国家“十二五”重点规划图书
信息安全管理体系丛书

ISO/IEC 27001:2013 标准解读及改版分析

- 丛书顾问：蔡吉人　周仲义
- 丛书主编：吕述望　赵战生　陈华平
- 执行主编：谢宗晓　吕茂强

谢宗晓　巩庆志　编著

中国质检出版社
中国标准出版社

ISO/IEC 27001:2013
标准解读及改版分析

谢宗晓　巩庆志 ◉ 编著

中国质检出版社
中国标准出版社

北　京

图书在版编目(CIP)数据

ISO/IEC 27001:2013 标准解读及改版分析/谢宗晓,巩庆志编著.
—北京:中国标准出版社,2014.4
ISBN 978-7-5066-7492-8

Ⅰ.①I… Ⅱ.①谢…②巩… Ⅲ.①信息安全—风险管理—质量管理体系—国际标准—研究 Ⅳ.①TP309—65

中国版本图书馆 CIP 数据核字(2014)第 029003 号

中国质检出版社
中国标准出版社 出版发行
北京市朝阳区和平里西街甲 2 号(100029)
北京市西城区三里河北街 16 号(100045)
网址:www.spc.net.cn
总编室:(010)64275323 发行中心:(010)51780235
读者服务部:(010)68523946
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 9 字数 298 千字
2014 年 4 月第一版 2014 年 4 月第一次印刷
*
定价 32.00 元

前言

preface

关于本书的写作目的及其与相关书籍之间的关系

本书主要为需要 ISO/IEC 27001：2013《信息安全管理体系　要求》升级换证的组织提供指导。

虽然 ISO/IEC 27000 标准族只发布了一部分，大部分还在开发中，我们在《信息安全管理体系实施指南》第 3 部分中对截至 2012 年 9 月的进展情况做了介绍，即已经公布的标准，ISO/IEC 27000 标准族改版较频繁，例如：关于信息安全风险管理的 ISO/IEC 27005 就有 2008 年的版本和 2011 年的版本。作为致力于指导信息安全管理体系实施的系列丛书，我们当然有义务把最新版本的标准介绍给大家。

ISO/IEC 27001：2013 一经发布，意味着已经获取 ISO/IEC 27001：2005 认证的组织需要改版。截至 2012 年，中国大陆地区已经有 1490 家组织获得认证，全世界范围内已经有 19577 家组织获得 ISO/IEC 27001：2005 认证。

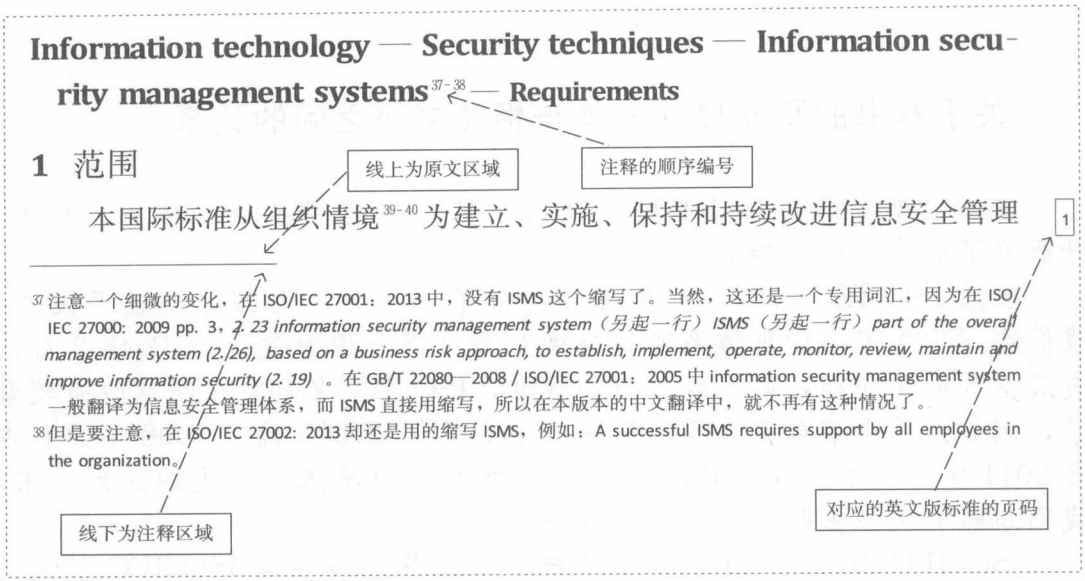
由于 2012 年 10 月出版的《信息安全管理体系实施指南》、《信息安全管理体系实施案例》和《信息安全管理体系审核指南》都是基于 ISO/IEC 27001：2005 的，因此，最紧要的就是在已经出版的信息安全管理体系丛书的基础上，重点关注新版修改的部分，迅速满足 ISO/IEC 27001：2013 升级换证的要求。当然，我们会陆续依据 ISO/IEC 27001：2013 完成相关信息安全管理体系丛书的改版。

关于本书的主要内容以及如何阅读本书的指导

本书首先给出了一个完整的中文版 ISO/IEC 27001：2013，在词汇的

选择上，我们尽量与 GB/T 22080—2008 / ISO/IEC 27001：2005 保持一致，没有在其中出现过的，则依据 GB/T 5271.8/ISO/IEC 2382-8：1998《信息技术 词汇 第 8 部分：安全》或 GB/T 29246—2012 / ISO/IEC 27000：2009《信息技术 安全技术 信息安全管理体系 概述和词汇》。

为了最大限度地保持读者阅读过程的流畅性，本书对标准条文的解释采用脚注的形式，具体如下所示：



除此之外，本书还给出了以下内容：

ISO/IEC 27001：2013 与 ISO/IEC 27001：2005 正文章节的对应，以 ISO/IEC 27001：2013 为主，将 ISO/IEC 27001：2005 中曾经涉及的内容做了对应；

ISO/IEC 27001：2013 与 ISO/IEC 27001：2005 附录 A 章节的对应，以 ISO/IEC 27001：2013 为主线，将 ISO/IEC 27001：2005 的控制措施对应到这些章节上，可作为编制改版的适用性声明的参考；

ISO/IEC 27001：2005 与 ISO/IEC 27001：2013 附录 A 章节的对应，与上述相反，以 ISO/IEC 27001：2005 为主线，将 ISO/IEC 27001：2013 的控制措施对应到这些章节上，可作为编制改版的适用性声明的参考；

虽然本书中没有给出 ISO/IEC 27002：2013 的中文版，但是由于在解读过程中涉及诸多 ISO/IEC 27001：2013 附录 A 的内容，因此对于本

书中所涉及的控制措施的实施指南，我们与英文版的 ISO/IEC 27002：2013 的页码进行了对应。

最后一部分给出了最新的 ISO/IEC 27000 标准族的工作进展情况，时间截至 2013 年 11 月。

由于更关注改版分析，因此《信息安全管理体系实施指南》中解读的内容，在本书中不再赘述。对标准更详细的解读和更深入的理解，请阅读《信息安全管理体系实施指南》，对标准实施落地的讨论，请阅读《信息安全管理体系实施案例》。

其他信息

一般情况下，作者在写前言的时候都要写上“仓促成稿，谬、误之处难免，恳请读者批评指正”，表示自己的能力还没有发挥出来，或者给书中的错误找个台阶，但是 ISO/IEC 27001：2013 和 ISO/IEC 27002：2013 的正式版 2013 年 10 月才公布，我们所描述的“仓促”是一个事实，当然这不应该成为错误多的理由，对于书中的谬误或讨论，可直接发至我的信箱：xiezongxiao@vip.163.com，我们一定尽快修改。

至于为什么不能“慢工出细活”，原因是有太多的人问我 2013 版的 ISO/IEC 27001 与 2005 版相比，到底有什么区别？每天都耐住性子看英文论文的我，还是很理解对着一个英文标准看的人是什么心情，再加上标准条文晦涩难懂。于是我们和中国标准出版社的王成编审和曹剑锋编辑决定在最快的时间给大家提供中文版的 ISO/IEC 27001：2013。即使会有一些错误，但是鉴于购买本书的读者具有一定的信息安全专业知识和相关从业经验，因此我们相信本书的读者有自己的判断能力，而且为了防止误读，凡可能产生歧义之处，我们都给出了对应的英文版原文。

编著者

2013 年 11 月 24 日

目录

contents

ISO/IEC 27001：2013《信息安全管理体系　要求》

本书附录

ISO/IEC 27001：2013 从此处开始

ISO/IEC 27001：2013《信息安全管理体系　要求》（Second edition 2013-10-01）[1]

前　言

ISO[2]（国际标准化组织）与 IEC[3]（国际电工委员会）为全世界范围内的标准化构建了专业体系。国家作为 ISO 和 IEC 的成员通过专业的技术委员会参与到国际标准的开发过程[4]。技术委员会[5]由各个组织所建立，处理专门领域的技术活动，ISO 和 IEC 在共同的兴趣领域合作成立技术委员会，其他与其有联系的政府或非政府国际组织也参与其中的工作。在信息技术领域，ISO 和 IEC 建立了一个联合技术委员会：ISO/IEC JCT1[6]。

1 ISO/IEC 27001：2005 正文字体为 Arail，ISO/IEC 27002：2005 正文字体为 Times New Roman。现在 ISO/IEC 27001：2013 和 ISO/IEC 27002：2013 正文字体都换为 Cambria，我们把本书中所有的正文英文字体也改成了 Cambria。示例如下：Cambria、Arail、Times New Roman。

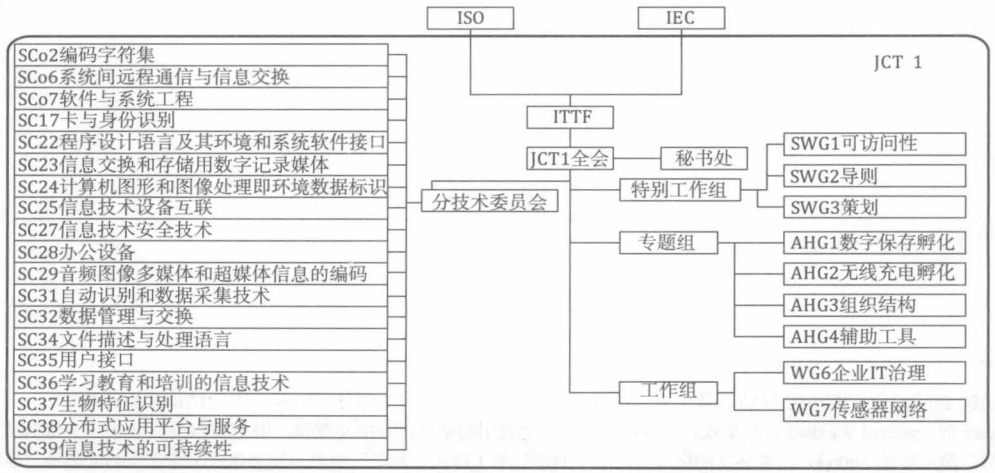
2 ISO 成立于 1947 年，总部在瑞士日内瓦，是非政府性国际组织，目前是世界上最大的国际标准制定组织和出版组织之一。

3 IEC 成立于 1906 年，总部也在日内瓦，1947 年作为电工部门并入 ISO，1976 年重新剥离，是制定和发布国际电工电子标准的非政府性国际机构。

4 国际标准化组织的成员资格一般为最能代表该国家标准化的机构，成员分为三类：1）成员体，一个国家只能有 1 个具有广泛代表性的国际标准化机构，可以参加投票。2）通讯成员，需支付会费，可以参加技术机构活动，但是不能投票。3）注册成员，需支付会费，通常来自没有建立国家标准化机构的欠发达国家。

5 技术委员会，technical committees TC，联合技术委员会，joint technical committee JCT。

6 ISO/IEC JCT1 是 ISO 和 IEC 的联合技术委员会，即信息技术标准委员会。目前 JCT1 有 3 个特别工作组，4 个专题组，2 个工作组，19 个分技术委员会。结构如下：



其中，ITTF 为信息技术任务组。秘书处由美国 ANSI 承担。

国际标准的起草与 ISO/IEC 导则[7]第 2 部分中所规定的准则保持了一致。共同技术委员会成立的主要任务是准备国际标准[8]，被共同技术委员会接受[9]

[7] ISO/IEC Directives，ISO/IEC 导则，其中第 1 部分：技术工作程序，第 2 部分：国际标准的结构和编写规则。

[8] prepare International Standards，起草或者准备国际标准，此处用起草更符合中文逻辑，但是技术委员会相当一部分工作并不是写，而是接受（adopt）已经成文的标准，应该“判断”的工作比“起草”更多，当然这些工作笼统的讲都是“准备”。

[9] 这里的接受为 adopt，也有正式通过的意思。可见技术委员会也承担了类似杂志编委会的职责。

的国际标准草案分发[10]至各个国家投票。国际标准的正式发布[11-12-13-14]需要至少有75%的投票成员国家投赞成票。

需要引起注意的是本文档的某些元素可能涉及专利权利，ISO 和 IEC 并不负责识别任何这种专利权利。

ISO/IEC 27001 由联合技术委员会 ISO/IEC JTC1 信息技术标准委员会，

---

10 原文为 circulated，流通。文档这种流通，我们一般用分发（distribute），流通本身有扩散（diffusion）的含义，好像更为形象一些，但是容易产生歧义。

11 原文为 publication as an International Standards，就是被出版为国际标准，直接的意思就是发布，与平时的发布消息等不同之处在于国际标准是收费出版物。

12 一个国际标准的开发过程大致为如下 6 个步骤：S1: Proposal stage 提案阶段，这个阶段的目的是确定有必要就某个特定的课题开发国际标准，S1 阶段的文档产物为 NP（New work item Proposal）；S2: Preparatory stage 准备阶段，通常会建立一个工作小组来准备工作草案（working draft），在这个阶段草案会被提交给工作小组的上一级委员会；S3: Committee stage 委员会阶段，一旦开发出第一个 CD（Committee Draft 委员会草案），将会分开征求意见，一旦通过，该文档会被提交为 DIS（a draft International Standard 国际标准草案）；S4: Enquiry stage 调查阶段，DIS 会分发给所有的 ISO 成员问询意见。如果超过三分之二的成员国通过，则文档成为 FDIS（a final draft International Standard 最终国际标准草案）。问询意见大约需要 5 个月时间。S5: Approval stage 批准阶段，FDIS 被分发至所有的 ISO 成员国，以确定“是或否”选项，大约需要经过 2 个月，本阶段通过需要三分之二的成员国通过，且不超过四分之一的成员国反对；S6: Publication stage 发布阶段，注意，文本自 FDIS 至正式发布一般不会有大的改动，但是之前的文本经常有较大的改动。除此之外，所有的国际标准在发布的三年之内或第一次评审之后的每隔五年都需要评审，以确定该标准被确认、修改或废弃（Confirmation, Revision, Withdrawal）。更详细的开发过程介绍可以参考 http: //www. iso. org 中标准开发栏目。

13 根据 ISO/IEC 导则，第 1 部分 2. 1. 6 的规定，一个标准一般应在 36 个月内完成，JTC1 还提出三种时间框架，包括：默认时间框架、加速时间框架和延长时间框架。表中时间单位为月。

工作阶段	细分阶段	默认时间框架	加速时间框架	延长时间框架
S1- S2	新项目注册	0		
S3	CD 注册	12		18
S4	DIS 注册	18	6	30
S5	FDIS 注册	30	18	43
	启动 FDIS 投票	32	20	45
	分发 FDIS 表决汇总	35	23	47
S6	IS 出版	36	24	48

14 我国国家标准的产生流程跟国际标准类似，大致阶段如下：

阶段名称	阶段工作	阶段成果	完成时间/月
预阶段	提出新工作项目建议	PW1	
立项阶段	提出新工作项目	NP	3
起草阶段	提出标准草案征求意见稿	WD	10
征求意见阶段	提出标准草案征求意见稿	CD	5
审查阶段	提出标准草案送审稿	DS	5
批准阶段	提供标准出版稿	FDS	8
出版阶段	提供标准出版物	GB、GB/T、GB/Z	3
复审阶段	定期复审	继续有效/修订/修改/废止	60
废止阶段		废止	

更多的信息请参考：中国电子技术标准化研究院，全国信息技术标准化技术委员会和全国信息安全标准标准化技术委员会编著，《信息技术标准化指南》，中国标准出版社。

SC27，IT 安全技术分委员会[15]负责[16]。

第二版（ISO/IEC 27001：2013）是第一版（ISO/IEC 27001：2005）的技术修订，同时第一版被废除和取代。

0 引言

0.1 通用

本标准为建立、实施、保持和持续改进信息安全管理体系提供要求[17]。采用信息安全管理体系应当是一个组织的一项战略性决策。一个组织的信息安全管理体系的建立和实施[18]受其需要和目标、安全要求、组织应用过程和组织规模和结构[19]的影响。所有的影响因素会随着时间而变化[20]。

信息安全管理体系通过应用风险管理过程保持信息的保密性、完整性和可用性[21-22]，并给予相关利益方[23]风险已得到充分[24]管理的信心。

---

15 SC 27，即 JCT 1/SC 27，信息技术安全技术，是 19 个分技术委员会的其中之一。

16 此处原文也是 prepared。

17 提供要求为：provide requirements for……，ISO/IEC 27001：2005 中的描述为 provide a model for……，为……提供模型。这是一个非常大的变化，ISO/IEC 27001：2005 强调的是模型，是方法论，整篇都是建立在 Plan-Do-Check-Act 的 Deming 环，在引言中也用了大量的篇幅说明什么是过程方法，标准中如何理解过程方法。显然，在 ISO/IEC 27001：2013 已经抛弃了这个思路，本标准首要的目标是紧扣标题，即提供要求。事实上，即使在 ISO/IEC 27001：2005 的应用中，也已经默认该标准的主要任务就是提要求。

18 建立和实施，establishment and implementation，ISO/IEC 27001：2005 中为设计和实施（design and implementation），ISO/IEC 27001：2013 中的描述更宽泛了，建立的过程不仅仅包括设计。如果从后面的因果关系来看的话，应该说描述的更准确了，文中描述的这些因素要影响整个建立过程。

19 原文为：organization's needs and objectives, security requirements, the organizational processes used and the size and structure of the organization。此处描述与 ISO/IEC 27001：2005 稍有变化，不同之处是 the processes employed，修改为 the organizational processes used。两者区别不大，就是指代关系更清楚了一些。

20 本句为新加。这句话比较原则性，用哲学语言讲就是世界是变化的。ISO/IEC 27001：2005 本来有一句很实在的话，反倒被删除了，如下：例如，简单的情况可采用简单的 ISMS 解决方案（e. g. a simple situation requires a simple ISMS solution）。

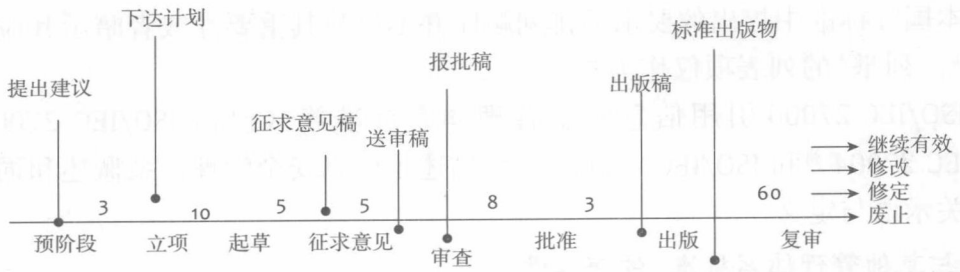
21 保密性、完整性和可用性，对应词汇为 confidentiality、integrity and availability。注意，不是信息安全定义中的 7 个属性，ISO/IEC 27001：2013 和 ISO/IEC 27001：2005 一样，反复被强调的是 3 个属性。另外 4 个属性为：真实性（authenticity）、可核查性（accountability）、不可否认性（non-repudiation）和可靠性（reliability）等。

22 在 ISO/IEC 27001：2013 中对信息安全只强调保密性、完整性和可用性是有其逻辑的，因为 ISO/IEC 27000: 2009 中将其定义为：preservation of confidentiality (2. 9), integrity (2. 25) and availability (2. 7) of information. *NOTE In addition, other properties, such as authenticity (2. 6), accountability (2. 2), non-repudiation (2. 27), and reliability (2. 33) can also be involved.* 注意斜体部分，其他 4 个属性是以“备注”的形式给出来的。但是在 ISO/IEC 27001：2005 中只强调这 3 个属性不太符合逻辑，因为在其术语与定义中引用 ISO/IEC 27002: 2005 将信息安全定义为：preservation of confidentiality, integrity and availability of information; *in addition, other properties, such as authenticity, accountability, non-repudiation, and reliability can also be involved* 。斜体部分讨论这 4 个属性时，是并列关系。

23 相关利益方，interested parties。这是标准中出现比较频繁的术语。

24 此处程度副词用的是 adequately。

流程如下所示：



信息安全管理体系整合[25]在组织流程和整体的管理结构[26]中非常重要，而且在过程、信息系统和控制措施的设计中都要考虑信息安全[27]。按照组织的需要实施信息安全管理体系是本标准所期望的[28]。

本国际标准可用于内部和外部各方评估组织能力是否满足了组织自己的信

25 这里的整合是 integrate，也有一体化的意思，强调最后的一体，但不强调原来的主次之分，都可独成体系。Embed，嵌入、插入，强调主次之分，把不成体系的东西嵌入到成体系的东西上。Align，使整齐、使排成一线，强调两者的校对、校正，之后不一定合二为一。

26 原文为 organization's processes and overall management structure。

27 这句的原文和上一句其实是一起的，It is important that the information security management system is part of and integrated with the organization's processes and overall management structure and that information security is considered in the design of processes, information systems, and controls. 这一句中 and 连接的前后，乍看不是非常连贯，前面是说信息安全整合，就是从组织整体角度去考虑信息安全，后面部分强调的是在几个常见的活动中应该考虑信息安全。其实，还是一致的问题，只是前面说信息安全管理体系，后面则是说广义的信息安全。但是后面三个关键活动（design of processes, information systems, and controls）怎么并列起来的是个疑问，可以这样理解，processes 关系到所有的活动，再密切一些就是 information systems，更关系密切是 controls，这样看，倒是一个逐步细化的描述。

28 按照组织的需要实施 ISMS 是本标准所期望的，原文为：It is expected that an ISMS implementation will be scaled in accordance with the needs of the organization。这句话在 ISO/IEC 27001：2005 中本来放在“简单的情况可采用简单的 ISMS 解决方案”前面，现在转移到这里，但是后面的那句实在话“例如……”被删了。“按照组织的需要实施 ISMS 是本标准所期望的”，这种句式在中文中很不常见，为了与 GB/T 22080—2008 / ISO/IEC 27001：2005 保持一致，我们沿用了这个译法。实际上，这种 It 做形式主语加被动语态的句子可以换种方式表达，或者 expected 的主语直接省略掉，如前一段中，All of these influencing factors are expected to change over time，可以直接理解为：所有的影响因素会随着时间而变化。此外，为了表达得更加客观，在标准和学术论文中会大量使用 It 做形式主语的句式，例如上一句的句式为：It is important that. . . 。

息安全要求[29-30]。

本国际标准中提出的要求的排列顺序并不反映其重要性或者暗示其应用的顺序[31]。列举[32]的列表项仅作为参考。

ISO/IEC 27000 引用信息安全管理体系标准族（包括 ISO/IEC 27003[2]，ISO/IEC 27004[3]和 ISO/IEC 27005[4]）[33] 描述了信息安全管理体系概述和词汇以及相关术语与定义。

0.2 与其他管理体系标准[34]的兼容性[35]

本国际标准应用了 ISO/IEC 导则 第 1 部分附录 SL 中所定义的 high-level structure，identical sub-clause titles，identical text，common terms，and core definitions[36]，联合 ISO Supplement，因此与其他采用附录 SL 的管理体系标准保持了兼容性。

---

29 原文为：This International Standard can be used by internal and external parties to assess the organization's ability to meet the organization's own information security requirements. 同样的意思在 ISO/IEC 27001：2005 中的描述为：This International Standard can be used in order to assess conformance by interested internal and external parties. 注意其中的微妙区别，ISO/IEC 27001：2005 强调了符合性（conformance），或者翻译为一致性，但是 ISO/IEC 27001：2013 中用了 the organization's ability to meet the organization's own information security requirements。应该说这个描述避免了争论，但是其实不利于落地，原因很简单，能力是个过于宽泛的词汇，而且根本不具备可测量性，例如，某管理者说，我们一定要让有能力的员工得到升迁，或者说我们不能让老实人吃亏。这些话基本都沦落为空话，因为怎么是有能力？什么样是老实人？在具体的操作中有太多的解释和理解。一般而言，非常正确无懈可击的话往往都是空话。这与高考的困境是一样的，高考的目的是选拔人才，八股取士固然有很多弊端，但是废除高考，靠能力选拔的逻辑更是馊主意，这种逻辑类似于古代的“举孝廉”，最后的必然结果是由于选拔标准浮动大，考试沦落为“找关系”。本标准也是，这句描述是绝对的退步，断不会改变 ISO/IEC 27001 关注点在“符合性”的现状。至少目前国内而言，诸多问题都是“可操作”远比“理念好”稀缺得多。

30 如上所述，所有过度抽象，应用范围过大的方法或实践都面临操作性不强的问题。控制点与业务流程的整合在理念上毫无疑问是正确的，如何真正落地，可以参考航空安全的案例，例如，起飞前的检查表与起飞的操作流程就很好的融为一体。当然，这包括了多方面的影响因素，例如：Human Factors of Flight-Deck Checklists: The Normal Checklist（NASA Contractor Report 177549），访问 http: //www. nasa. gov/，有大量可以下载的类似参考资料，其中也有许多是专门针对风险管理和信息安全的资料。

31 要求是同等重要的，这在附录 A 中尤其重要，按照标准的描述顺序，很容易理解为按照重要度排列。这个说法在 ISO/IEC 27002: 2005 中也出现过，其实想表达的意思是，所有的要求和控制措施都很重要，排列成现在这个样子就是为了阅读方便。

32 列举用的词汇为 enumerated，可翻译为列举、枚举等。

33 其中［2］［3］［4］是其在参考书目中的顺序编号，ISO/IEC 27000 中对信息安全管理系体标准族做了综述。关于这几个标准较为详细的介绍请参考：谢宗晓编著，《信息安全管理体系实施指南》，中国标准出版社。尤其是 ISO/IEC 27000，其中介绍的较为详细，ISO/IEC 27005 则可以参考本丛书中的《信息安全风险管理》分册。

34 从此处的描述加上本标准的结构，我们可以得知管理体系标准不仅仅指那些采用 PDCA 模型的标准。

35 本小节与 ISO/IEC 27001：2005 相比变化较大。ISO/IEC 27001：2005 中采用的 PDCA 模型，因此特别强调了同样采用 PDCA 模型的 ISO9001: 2000 与 ISO14001: 2004 的整合，甚至附录 C 中还进行了对应。但是 ISO/IEC 27001：2013 中已经完全抛弃了原来的框架，因此，不再强调与这两个标准的整合。ISO/IEC 27001：2013 强调的是由于与 ISO/IEC 导则附录 SL 所定义的通用方法保持了一致而导致的整合可能。

36 此处原文为：high-level structure, identical sub-clause titles, identical text, common terms, and core definitions。

附录 SL 中定义的通用方法对选择一个管理体系满足两个或更多管理体系标准要求的组织是有帮助的。

Information technology — Security techniques — Information security management systems[37-38] — Requirements

1 范围

本国际标准从组织情境[39-40]为建立、实施、保持和持续改进信息安全管理 1

[37] 注意一个细微的变化，在 ISO/IEC 27001：2013 中，没有 ISMS 这个缩写了。当然，这还是一个专用词汇，因为在 ISO/IEC 27000: 2009 pp. 3，*2. 23 information security management system（另起一行）ISMS（另起一行）part of the overall management system (2. 26), based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security (2. 19)* 。在 GB/T 22080—2008 / ISO/IEC 27001：2005 中 information security management system 一般翻译为信息安全管理体系，而 ISMS 直接用缩写，所以在本版本的中文翻译中，就不再有这种情况了。

[38] 但是要注意，在 ISO/IEC 27002: 2013 却还是用的缩写 ISMS，例如：A successful ISMS requires support by all employees in the organization。

[39] 情境，context，有上下文、来龙去脉等含义。这个词汇在中文中并不常用，在英文论文中是常用词汇。有些词汇，例如，rank、context 翻译过来之后就没有原来那么生动了。“情境”还是没有“上下文”这么准确，但是直接用“上下文”又不符合中文的习惯。在 GB/T 22080—20080/ISO/IEC 27001：2005 中，This International Standard specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented ISMS within the context of the organization's overall business risks. 这句的翻译并没有刻意强调 context，而是翻译成：本标准从组织的整体业务风险的角度，为……

[40] 在管理学的研究中，Unit of analysis（分析层次/单元）或 Unit of observed（观察层次/单元）是非常重要的。例如，如果研究问题是组织信息安全管理的有效性的影响因素，那么观察样本就不能仅仅是个体行为，而应该是组织。这时候的 context 绝不仅仅是角度问题，而是真正的“上下文”，就是我们的研究是围绕什么，就是说这些要求是围绕“组织”的，而不是个体、工作组或者其他。分词层次有许多种，常见的有“组织层次（Organizational-level）”、“个体层次（Individual-level）”和“工作组层次（Group-level）”等。

体系规定了要求[41-42]，也包括裁剪[43]符合组织需要的[44]信息安全风险评估和处置的需求[45-46]。本标准规定[47]的要求是通用的，适用于各种类型、规模和特性的组织。组织生成符合本标准时，对于条款 4 到10[48] 的要求不能删减。

---

41 本句原文为：This International Standard **specifies** the requirements for establishing, implementing, maintaining and continually improving an information security management system **within the context of the organization**. 在引言中的描述为：This International Standard has been prepared to **provide** requirements for establishing, implementing, maintaining and continually improving an information security management system. 这一句和引言中的描述比较类似，注意两者的区别。此处用的是 specify，引言中用的是 provide。这里语气比较重，类似于说明书之类的东西，引言中的描述则比较笼统。此外，这里还加了一个限定，就是 within the context of the organization。

42 在 ISO/IEC 27001：2005 描述是这样的：This International Standard specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented ISMS **within the context of the organization's overall business risks**. 注意 ISO/IEC 27001：2013 中把对 overall business risk 的强调分开了。

43 裁剪，tailor。这里“裁剪”一词用在了风险评估和处置，而不是用在 ISO/IEC 27001。但是，到底什么是可以裁剪的，风险评估和处置流程？风险？还是 ISO/IEC 27001？首先，风险是不能被裁剪的，所有的风险都要有相应的处理，这是原则。一般“要求类”的是可以裁剪的，例如 ISO/IEC 27001，因此其中都有专门说明条款描述裁剪要求。风险评估和处置的流程是环环相扣的，删掉任何一个环节都可能导致下一个步骤无法实施，例如，不做资产识别当然无从识别资产面临的威胁和自身的脆弱性。虽然风险评估有诸多方法，但是基本的六因素（资产、威胁、脆弱性、控制措施、可能性、影响）是不可裁剪的。

44 这里把裁剪限定为适合组织的需求（the needs of the organization），意义不大。可能是为了持续的强调不要设计“放之四海而皆准”的管理体系或风险评估。这种描述和前面的讨论是一样的，理念是完全正确的，但是并没有可操作的流程来保证“适合组织的需求”。如同“因材施教”，是个非常好的理念，但是根本没有可操作的方法，怎么判断学生是什么材料，这需要非常强大的师资保障，如果过度强调这个理念，不但不会提高教育质量，反而落入没有标准、无法证伪的诡辩状态。当然，出现这种情况的原因在于毫无益处的吹毛求疵，这些争论往往抓住一点，而不考虑可操作性，站在道德正确的角度去讨论问题。最后博弈的结果就是公开言论和公开文档都先占据道德正确的位置，之后再在安全的范围内解决可操作性问题。因此，我们在理解标准时，在满足符合性的前提下，应该根据自己组织的实际，不要机械的理解，裁剪成自己想要的样子。

45 需求，need，要求，requirement。

46 本句原文为 This International Standard also includes requirements for the assessment and treatment of information security risks tailored to the needs of the organization。注意，这里主语 This International Standard 是重复出现的，按照常见的句式，加上前面的句子，可能会这样：This International Standard specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organization, *also including requirements for the assessment and treatment of information security risks tailored to the needs of the organization*。如果改成伴随状语可能就成了强调主句，没有并列的含义了。

47 上一句的规定是 specify，这里的规定是 set out，有陈述、罗列的意思。这两个词沿用了 GB/T 22080—2008 / ISO/IEC 27001：2005 中的翻译。

48 英文原文中加了下划线，此处保持统一。

2 规范性引用文件[49]

下列文件中的条款通过本标准的引用而成为本标准的条款。凡是注日期的引用文件，其随后所有的修改单（不包括勘误的内容）或修订版均不适用于本标准，然而，鼓励本标准达成协议的各方面研究是否可适用这些文件的最新版本。凡是不注日期的引用文件，其最新版本适用于本标准。 1

ISO/IEC 27000[50]，Information technology — Security techniques — Information security management systems — Overview and vocabulary

3 术语和定义

根据本文档的目的，术语和定义在 ISO/IEC 27000[51] 中给出。 1

4 组织情境[52]

4.1 理解组织及其情境[53]

组织应[54]确定与其目标相关和影响信息安全管理体系获得预期结果[55]内部与外部的要点[56]。

---

49 这段客套话，表述略有区别，ISO/IEC 27001：2013: **The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application.** For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies. 在 ISO/IEC 27001：2005 描述如下：**The following referenced documents are indispensable for the application of this document.** For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies. 国家标准的描述都是一致的，显然与英文不尽相同。在这个形式问题上，国家标准比国际标准更规范。

50 这个是没有标注年号的标准。目前这个标准有中文版本：GB/T 29246—2012 / ISO/IEC 27000: 2009 信息技术 安全技术 信息安全管理体系 概述和词汇。

51 可以购买该标准的中文版，或者参考：谢宗晓编著，《信息安全管理体系实施指南》，中国标准出版社。

52 这里所说讨论的情境（context），倒是有环境的含义了。此处原文为 context of the organization，即组织的情境、环境或上下文。这部分在 ISO/IEC 27001：2005 中也有，但是没这么强调出来，这些内容在 ISO/IEC 27003 中有比较详细的介绍。

53 其实这里比较通俗的讲就是：了解组织和组织情况。但是不是很书面，因为 context 在英文里面也是书面用语，日常用语中不多见。

54 Shall，应。

55 预期结果，Intended outcome (s)。

56 要点，原文为 issues，有重要问题的含义。注意，ISO/IEC 27001：2005 中没有这个词汇，即使出现与此处的含义也完全不同。例如，4.3.2 a）approve documents for adequacy prior to issue; 这里的 issue 指的是文件发布。