的术语中，漏洞可以被威胁来利用。下一步是评估过程，就是为每项资产和每项资产的威胁找出相关可能利用的漏洞。一项资产可能面对多种威胁，每 种威胁又可能被多个漏洞利用。您需要把它们全都识别出来，有一种方法可以参考，特别是对于计算机硬件和软件，可以参考标准的业界来源如 bugtraq 和 CVE。原厂商关于漏洞的更新也可以纳入考量，另外，所有的漏洞并不能被一下子全部发现出来，组织需要不断的跟踪和识别新的漏洞。

影响

威胁对漏洞的成功利用可以造成资产可用性、机密性和完整性的影响。这些影响应该被尽可能的识别出来，并且赋于相应的货币价值。标准明确规定影响应该在这三方面得到评估；一种威胁可以利用多个漏洞，而成功的利用可能造成多种影响。

标准的要求是对每项潜在的影响测评出对业务可能带来的损失。这项工作的目的是排序应对措施，以便同组织可接受的风险起点相对关联。划分出可能的损 失，而不是尝试着计算出准确的数值也是可以接受的。可以在管理团队的指导下，依照组织的大小及目前风险应对架构，设定一些财务级别。在评估潜在风险代价 时，所有的代价包括直接的、间接的和由它们派生来的，都应该记入其中。

风险评估

简单讲，在这一流程之前都是关于数据收集和事实评估的。此前的各个阶段都有些事实上的关联。漏洞的识别方式可以分为技术的、逻辑的和物理的。组织针对这些 所做的决策将和他们统计这些威胁的动作有关。这意味着现在实际分析出来的风险同组织整体的“风险追求”有关，“风险追求”即组织对风险所采取的愿望。风险 评估包含识别潜在的业务伤害，它们来自每项识别出的风险。

可能性

在此前，评估是在各种识别出的威胁拥有相同的发生的可能性下进行的。真实情况并不会如此，所以有必要评估相关影响发生的可能性或者概率。概率可以分级为“非常不可能”到“时常会发生”。

计算风险级别

最后一步的工作是对每项影响计算出风险级别，并且将详细情况转交组织资产和风险日志。风险级别是影响和可能性综合作用的结果。经常将风险划为三个级别： 低、中和高。当可

能的影响较低，而可能性也低时，风险级别可认定为低；当可能的影响和可能性都是高时，风险级别可认定为高；其它界于两者之间的可认定为中 级。然而，每个组织都可以根据自身实际情况分类和设定每项影响的风险级别。

信息安全管理之风险应对计划

ISO 27001第4.2.2.a 及 ISO 27002条文4.2中要求组织“明确风险处置计划，它为信息安全风险管理指出了适当的管理措施、资源、职责和优先级”。这一条文和详细处理管理责任细节 的条文5有交叉引用。风险处置计划一定要得到记录，它应该被设置于组织的信息安全政策方面，应明确识别该组织的风险应对方法，以及接受风险的准则。当有风 险应对框架时，这个准则应当和信息安全管理标准的要求相一致。

标准的第4.2.2.a 及第5条文都要求风险应对计划需要得到正式的定义和描述，它应该包含高优先级的信息安全行动。角色与职责的描述、操作流程的详情、日后的检视及更新等都应该得到正式的定义和分配。

记录风险处理计划

风险处理计划的核心是一个详细的时间表，它显示出，对于每一项确定的风险，该组织决定如何对待它，哪些控制已经到位，哪些额外的控制被认为是必要 的，以及实施它们的时间框架。对每项风险，可接受的风险程度需要得到确定，同样要确定可将风险置于一个可接受水平的风险处理选项。

风险处置计划和风险评估计划相关联，详细的情况在前面风险评估章节中有讲到，目的是为了识别和设计恰当的控制措施，以及如在适用性声明中所描述的那 样，部署、测试和改进董事会设定的风险管理方法。这一计划也应确保有足够的经费和实施资源来部署选定的控制措施，并应列清楚它们具体是什么，有哪些。

风险处理计划也应确定执行和持续改进它所必需的个人能力和广泛的培训和宣传。

风险处理计划和 PDCA 方法

风险处理计划是同 ISMS 的 PDCA 循环中所有四个阶段联系起来的关键文件计划。它是一种高层次的，记录在案的关于谁负责交付哪些风险管理目标、如何实现、要用到哪些资源，以及如何评估和改进它们。

适用性声明 SoA


Statement of Applicability

ISO 27001:2005 Controls				
Clause	Sec	Control Objective/Control		
Security Policy	5.1	Information Security Policy		
	5.1.1	Information Security Policy Document		
	5.1.2	Review of Information Security Policy		
Organization of information security	6	Internal Organization		
	6.1.1	Management Commitment to information security		
	6.1.2	Information security Co-ordination		
	6.1.3	Allocation of information security Responsibilities		
	6.1.4	Authorization process for Information Processing facilities		
	6.1.5	Confidentiality agreements		
	6.1.6	Contact with authorities		
	6.1.7	Contact with special interest groups		
	6.1.8	Independent review of information security		
	6.2	External Parties		
	6.2.1	Identification of risk related to external parties		
	6.2.2	Addressing security when dealing with customers		

虽然适用性声明在 ISMS 中是至关重要的，并且附于认可的 ISMS 证书，从这份文档这儿，审计人员将开始确认是否有适当的控制措施部署到位和在运作之中，它的准备工作只能在风险评估计划完成，也就是风险处置计划制定完成时得到进行。

适用性声明是关于 ISO 27001的附件 A 中的哪些控制适用于该组织，哪些不适用的声明。此外，它也可以包含来自其他来源的控制措施。

控制措施和附录 A

标准的4.2.1.g 中要求组织从 ISO 27001的附件 A 中选择控制目标和控制项，这些已普遍被认为是一个组织所需要的，对这些控制的选择和排除需要有合理的解释。然而，它明确要求组织要彻底照章进行，并且表明，可以从其他的来源选择额外的控制。

ISO 27002提供了关于标准附件 A 中所列控制目标和部署的最佳实践。然而，一些组织可能需要做得比 ISO 27002规定的要求更多，要多到何种程度，取决于其中技术和威胁的不断演进情况，毕竟 ISO 27002的初版已经定稿和发布。

控制

控制是安全漏洞的对策。正式的 ISO 27002定义是“一种管理风险的措施，包括政策、程序、指引、实践或组织结构，它可以是一个行政的、技术的，管理的或法律的性质。”控制也用作“保障”或“对策”的代名词。

除了明知接受符合组织风险应对计划中关于风险接受准则要求的风险，以及通过合同或保险的方式转让风险之外，组织可以决定实施控制，以降低或减少风险。

残余风险

对每一项单独的风险提供全面所有的安全并不可能也不现实，但是可以通过将大多数风险控制到一个适当的水平以获得有效的安全，在这个水平管理层可接受剩余的风险。管理部门必须正式接受剩余的风险。

控制目标

从控制目标中选择控制。控制目标是一个组织企图来控制它的一些进程或资产，以及打算通过使用一些控制要达到的目的的声明。一个控制目标可能包含多项控制。

ISO 27001的附件 A 列出相应的控制目标，并列出要实现每项控制目标必需采用的最小控制措施。组织必须选择它的控制目标，以及选择相应的控制措施并执行，以便使它能够实现确定的目标。

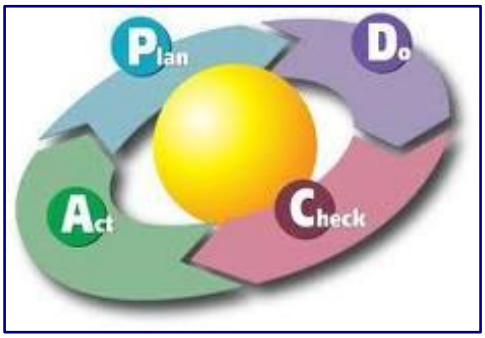
安全事件响应计划

重要的是，在考虑控制时，可能出现的安全事故的检测也需要定义、考虑和计划。标准条文 4.2.2.h 中要求实施控制措施以便“及时发现和响应安全事件”。实际上，在选择附录 A 所列的独立控制项时，应考虑包括需要搜集和保留哪些证据，控制的实施效果要得到什么样的测量。关于实施效果的测量，要保证如下两点儿：

1.控制已得到实行，并得到有效地运作

2.如标准所要求的，每项风险都已经被降低到可接受的水平。实施控制过程中的任何错误，或执行过程中的失败，都能够被及时发现和得到及时的纠正，无论是通过自动或手动的方式，都能有效地减少或降低未来可能发生的任何风险到可接受的水平。

执行——实施和运作信息安全管理体系



依照 ISO 27001，部署信息安全管理体系 ISMS 的第一阶段在适用性声明 SoA 完成之后。SoA 必须识别出控制目标和选定的控制措施，以及选定它们的原因，它又 指回到风险评估和风险应对计划。标准还要求识别出目前已实施的控制，以及识别出信息安全管理体系日常运作中涉及到的绝大多数控制。

差距分析

下一步的关键是进行差距分析。差距分析的目的是确定风险评估进程中识别出的控制和 SoA 中记录的控制，以及实际部署的控制之间的差距。在大多数组织 中，实际上拥有的控制措施和它们所需要的并不一致，这种情况并非罕见。这种不一致并非仅仅是说组织缺乏相应的控制措施，而且包含组织很不容易发现已有的控 制措施没有得到恰当正确的操作，或者这些控制根本没有必要。差距分析需要同时对信息安全管理体系和流程管理方面进行评估，同时还要对已经实施的技术控制进 行评估，最好是由独立于被评估领域之外的专家进行。

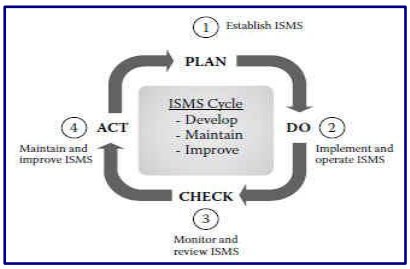
差距分析使本组织能够将风险处置计划的第二和最重要的部分放在一起，“管理信息安全风险的管理行动、资源、责任和优先级别”是一套详细的行动计划， 运用它们，可使组织切实履行其信息安全管理体系。如前所述，风险处理计划是链接信息安全管理体系 PDCA 循环的四个阶段的关键文件，并确保一切需要做的是 得到了贯彻执行。

部署实施

信息安全管理体系的设计和实施的其余第二阶段包括以下五项活动：

1.实施风险处理计划和 SOA 中确定的控制；
2.定义如何衡量和评估所有控制的有效性；
3.实施信息安全意识，教育和培训的培训和宣传方案；
4.管理信息安全管理体系，所有的联锁控制和程序必须继续工作，新的威胁需要得到识别、评估和进行必要的处理。人员需要招募和训练，要监督他们的绩效表现，以及按照业务不断变化的需求开发他们的技能。ISMS 的有效性必须加以管理，长期的持续改进必需得到计划和领导；
5.实施事件检测和响应程序，它连接到 ISO 27002第13条款，信息安全事件管理。它包含两项控制目标和五项控制。开发和实施信息安全事件管理流程合乎标准的要求，并且经常开始于信息安全管理体系项目的启动。

检查——监控和评审信息安全管理体系



标准的4.2.3整个章节都是关于监控和评审的。它强烈的反映出管理层积极参与信息安全管理体系的长期管理的需求，同时认识到，信息安全威胁环境的变化快于商业环境。下面我们将粗略地讨论三种类型的活动，即：监控，审计和评审。

监控

监控，也可称为监督，它的首要目的是尽快地检测出程序的错误和信息安全事件，以便能速度采取纠正行动。监测应是正式的、系统化的和广泛的。附录 A.10.10安全类别监测中包含专门监控 IT 相关的活动，这些都与 ISO 27001的此部分相关联。第13章信息安全事故管理，也是监控的核心部分，它提出，组织必须监测偏差和事件，响应它们和从中学习。

审计

审计，另一方面，是经过专门设计和规划，用以确保在 SOA 记录中的控制是有效的及正在使用中的，并确定不合格和改进的机会。
控制目标15.2（符合安全政策和标准，以及技术合规检查）中有特别针对这一问题，强调要有计划地定期进行在流程和技术层面人合规检查。A.15.3提出审计工具的安全性要求。审计在 ISO 27001的第6条文有更深入的要求，其中规定了如下两个重要方面：

1.审计程序“应该策划审计方案，考虑审计过程和区域的状况及重要性，以及上次审计的结果。”
2.“受审计区域的管理负责人应确保立即采取措施以消除发现的不符及其原因，跟踪活动包括所采取措施的验证及验证结果的报告。”

再次重复一篇，标准清晰的指出，组织各级管理在信息安全管理体系的有效实施、维护和改善方面扮演重要角色。这必需纳入到管理和监督工作的职责描述、劳动合同、文化导向和其他培训及绩效评价中。

评审

评审也作审查，对内部和外部审计政策、业绩报告、异常报告、风险评估报告和所有相关的政策和程序进行评审，以确保信息安全管理体系在不断变化的背景下继续有效。

这一阶段当然和附件 A 以及 ISO 27002的相关章节有密切的关联，具体关联如下：
1. A.5.1.2 信息安全策略的评审
2. A.5.1.8 信息安全的独立审查
3. A.10.2. 第三方服务的监测和审查
4. A.10.10 监测本身就是一项控制目标
5. A.11.2.4 用户访问权限的审查
6. A.12.2 应用程序的正确处理，是监测程序的使用和数据处理的控制目标
7. A.13.2.2 从信息安全事故中学习
8. A.14.1.5 测试、维护和重新评估业务连续性计划

所有的这些控制都必须在 ISMS 第三阶段的开发和实施阶段得到解决。监控和评审报告活动的相关发现和输出要被转移至纠正和改进行动，并且，出于 ISMS 的目的，用以证明决策过程和实施这些决策的审计记录需要保存在 ISMS 的记录中。

行动——保持和改进信息安全管理体系

这是非常简短的章节，它反映了 ISO 27001的4.2.4条款的简单需求。这一条款列出了从前面监控和评审活动中学习到的所有东西的要求，它们需要得到实施。它也和第8章有密切关联，其中 8.1持续改进；8.2纠正措施；8.3预防措施，它描述了这项活动的目的和它一定要成为组织信息安全管理体系日常管理工作中的必不可少的一部分。

管理评审

这里也和管理评审有关系，管理评审应该导致“采取适当的纠正和预防措施”，以及随时随地推进可能影响 ISMS 的变革，和改进的建议。

需要注意的是纠正性和预防性措施应基于风险评估的结果区分优先级别。

分析和评估风险对任何组织都是必需的核心竞争力，对实现和维护 ISO 27001标准认可的认证非常重要。标准的最后语句也指出：“对非符合项的预防措施通常要比纠正行动更具成本效益。”它总结了标准基于风险的，具有成本效益的，常识性的方法。

组建信息安全管理体系项目指导委员会

信息安全管理体系项目需要一个有适当组织架构和资源的项目团队。这是一个常识，它也反应了 ISO 27001条款5的要求，以及附录 A.6.1.1到 A.6.1.3的控制要求。

展示管理承诺

ISO 27001条款5要求管理层展示其承诺的“建立，实施，运行，监控，审查，维护和改进信息安全管理体系”，并且给出如下需提供证据的步骤：

1.建立信息安全政策，它应该得到正式的讨论，并由董事会或高层管理团队进行签署；
2.确保信息安全管理体系目标和计划的建立，它最好由信息安全管理体系项目团队来完成；
3.建立信息安全的角色和职责，它应从建立 ISMS 项目团队入手；
4.传达信息安全的重要性给组织，为信息安全管理体系和它的持续改进提供支持；
5.为信息安全管理体系的开发和部署的各个阶段和方面提供足够的资源；
6.决定风险的接受和控制标准，这些标准应在正式的管理会议上完成；
7.确保信息安全管理体系审计的进行；
8.对信息安全管理体系进行管理评审。

项目小组/指导委员会

最高管理者应建立一个由业务牵头的项目小组或指导委员会，负责设计和实施信息安全管理体系。这个团队应该是由一名对业务负责的高层经理来领导，最好 的人选是组织的 CEO。经验告诉我们，这个团队不应该由 IT 经理来带领，因为 IT 经理没有足够的跨业务和商业管理经验及威信，将业务作为一个整体来建立和 实施管理制度。

在总经理带领下的项目小组，应包括关键的职能部门经理以及 IT 和信息安全的技术专家。如果内部没有足够的资源，应该使用外部的技术专长；当使用外部承包商时，要应用和第三方合约相关的各类控制，如 A.6.1.5的保密协议和 A.6.2的外部各方。

信息安全协调

控制 A.6.1.2要求组织的不同部分的代表在整个组织内共同协调信息安全。在所有除了非常大型的组织里，这个团队应该是信息安全管理体系项目组原班人马。这个团队也被赋予信息安全责任和分配详细的任务，详情见 A.6.1.3，分配信息安全责任。

发动信息安全管理体系项目

信息安全管理体系项目实施的前期预备应至少包括以下四个阶段：
1.认知——开发包括董事会、高级管理层和关键职能经理之间的理解，关于为什么需要信息安全管理体系，以及哪些需要参与进来。
2.学习——深度开发项目组和需要直接参加项目的人员的技能和知识。
3.范围——制定哪些在信息安全管理体系范围内，哪些在信息安全管理体系范围之外。
4.策略的制定——为组织开发并批复信息安全政策。这项政策规定了在业务目标范围内的信息安全管理体系的方向。

意识认知

信息安全管理体系的部署是一个商业项目，而不是技术或 IT 项目。

除非获得会对业务的成功有重要影响力的董事会、高层管理及高阶业务和职能经理们的积极支持，否则项目会失败。

ISO 27001标准在第5条还明确规定，管理层“应当提供其承诺的建立，实施，运行，监督，审查，维护和改进信息安全管理体系的证据。”在此，标准中明确要求 了相关的控制和持续改进，任何制定和实施信息安全管理体系的组织必需得到高阶管理层的充分参与。本标准第5节支持的论点是，如果没有高层管理者的支持，组 织根本无法实现一个有用的信息安全管理体系，更不用说取得被认可的认证。

认知工具箱

最常用的开发意识认知的方法包括：
1.采购和分发标准
2.邀请内部或外部专家进行关于标准和实施要求的演讲和研讨会
3.使用电子学习或其他内部沟通和培训工具
4.大规模人员的集中讲解和培训学习班

重要的是，所有的意识建设活动需集中在该组织从信息安全管理体系实施中可获得的具体利益，以及该组织面临具体的威胁及风险，因为这样做有助于建立参与这一进程的所有工作人员的理解和承诺。

信息安全管理体系绩效评估

ISO/IEC 于2009年发布了正式版的 ISO 27004专门用于信息安全管理的绩效评估。这一标准提供各类组织如何衡量和报告他们的信息安全管理体系的有效性的方法。它涵盖 ISO 27001 中定义的信息安全管理流程和 ISO 27002中定义的安全控制。

为了便于评估信息安全管理体系的有效性的，ISO 27004提供用于开发和使用的测量和评估指南和建议，包括信息安全管理体系策略和目标，以及 ISO27001中特别指定的安全控制。ISO 27004标准也适用于实施信息安全管理体系的各类规模的组织。

这些衡量应该允许信息安全活动得到有针对性的评估、各个阶段的信息安全活动达到得的各项水准得到监控，各类不同的组织也可以得到相应的参照值，并进行信息安全有效性的评比。

美国国家标准技术研究所 NIST 也有发布相关的信息安全绩效评估指南，编号文档：SP800-55。它是开发信息安全管理体系的衡量和矩阵的指南。

ISO 27004可以从 ISO 网站进行购买；NIST SP800-55可以免费下载，和作为参考。

备战信息安全管理体系审核

信息安全管理第三方认证为组织的信息安全体系提供客观公正的评价，使组织在信息安全管理方面有更大的可信性，并且能够使用证书向利益相关的组织提供信心保证。

在允许外部审计师进行正式的认证审核之前，组织很有必要进行一项针对信息安全管理体系的设计和实施的全面的复查。

复查应该由组织的内部审计团队进行，在 ISO 27001的第6章节中有强制性规定内审团队要负责审计活动。

一项全面、逐步的审核很有必要，它不仅能找出安全认证计划中可能漏掉的关键步骤，而且是确保信息安全管理体系得到适当和全面部署的最好的方法。

评审的流程需按照 ISO 27001中关于评审的要求得以建立和归档，当一个详细的审核完成后，管理层应该评审相关的发现，并且这些报告应该按照 ISO 27001的第7章节的要求进行存档。

ISO 27001主要咨询及认证机构清单

已知国内主要的信息安全管理体系认证机构：
DNV 中国 www.dnv.com.cn
BSI 中国 www.bsigroup.cn
通标标准技术服务有限公司 www.cn.sgs.com
Bureau Veritas 中国 www.bureauveritas.cn
中国信息安全认证中心 www.isccc.gov.cn
广州赛宝认证中心 www.ceprei.org
香港品质保证局 www.hkqaa.org

已知的比较活跃的信息安全管理体系咨询顾问公司：
科飞管理咨询公司 www.cofly.com
谷安天下 www.gooann.com
上海天帷企业管理咨询公司 www.tanovo.cn
中奥常州认证咨询有限公司 www.czzhongao.com
深圳誉杰咨询管理有限公司 www.yujie.org.cn
上海天帷企业管理咨询有限公司 www.tanovo.cn
中信保国际集团 www.bytewatch.com.cn
深圳市易聆科 www.szelink.com
宏儒 www.hr9000.com
北京楚齐咨询有限公司 www.bjbort.com
中科天智 www.52cmmi.com
华鑫创顾问集团 www.hxiso.com
北京润成国际标准技术 www.rcist.com
金证 IT 服务管理认证咨询 www.cn27001.com
北京趋势引领 www.trendsetting.com.cn
Maximus Consulting www.maximusholding.com

*注：如果您发现有组织不在这个名单中，请告知，以便添加。

ISO27001:2005 课程简介

ISO 27001也有些培训课程，典型的比如面向 Internal Auditor（内审员）和 Lead Auditor（主任审核员）的培训课程。

虽然不比专业的信息安全及审核方面的认证如 CISSP 和 CISA 等含金量高，但是仍然很值得实施信息安全管理体系的组织和人员参加。

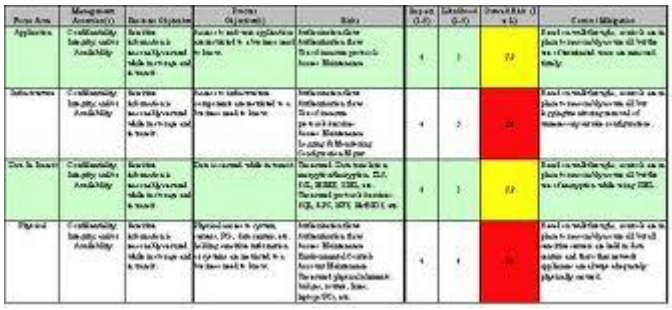
内审员的培训课程一般为三天，适合欲建立一套符合 ISO 27001标准的信息安全管理体系的企业，组织中将要执行内审的人士以及 IT 经理、系统经理、IT 安全经理等。

主任审核员的培训课程一般为五天，是内部审核员的进阶课程，适合于想把信息安全管理体系引入组织的人员以及立志为第三方认证机构工作的人员，它如何管理和领导信息安全管理体系审核活动。

请注意，由于组织中信息安全相关人员的职责有些差异，所以相关的培训课程也会不断地变化，例如 BSI 已经更新了相关的信息安全管理体系课程，以便更加有角色的针对性。

1. 精要课程(2天)
2. 建立与实施课程(3天)
3. 专员课程

ISMS 风险评估/管理工具简介



为了简化在信息安全管理体系的工作量，有组织机构设立了相关的文档范例和模板，甚至开发出相应的管理系统。

一方面，是可用来参考的流程类文档如方针政策、标准、作业流程和操作指南等。我们的建议是最初起草这些文档时，不要在它们的基础上更改，如果有相关的文档管理系统，则应先按照标准化文档的要求自行准备，之后再和参考范例文档进行对比，并做相应的改进。

另一方面，是模板，我们建议初次开始导入信息安全管理体系的组织先自行开发各类模板，如资产登记清单，风险评估模板，控制措施清单等。如果有相关的文档管理系统，则可考虑使用集中的文档管理系统。

之所以建议初始导入 ISMS 的组织先自行建立它们是方便组织对整个过程的深入了解和掌握，这样做也更容易形成管理体系文件架构，然后最底层文件，即用于证明 ISMS 各项活动的记录表格就比较容易得到完成。

初步建立起文档体系的组织可以考虑选择管理工具包，即自动化的管理系统，常见的一些 ISMS 系统的功能包括：资产管理、风险管理等等。

组织可以考虑自行开发或采购商业化产品，自行开发的产品会更适合组织的实际需求；商业化的产品会给组织带来更多的专家经验。组织亦可以考虑外包这类系统的开发和维护，甚至使用“云”信息安全管理系统。

注意，也有供应商会将更多功能整合，比如 IT 系统的监控、日志审计和管理控制平台等，一般我们不推荐和 ISMS 文档管理系统整合，但是组织想根据自身情况考虑一下也无妨。

结束语：本小册子部分内容为翻译，部分为原创，由于作者知识面和水平有限，而且标准本身也不断地更新，所以请读者批评指正，以便在后续版本中不断更新。