ISO27001:2013 新版解读精要 V1.2

1. 综述

ISO/IEC 27001（信息安全管理体系国际标准）是全球范围内发展最为快速的管理体系标准之一，2005 年发布迄今在全球 100 多个国家中已签发 17,500 多张证书，证书数量保持每年两位数增长。信息安全最佳实践标准 ISO/IEC 27002 为该 ISO27001 的使用提供了必要的支持。这两个标准均通过国际标准化组织（该组织的成员包括 47 个国家标准机构）达成共识的方式而制定。

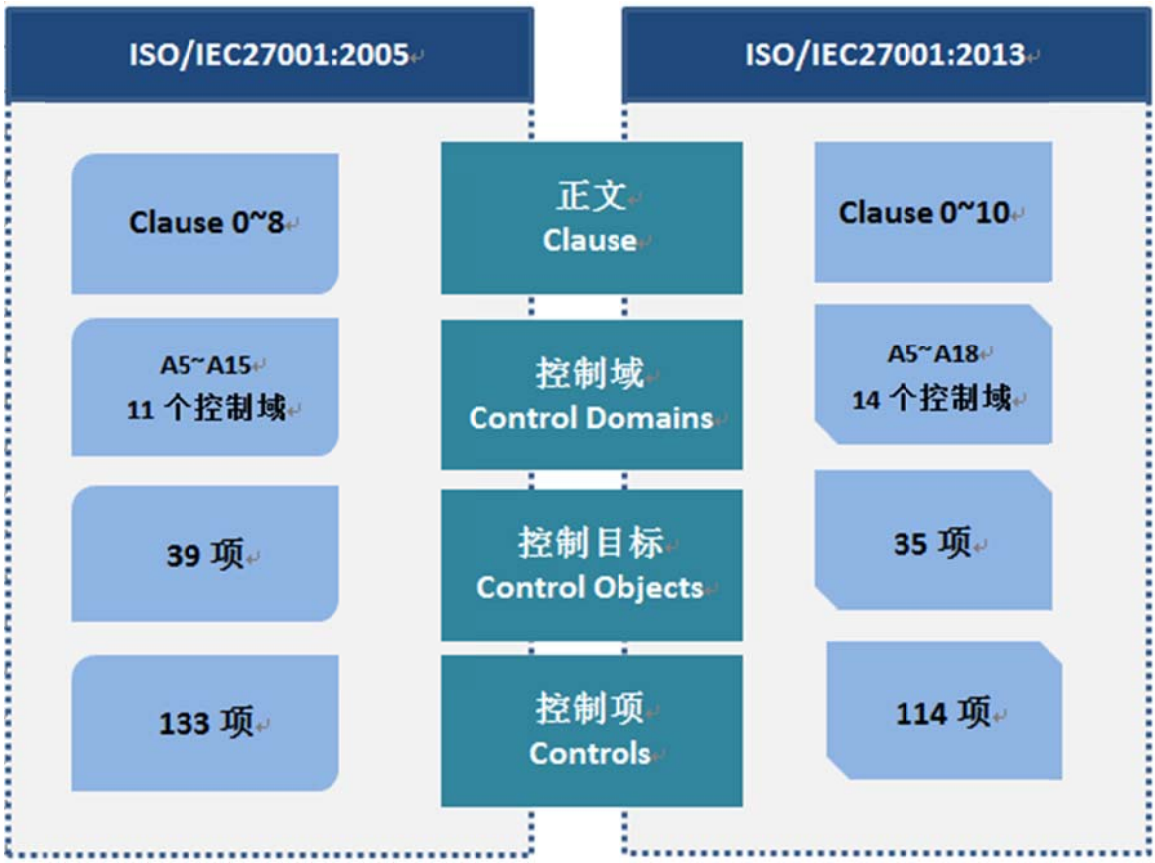
信息安全管理体系国际标准新版 BS ISO/IEC 27001:2013 与 BS ISO/IEC 27002:2013 在 2013 年 10 月已正式发布。相关的几个标准，包括 27003,27004,27005 亦正在修订中。

ISO27001:2013 版（以下简称新版）看到了许多可喜的变化，包括大幅修改了结构，以适应未来管理体系标准中使用的新的架构，简化与其他管理体系的整合；删除了旧版中重复、不适用的内容，**结构上更清晰，内容上更精炼，逻辑上更严谨**，并且在管理要求的定义上变得更具弹性，**给予组织更灵活的实施空间**。值得信息安全从业人员去学习、实践。

本文为“ISO27000 标准族新版解读系列”的第二篇，笔者从 ISMS 项目实施及咨询顾问的视角，和大家一起来研究一下新版标准的变化以及如何将现有体系向新版转换；由于 ISO27001:2013 推出不久，笔者接触时间有限，文中如有不当之处，敬请读者指正。(笔者的 QQ 及邮箱为 46040336@QQ.COM)。

2. 标准新版与旧版的差异

2.1 整体变化



注：图 1, ISO 27001:2005 有 11 个域、133 项控制措施，新版调整为 14 个域、114 项控制措施。

2.2 正文的变化

a) 编写架构

新版编写终于想到采用了标准化的ISO Annex SL通用架构(同ISO22301)，采用此架构的好处在于可将各标准的要求，以统一的架构进行描述。Annex SL架构考虑了管理体系间的兼容性，有利于不同管理体系间进行接轨、整合。

b) PDCA 与持续改进

PDCA 是旧版标准中强调在体系建设及实施过程使用的过程方法，新版标准中虽已不见旧版 0.2 中大段对过程方法 PDCA 模型的描述，而仅用正文 10.2 中的一句“持续改进”一言概之，但从标准编写的目录结构上看，新版调整为 Planning-Support-Operation-Performance evaluation-Improvement，架构上其实是更趋 PDCA 了。至于为什么在 Planning 与 Operation 间插一个 Support，而不是把 Support 的内容简单纳入到 Leadership 和 Planning 以保持框架的简洁，个人是不大理解。或许这正是 BSI/ISO 的特色吧。

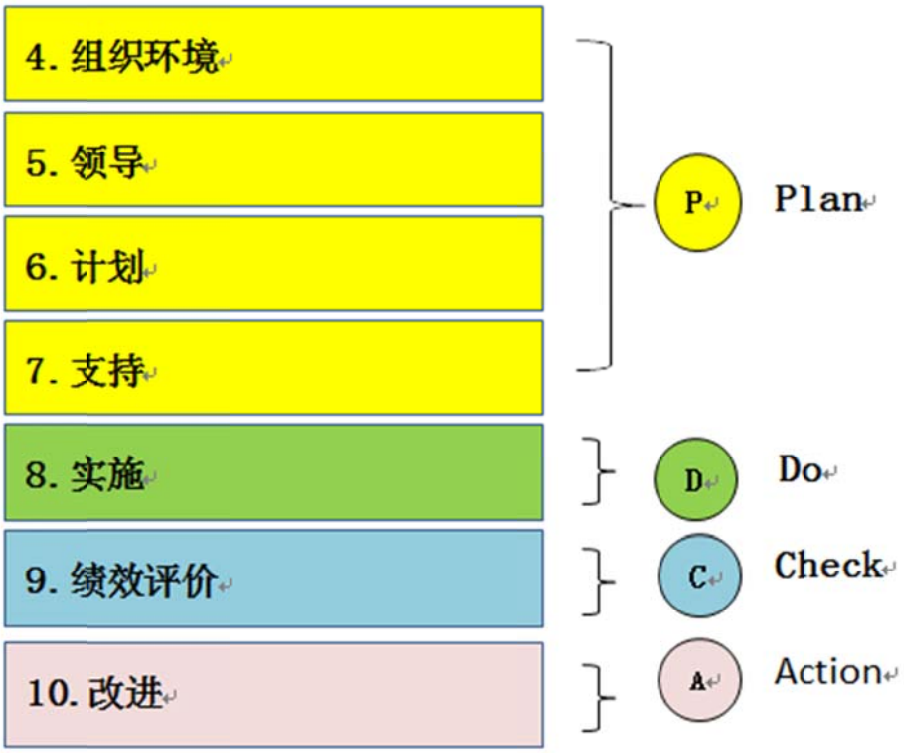


图 2 ISO27001:2013 文件结构与 PDCA

c) 风险评估方法

新版简化了对风险识别、风险分析的要求的描述，不再强调对资产责任人、威胁、脆弱性这类风险要素进行识别，这意味着组织可选用的风险评估的方法可以更加宽泛和灵活，组织可以根据自身的情况，选用简化的风险评估方法，或继续使用现行的方法（如果是合理的话）。新版中依然未明确评估周期（6.1.2）。（**老李点评**：实操层面，当前风险评估可参照的标准有 ISO31000，GBT20984，ISO27005，但此类标准都有各自的问题，包括逻辑性、可操作性等，实际应用中要有所取舍或综合运用）。

d) 风险属主

6.1.2 识别风险中“风险属主”替代了“资产责任人”。要注意的是资产所有者未必是风险属主，风险属主可以是资产的管理者、该风险管控的负责人（如部门领导）、或组织领导者等。（6.1.2）

e) 风险处置

组织可自行选择所需控制，而不仅限于从标准附录 A 中选择；明确了风险处置计划和残余风险需要风险属主审批。（6.1.3）。注意，RTP 中的风险属主可能是一个人、多个人或一个代表，也包括非 IT 人员。

f) RA 参考标准

明确信息安全风险评估和风险处置过程与 ISO31000:2009 相一致。备注中的风险评估参考文件从 ISO/IEC TR 13335-3，《信息技术-IT 安全管理指南-IT 安全管理技术》变成了 ISO31000:2009。（6.1.3）

g) 信息安全目标

对信息安全目标及实现的要求独立为 6.2，6.2 中对目标的制定、沟通、测量、时间计划、更新、职责等的要求比旧版更为明确。6.2 中提到“The organization shall establish information security objectives at relevant functions and levels.”。

h) 文档要求

旧版中 4.2 Documentation requirements 变成了新版的 7.5 Documentation information ，对于文件“编制和更新”的要求独立出来。旧版的 4.3.2 文件控制与 4.3.3 记录控制，合并为新版的“文件控制”。此块要求变得精简，架构上更灵活，通用性强。而旧版 4.3.1 中对于强制性文件的要求在新版中不再有。

注：新版中的Document information，指的可能是document（文件），也可能是record（记录），其目的是为了证明过程已经实施，表明体系的有效性。

新版中关于文档控制的要求基本不变。但要留意新版对保留过程文档信息 Documentation information 的要求几乎散布了标准各个章节，包括：

4.3 Scope of the ISMS 5.2 Information security policy 6.1.2 Information security risk assessment process 6.1.3 Information security risk treatment process 6.1.3 d) Statement of Applicability 6.2 Information security objectives 7.2 d) Evidence of competence 7.5.1 b) Documented information determined by the organization as being necessary for the effectiveness of the ISMS 8.1 Operational planning and control 8.2 Results of the information security risk assessments	8.3 Results of the information security risk treatment 9.1 Evidence of the monitoring and measurement results 9.2 g) Evidence of the audit programme(s) and the audit results 9.3 Evidence of the results of management reviews 10.1 f) Evidence of the nature of the nonconformities and any subsequent actions taken 10.1 g) Evidence of the results of any corrective action

对document的要求在以上标准条款中都有重复，个人觉得行文比较罗嗦，当然也可理解为BSI/ISO比之前更加重视对管理文档化的要求。

老李点评：除了正文中的Documentation information的（通用）要求外，你还可以看到附录A的多项控制措

施中也提到documented即文件化的要求，可以理解为标准对于文件的要求在整体上放宽了但在局部却变得更严了？大家知道管理制度文件并不是越多越好的，但问题来了，哪些文件是要写的？哪些是可以不写的？编写文件的重点或颗粒度该如何把握？这就要看各人的经验和把握了。老李认为最好的作法的是“编写文件，但要忘记文件”，什么意思呢，其实大家知道日常工作中是没有人是读着文件做事的，所有安全管理要求和控制措施应融合到已有的工作内容中去，并实现管理的流程化和电子化，达到管理制度从“有形”到“无形”，这才是安全落地的终极目标，否则相关的问题是很多的，典型如“两张皮”等。关于此项的探讨敬请期待老李本系列文章四，《信息安全管理体系落地的最佳实践》。

i) 外包安全

明确了外包涉及的风险应受管控（这个来得有点晚，但也算跟上了潮流）。对应的是附录 A.15 供应商关系中的 5 项参考控制措施。（8.1）

j) 测量与绩效评价

旧版 4.2.2 控制措施有效性测量和 4.2.3 Monitor and review the ISMS 在新版中进化成了第 9 章 Performance evaluation。绩效评价的要求包括：监视、测量、分析、评价；并以 5W1H（测什么？如何测？何时测？何时分析？谁来分析？谁负责评价？）的方式提出了监视和测量的要求。相比旧版相关要求显得逻辑更清晰，要求更明确，档次上也更高？

k) 管理评审

新版中简化了管理评审程序要求，将管理评审原先要求的 9 大输入 5 大输出调整为新版的 6 大审查项目。而评审周期从“每年至少一次”变为**“按计划定期执行”。**(9.3)

l) 持续改进

取消了旧版8.3预防性控制的要求，因风险评估与处置本身就是一套系统性的预防性控制方法。新版增加了“应评审已执行纠正措施的有效性”，同时要求应确认“是否有相似的不符合项存在或可能发生”。（正文条款10）。这可看到给体系的内部审核人员提出了更明确的工作要求。

m) 从标准正文中删除的要求

旧版条款	要求	老李解读
4.2.1(g)	The control objectives and controls from Annex A shall be selected as part of this process as suitable to cover these requirements.	新版中明确组织可选择任何适用的控制，包括但不限于附录A的内容。
4.2.1(i)	Obtain management authorization to implement and operate the ISMS.	旧版在风险评估条款里谈这个，有点多余，该删
4.2.3(a)(1)	promptly detect errors in the results of processing;	4.2.3为 监控和评审ISMS。此项要求显得难以操作/很莫名
4.2.3(a)(2)	promptly identify attempted and successful security breaches and incidents;	4.2.3为监控和评审ISMS。此项要求太具体/不适当
4.2.3(a)(4)	help detect security events and thereby prevent security incidents by the use of indicators; and	4.2.3为监控和评审ISMS。此项要求太具体/不适当
4.2.3(a)(5)	determine whether the actions taken to resolve a breach of security were effective.	4.2.3为监控和评审ISMS。此项要求太具体/不适当
4.2.3(h)	Record actions and events that could have an impact on	4.2.3为监控和评审ISMS。

旧版条款	要求	老李解读
	the effectiveness or performance of the ISMS (see 4.3.3).	此项要求太具体/不适当
4.3.1	Documentation shall include records of management decisions, ensure that actions are traceable to management decisions and policies, and the recorded results are reproducible. 文件应包括管理层决策的记录，确保措施可以追溯到管理层决策和策略，确保记录结果是可重复；	旧版：记录管理要求和管理决策与可重现？这是哪个和哪个啊？ 注：4.3.1为 总则
4.3.1	It is important to be able to demonstrate the relationship from the selected controls back to the results of the risk assessment and risk treatment process, and subsequently back to the ISMS policy and objectives. 重要的是能够证明所选择的控制措施与风险评估和风险处理过程的结果之间的关系，以及追溯到信息安全管理策略和目标。	在新版正文的风险评估中有要求。旧版4.3“文件控制”中此项要求自然删去。
4.3.1(c)	procedures and controls in support of the ISMS;	由新版7.5.1A取代
4.3.2	A documented procedure shall be established to define the management actions needed to:	由新版7.5.3取代
4.3.3	The controls needed for the identification, storage, protection, retrieval, retention time and disposition of records shall be documented and implemented.	原记录控制转到新版的7.5.3，统一为文件控制
4.3.3	and of all occurrences of significant security incidents related to the ISMS.	原记录控制转到新版的7.5.3，统一为文件控制
5.2.1(b)	ensure that information security procedures support the business requirements;	罗嗦了
5.2.1(d)	maintain adequate security by correct application of all implemented controls;	多余
6(d)	The responsibilities and requirements for planning and conducting audits, and for reporting results and maintaining records (see 4.3.3) shall be defined in a documented procedure.	太罗嗦、多余
8.3	The documented procedure for preventive action shall define requirements for:	新版中不再采用preventive action提法
8.3(e)	The priority of preventive actions shall be determined based on the results of the risk assessment.	新版中不再采用preventive action提法

2.3 附录 A 的变化

综述：控制措施的设置上，ISO27001:2013保留了多数老的控制项，但对旧版中相近或类似的项进行了整合，删除了部分过时的或太过于具体的控制措施。针对这几年信息技术的发展，将移动设备管理列入了控制项（A.6.2.1 Mobile device policy）。

域的结构：在新版中，“加密控制”和“供应商管理”则成为独立的领域。旧版中的（Communications & Operations）域，拆分成（Operations security）和（Communications security）两个域。

老李点评：操作安全和通信安全的管理领域相对独立，各自的内容也不少，旧版标准中混在一起谈本来就

不合适，我们在ISMS项目实施过程每到此处都觉得挺别扭，8年后的今天标准才纠正了此类问题。

a） **新增控制措施**

编号	控制项	说明	老李解读
A.6.1.5	Information security in project management项目管理中的信息安全	Information security shall be addressed in project management, regardless of the type of project. 无论何种项目，均应考虑安全问题。	在项目早期就应考虑项目的安全风险，并进行控制；特别是外包项目，合作项目。信息安全应包含在项目管理方法中。要注意此控制项并非独立的控制项，落实上与人员安全、访问控制、供应商关系内的各控制项紧密相关。
A.12.6.2	Restrictions on software installation 限制软件安装	Rules governing the installation of software by users shall be established and implemented. 应建立和实施用户软件安装管理规则	一为终端安全；二为知识产权考虑。此项控制加进来很好，但在国内落实普遍会遇上困难。。。
A.14.2.1	Secure development policy 开发的安全策略	Rules for the development of software and systems shall be established and applied to developments within the organization. 应建立和应用组织内部的软件和系统开发准则。	新版要求建立适用于软件开发生命周期的安全策略（落实上可单列，也可包含在整个开发策略中）；其要求也与软件开发的项目管理（安全）相关。如从文件编写考虑，此文件可包含A.14.2中大部分控制要求。
A.14.2.5	Secure system engineering principles 安全系统工程原则	Principles for engineering secure systems shall be established, documented, maintained and applied to any information system development efforts. 基于安全工程原则的信息系统工程原则应被建立、文件化、应用于内部信息系统工程活动。	与**A.14.2.1**开发安全策略不同的是，此项控制更技术、更细节，可包含旧版A.12.2的相关要求（如输入输出控制、身份鉴别、安全会话等）。此控制项可支撑A.14.2.1落地。
A.14.2.6	Secure development environment保护开发环境	Organizations shall establish and appropriately protect secure development environment for system development and integration efforts that cover the entire system development lifecycle. 组织应建立并适当保护系统开发和集成工作的安全开发环境，覆盖整个系统开发生命周期。	从环境控制角度关注开发安全保护。包括数据安全、访问控制、环境分离、异地备份等要求，比旧版更全面，旧版标准仅在A.10.1.4中提到开发环境分离的要求。本控制项提出每个系统的开发应单独评估其风险。
A.14.2.8	System security testing系统安全测试	Testing of security functionality shall be carried out during development. 在开发过程中应进行安全功能测试	新系统或更新的系统在开发过程中均需要全面的测试验证，如在一定条件下测试输

编号	控制项	说明	老李解读
			入和期望的输出。测试应包括内部测试及独立验收测试。测试尝试要系统重要性而定！此控制有利于开发的安全问题要及早发现，及时解决。
A.14.2.9	System acceptance testing 系统验收测试	对于新建信息系统和新版本升级系统，应建立验收测试方案和相关准则。	系统验收测试应包括信息安全要求测试（见14.1.1 和14.1.2）并遵循系统安全开发策略（见14.2.1），宜进行单元测试和系统集成测试。可使用代码分析工具及漏扫。
A.15.1.1	Information security policy for supplier relationships 供应商关系的信息安全策略	Information security requirements for mitigating the risks associated with supplier access to organization’s assets shall be documented. 为降低供应商访问组织资产带来的风险，宜与供应商协商并记录相关信息安全要求。	此项具体控制要求较多，也很有必要，编写文件/实施控制时应参见ISO27002:2013；典型的就是安全协议的签订了。
A.15.1.3	Information and communication technology supply chain 信息和通信技术的供应链	Agreements with suppliers shall include requirements to address the information security risks associated with information and communications technology services and product supply chain. 供应商协议应包括信息和通信技术服务以及产品供应链相关信息安全风险处理的要求。	新版提出了供应链安全的概念，至于什么是IT的供应链，与供应商的协议应包含什么要求，应参见27002。这是一个比较“高大上”的控制项，涉及当今的云计算服务等。具体落实时应细化和考虑操作性。
A.16.1.4	Assessment and decision on information security events评估和决策信息安全事态	Information security events shall be assessed and it shall be decided if they are to be classified as information security incidents. 信息安全事态应被评估，并且确定是否划分成信息安全事件。	为安全事件处理中新增的评估步骤，与A.16.1.2相关；信息安全事态：信息安全威胁的行为已经发生，可能造成负面影响。 信息安全事件：信息安全威胁的行为已经发生，且已经造成负面影响。
A.16.1.5	Response to information security incidents 信息安全事件的响应	Information security incidents shall be responded to in accordance with the documented procedures. 按文件化的程序响应	强调安全事件响应的规范性、程序化。替代旧版A.13.2中多项控制。
A.17.2.1	Availability of information processing	Information processing facilities shall be implemented with redundancy sufficient to meet availability	直接响应CIA三性中“可用性”的要求，算是一个必要的补充吧。

编号	控制项	说明	老李解读
	facilities信息处理设施的可用性	requirements.	

老李点评：主要新增的控制为项目管理安全和供应商安全管理，应重点关注，其他的多为优化及补充。

b） 新版中删除的控制措施

编号	控制措施	删除原因（老李解读）
A.6.1.1	Management commitment to information security 信息安全管理承诺	新版标准正文5领导已包含此要求，显然此项放在正文中比较合适
A.6.1.2	Information security coordination 信息安全协作	新版标准正文5领导已包含相关要求，显然此项放在正文中比较合适
A.6.1.4	Authorization process for information processing facilities 信息处理设施授权过程	主要在新版A.8.1.3资产的合理使用中体现。
A.6.2.1	Identification of risks related to external parties 识别外部组织风险	旧版此项控制同时包括风险评估及访问控制的要求；旧版的A6.2已整个取消，由新版的正文及A.15.1等取代。
A.6.2.2	Addressing security when dealing with customers 当与客户接触时强调安全	原要求有点多余。客户属于外部方的一种，与其接触时应受访问控制等所有适用的要求管控。
A.10.7.4	Security of system documentation 系统文档安全	定义狭窄，相关相要求已包含在其他控制中
10.2.1	Service delivery 服务交付	有点多余，纳入新版A.15.2.1
A.10.8.5	Business Information Systems 业务信息系统	多余。原要求已涉及所有控制要求。
A.10.9.1	电子商务 Electronic commerce	在新版中在合并控制项后取消
10.10.2	监视系统的使用 Monitoring system use	原要求为文件化操作程序与日志管理的集合体，定位不准。相关要求在新版A.12.1.1及A.12.4.1中重定义。
10.10.5	Fault logging错误日志	旧版此项要求太局限；统一纳入新版的A.12.4.1 事件日志
A.11.4.2	User authentication for external connections外部连接的用户鉴别	太具体/不合适，其要求由新版A.9.1，A.9.2的相关控制项体现。
A.11.4.3	Equipment identification in networks 网络上的设备识别	太具体/不合适。原文与指网络设备接入控制相关
A.11.4.4	Remote Diagnostic and configuration port protection 远程诊断和配置端口的保护	太具体/不合适，内容由新版A.13.1.1涵盖
A.11.4.6	Network Connection control 网络连接控制	太具体/不合适，内容由新版A.13.1.1涵盖
A.11.4.7	Network routing control 网络路由控制	太具体/不合适，内容由新版A.13.1.1涵盖
A.11.6.2	Sensitive system isolation 敏感系统隔离	部分已体现在A.13.1.3网络隔离中，其他相关要求由物理安全等体现
A.12.2.1	Input data validation 输入数据确认	太过具体，已纳入新版 A.14.2.5 安全系

编号	控制措施	删除原因（老李解读）
		统工程原则中考虑，早该删
A.12.2.2	Control of internal processing	太过具体，已纳入新版 A.14.2.5 安全系统工程原则中考虑，早该删
A.12.2.3	Message integrity 消息完整性	太过具体，已纳入新版 A.14.2.5 安全系统工程原则中考虑，早该删
A.12.2.4	Output data validation 输出数据确认	太过具体，已纳入新版 A.14.2.5 安全系统工程原则中考虑，早该删
A.12.5.4	Information leakage 信息泄露	原要求为应防止信息泄露的可能性。
A.15.1.5	Prevention of misuse of information processing facilities 防止滥用信息处理设施	已体现在“资产合理使用、访问控制、文档化操作”等控制中。旧版放在“符合性”里显得奇怪。（听说此项要求来自英国法律？）
A.14.1.2	业务连续性和风险评估 “应识别能导致业务过程中断的事件，及事件发生的可能性、中断的影响及信息安全后果； ”	同属风险评估，已在新版标准正文风险评估的要求中体现
A.14.1.4	业务连续性计划框架	包含在新版“A.17.1.1规划信息安全的连续性”中
A.15.3.2	Protection of information systems audit tools 保护信息系统审计工具	旧版原意是防止对审计工具的误用或损坏。其实显得罗嗦/重复了，审计工具作为软件资产的一种，已受访问控制及其他措施的管控。

老李点评：被删的三大原因，1 重复啰嗦，2 过于技术细节，3 定位/定义模糊

c） 合并/移位的控制措施

ISO27001:2005	ISO27001:2013	调整原因（老李解读）
A.10.10.1, Audit logging, A.10.10.2,Monitoring of system use, A.10.10.5, Fault logging	A.12.4.1, Event logging.事件日志	三合一了，精炼了点。旧版A.10.10.2和A.10.10.5和A.10中其他控制项有重复。
A.6.1.8 信息安全的独立评审	A.18.2.1 信息安全的独立评审	从旧版“信息安全组织”移到新版的“符合性”，显然更为合适。
A.10.1.3，职责分离	A.6.1.2 职责分离	从原归属的 A.10 通讯与操作管理，转移到新版的 A.6.1 内部组织，显然分类更为恰当。
A.6.1.3信息安全职责的分配 A.8.1.1 角色和职责	A.6.1.1信息安全的角色和职责	二合一是必须的。看到这里你会发现**旧版标准实在有太多冗赘的地方了**。至于“信息安全的角色和职责”，新版中放在 A.6 信息安全组织或 A.7 人力资源安全中我觉得都可以，最终新版选择放在了 A.6，类似的还有 A.6.1.2 职责分离。
A.11.5.1 安全登录程序	A.9.4.2安全登录程序	旧版A.11.5.5 会话超时和A.11.5.6

ISO27001:2005	ISO27001:2013	调整原因（老李解读）
A.11.5.5 会话超时 A.11.5.6 联机时间限定		联机时间限定显得过于技术/过于细节，使得原A.11.5不够精炼。**冗赘！**
A.10.9.1电子商务 A.10.9.3公共可用信息	A.14.1.2公共网络应用服务的安全	二合一了。电子商务也是公共在线服务的一种。
A.11.4.4 Remote Diagnostic and configuration port protection 远程诊断和配置端口的保护 A.11.4.6 Network Connection control 网络连接控制 A.11.4.7 Network routing control 网络路由控制	A.13.1.1 网络控制	三合一了。旧版的几个控制项过于具体/松散，看得出旧版的作者们对技术的分类、重要性把控不准。
A.12.2.1 输入数据验证 A.12.2.2 内部处理控制 A.12.2.3 消息完整性 A.12.2.4 输出数据验证	A.14.2.5安全系统的工程原则	对旧版分散的开发安全技术细节要求进行了整合，抽象为工程原则，这才像个标准的样子啊！

老李提示：读者如想详细研究标准旧版与新版中控制项的 MAPPING，请阅读 BSI 的《ISO27001-mapping-guide-UK-EN》。
不过 BSI 的这个文件中存在个别错漏，已在本文中纠正了。

d) 其他有关域的调整

旧版中“A.12.2应用中的正确处理”整个删除；而原A.12.3的内容不变，但独立为新版的“A10.加密控制”，成为仅包含两个控制项的最小的一个域。

相比旧版中“A.12信息系统获取、开发和维护”，新版的“A.14信息系统获取、开发与维护”是改进很大的一个域，新版A.14中的控制项的设置逻辑性更强（你也可以说旧版A.12的逻辑太乱），控制项的设定上也更加精简适用。

旧版“A.14业务连续性管理（ Business continuity management）”更名为“A.17 业务连续性管理中的信息安全”，A.17从域的名称及内容上专注/回归“业务连续性管理中的信息安全”，**相比旧版的“业务连续性管理”，从定位与表述上无疑更为恰当。**

3. 如何向新版转换

ISO 要求的证书转换期为国际标准发布后 18~24 个月，笔者建议已取得旧版认证的组织在 2014-2015 上半年可提前做好转换准备，而计划在 2015 年建设 ISMS 并取得证书的组织可考虑按新版标准要求进行建设。
组织如果要从旧版转换到新版，难度并不太大，要做的典型工作包括：

- 调整文件（一级如文件手册、策略、SOA、目标等，二级文件包括开发安全、操作安全、风险评估等）
- 调整风险评估工具（必要时）
- 调整测量、绩效的相关工具（必要时）
- 其他更高效的方法：请咨询我。或参阅老李的下文《ISO27001:2013 转换指南》(构思中)

4. 总结

ISO27001:2005 版中存的许多问题是明显的，当中有些问题在今天看来显得有些**低级**，也给组织依照标准建设 ISMS 带来了许多困扰（绝大数咨询公司实施 ISMS 项目时也只能将错就错）。相对旧版，ISO27001:2013 的改进是相当明显的，虽然这些改进有些姗姗来迟（BSI/ISO 自己的 PDCA 循环太慢了！）；但不管怎么说，better late than never（亡羊补牢—未为晚矣）。

对于新建管理体系的组织来说，参照新版标准建设 ISMS，由于风险评估过程、控制项要求基于文件得到简化，整体上应该是更容易实现，这对标准的实施及推广无疑是一个利好。总而言之，ISO27001:2013 是一个相当值得升级的版本。

对于国内众多已经通过 ISO27001:2005/GBT22080 认证的组织来说，为了顺利实现标准新版转换，笔者建议。。。。暂时没有太多建议，阅读理解好标准和老李飞刀系列文章就是个好开始！老李近期研究方向：IS27001 新版标准族，信息安全管理平台化，体系一体化整合。读者在体系建设与落地过程当中有任何问题或需求，可与老李联系，QQ/微信 46040336。欢迎加入网上最专业的 ISMS 探讨群：210674629，接头暗号“飞刀”。

5. 附录

5.1 标准新词(概念)

词汇	解释
Context of the organization 组织环境	组织的内部因素与外部因素，此类因素会影响组织完成既定的目标。“所有类型和规模的组织都面临内部和外部因素的影响，使得它不能确定是否及何时实现其目标”（参考 ISO31000：2009 5.3）
Interested parties 相关方	（4.2）. 代替原“利益相关者 stakeholders”
Leadership 领导	领导层，领导力。
Risk owner (6.1.2)风险属主	对风险管理持有权力和责任的个人或实体(ISO31000)
Documented information 文件化信息	各级文件及其实施记录

5.2 全球前十大取得 ISO 27001 认证国家

名次	国家名称	证照数量
1	日本	7,199
2	英国	1,701
3	印度	1,600
4	中国	1,490
5	罗马尼亚	866
6	台湾	855
7	西班牙	805
8	意大利	495
9	德国	488
10	美国	415

备注：截止 2012 年底，全球总共有 19,577 个组织取得 ISO 27001：2005 安全认证，仅在 2012 年发出的证书就高达 2,222 张，比 2011 年成长 13%。

数据源：ISO 国际标准化组织，2013 年 11 月。此数据不包含国内这几年通过 GBT22080 认证的组织，这个数字不会少啊，亲。

我们提倡：“工匠精神（Craftsman’s spirit）。是指工匠对自己的产品精雕细琢，精益求精的精神理念。工匠们喜欢不断雕琢自己的产品，不断改善自己的工艺，享受着产品在双手中升华的过程。工匠精神的目标是打造本行业最优质的产品，其他同行无法匹敌的卓越产品。”

