

# ISO27001:2013

## 新版信息安全管理体系标准变化精解





- 关于标准 —— 基本情况
- 关于新版 —— 内容精解
- 关于换证 —— 解决方案

# ISO27001:2005改版ISO27001:2013

## 改版背景

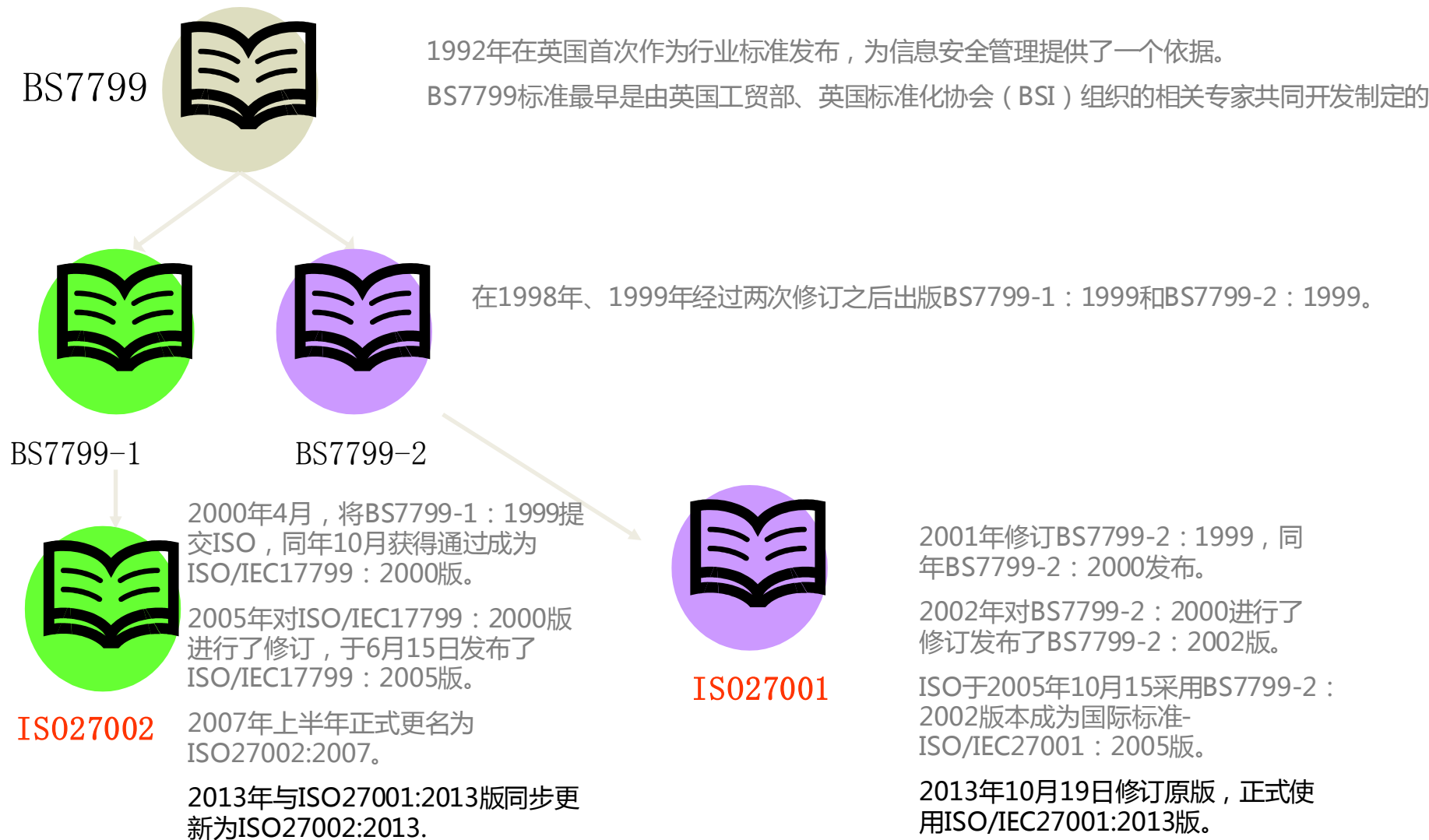
现版的信息安全管理体系ISO27001:2005标准已经使用了8年，日前ISO组织（国际标准化组织）终于将新版ISO27001:2013DIS版（国际标准草案 Draft International Standard）草稿向公众开放并征求意见，预计在今年6-7月会发布DIS最终版。ISO组织公布的正式版本的颁布时间为2013年10月19日。

## 改版影响

在新版公布后的18至24个月内是认证转换缓冲期，即原有已取得ISO27001证书的企业最迟需要在2015年10月19日前转换到新版标准。



# ISO27001的历史发展



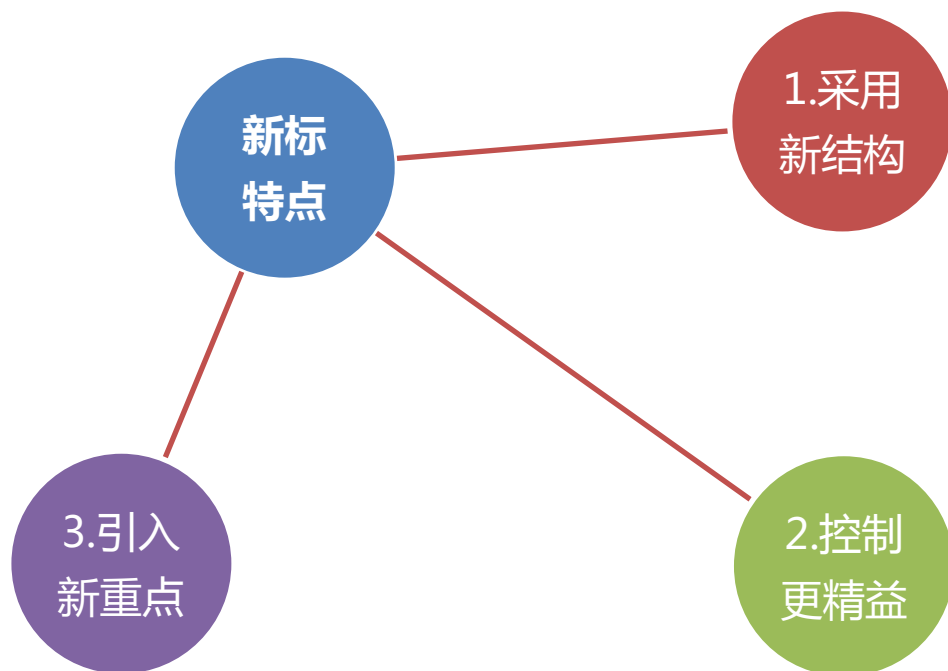
# ISO27000标准家族

序号	标准编号	标准名称	现行状态	序号	标准编号	标准名称	现行状态
1	ISO27000	信息技术 – 安全技术 - 信息安全管理体系 - 概论及术语	2009年出版	16	ISO/IEC 27032	信息技术 – 安全技术 – 网络空间安全指南	委员会草案
2	ISO27001	信息技术 – 安全技术 - 信息安全管理体系 - 要求	2013年改版	17	ISO/IEC 27033-1	信息技术 – 安全技术 – 网络安全 – 第1部分：概述和概念	2009年出版
3	ISO/IEC 27002	信息技术 – 安全技术 - 信息安全管理 - 为规范	2013年改版	18	ISO/IEC 27033-2	信息技术 – 安全技术 – 网络安全 – 第2部分：设计和实施网络安全指南	最终委员会草案
4	ISO/IEC 27003	信息技术 – 安全技术 - 信息安全管理体系 - 实施指南	2010年出版	19	ISO/IEC 27033-3	信息技术 – 安全技术 – 网络安全 – 第3部分：参考网络情境 – 威胁、设计技术和控制活动	最终委员会草案
5	ISO/IEC 27004	信息技术 – 安全技术 - 信息安全管理 - 测量	2009年出版	20	ISO/IEC 27033-4	信息技术 – 安全技术 – 网络安全 – 第4部分：使用安全网关确保网络间的通信安全 – 威胁、设计技术和控制活动	工作组草案
6	ISO/IEC 27005	信息技术 – 安全技术 - 信息安全风险管理	2008年出版	21	ISO/IEC 27034-1	应用安全 – 第1部分：概述和概念	最终委员会草案
7	ISO/IEC 27006	信息技术 – 安全技术 - 认证机构要求	2007年出版	22	ISO/IEC 27034-2	应用安全 – 第2部分：组织规范性框架	批准的新项目
8	ISO/IEC 27007	信息技术 – 安全技术 - 信息安全管理体系审核指南	委员会草案	23	ISO/IEC 27034-3	应用安全 – 第3部分：应用安全管理过程	批准的新项目
9	ISO/IEC 27008	控制审核员指南	委员会草案	24	ISO/IEC 27034-4	应用安全 – 第4部分：应用安全确认	批准的新项目
10	ISO/IEC 27010	行业间交流的信息安全管理	工作组草案	25	ISO/IEC 27034-5	应用安全 – 第5部分：协议和应用安全控制的数据结构	批准的新项目
11	ISO/IEC 27011	信息技术 – 安全技术 - 基于ISO/IEC 27002通讯行业信息安全管理体系	2008年出版	26	ISO/IEC 27035	信息技术 – 安全技术 – 信息安全事件管理	最终委员会草案
12	ISO/IEC 27013	信息技术 – 安全技术 - ? ISO/IEC 20000-1及 ISO/IEC 27001一体化实施指南	工作组草案	27	ISO/IEC 27036	信息技术 – 安全技术 – 外包安全指南	批准的新项目
13	ISO/IEC 27014	信息安全治理框架	工作组草案	28	ISO/IEC 27037	识别、收集、获取和保存数字证据指南	工作组草案
14	ISO/IEC 27015	金融及保险行业信息安全管理体系	批准的项目	29	ISO/IEC 27038	信息技术 – 安全技术 – 数字化修订详述	批准的新项目
15	ISO/IEC 27031	信息技术 – 安全技术 – 业务连续性的ICT准备能力指南	最终委员会草案				



- 关于标准 —— 基本情况
- 关于新版 —— 内容精解
- 关于换证 —— 解决方案

# 新标准特点



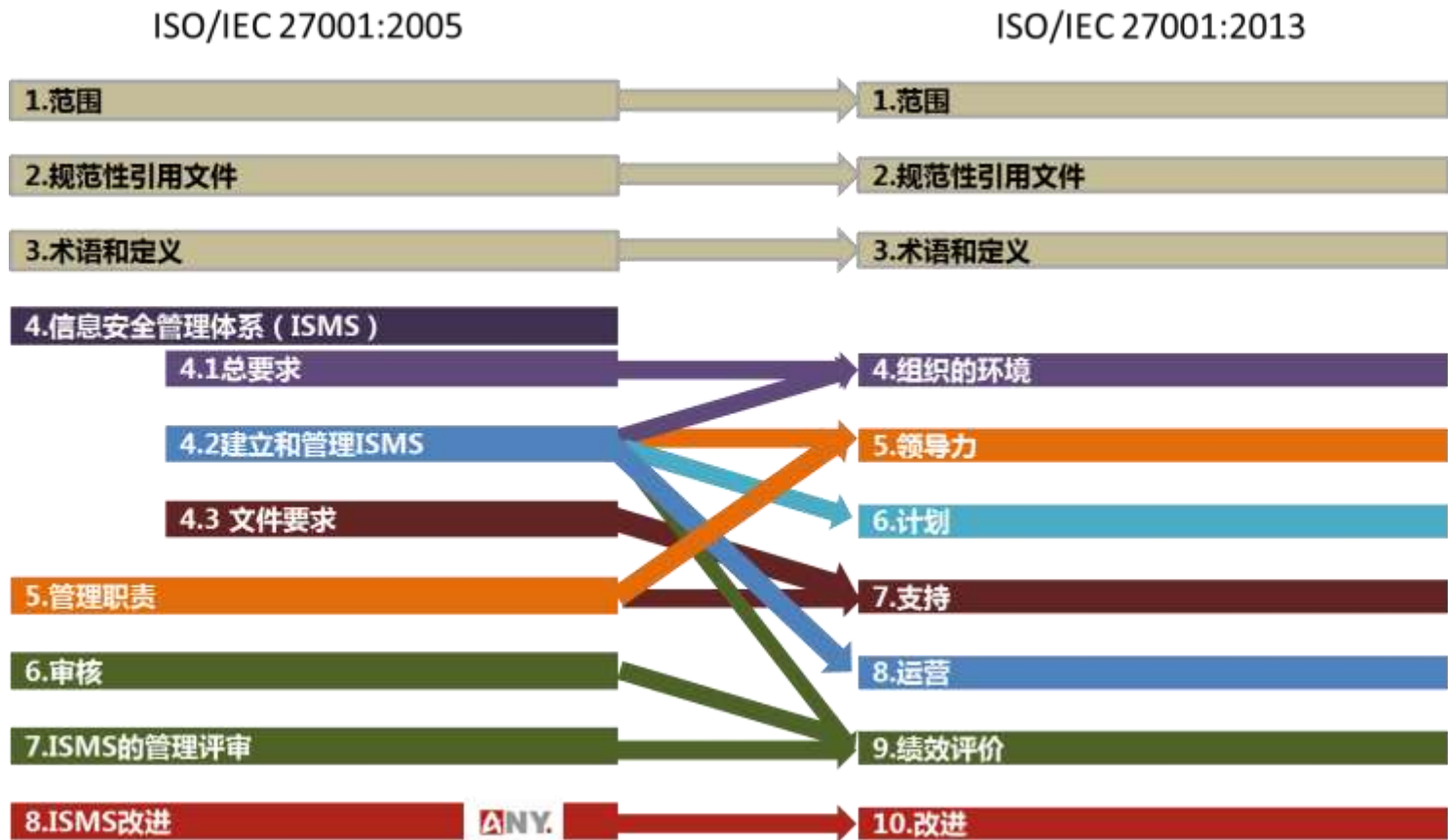
- 将原分布在各领域的加密及供应链管理控制项级别提升，组成新领域，形成新重点，以反映目前信息安全的发展趋势。
- 新增了智能型装置管理的控制项
- 强化ICT供应链委外管理的要求
- 完善了系统开发项目管理的信息安全要求

- 在新版当中采用ISO导则83做结构性要求，这个结构未来在ISO其他标准改版中会普遍采用。（ISO 22301已应用）
- 附录A中将旧版11个控制领域拓展到14个，结构更合理，表现更清晰。

- 附录A中将旧版133个控制项缩减到113个（未来仍可能有改动）。
- 将通信与操作管理领域拆分为通信安全与操作安全两个领域，比旧版标准更清晰的反应了实际的需求。
- 将旧版业务连续性管理更新为信息安全方面的业务连续性管理，表述更准确。
- 通过合并重复的控制项来精炼控制项的构成（如变更管理在不同的领域中有重复就予以合并）。



# 新标准正文部分架构变化



## Tips :

- 在新版中采用ISO导则83做结构性要求，从8个章节拓展到10个章节，重新构建了ISO标准PDCA的章节架构，这个结构在已发布的ISO22301中已经进行了应用，未来将在ISO其他标准改版中会普遍采用（包括ISO9000、ISO20000等）。



# 新标准正文部分内容构成

Plan Do Check Act

## 4. 组织的背景

- 理解组织现状及背景
- 利益相关方的期望
- ISMS的范围
- ISMS

## 6. 计划

- 处理风险和机遇的行动
- 可实现的IS目标和计划

## 8. 运行

- 运行计划及控制
- 信息安全风险评估
- 信息安全风险处置

## 10. 改进

- 不符合及纠正措施
- 持续改进

## 5. 领导力

- 领导力和承诺
- 方针
- 角色、责任和承诺

## 7. 支持

- 资源
- 能力
- 意识
- 沟通
- 文档信息

## 9. 绩效评价

- 监控、度量、分析和评价
- 内部审核
- 管理评审

内容  
新调整

# 核心内容的变化

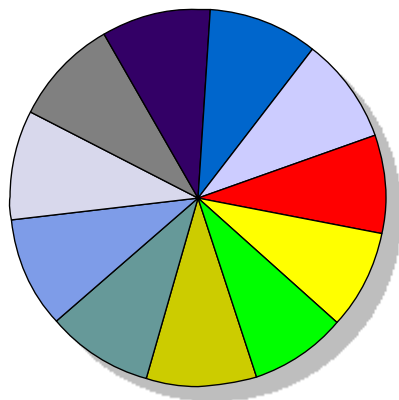
27001:2005 4.1建立ISMS	ISO 27001:2013 4.组织的背景
通过以下方面定义ISMS的范围和边界： <ul style="list-style-type: none"><li>•业务的特点;</li><li>•组织;</li><li>•位置;</li><li>•资产和技术;</li><li>•任何范围删减的细节与合理性。</li></ul>	通过确定外部和内部的情况，判断有关ISMS目的和影响，以实现预期的结果。 确定ISMS相关的要求与信息安全相关的利害关系人。 通过以下方面，确定ISMS的边界和适用性，建立ISMS的范围： <ul style="list-style-type: none"><li>•以往的外部 and 内部情况;</li><li>•利益相关方的需求;</li><li>•组织运转内外部的接口和依赖关系;</li></ul>

## Tips :

- 旧版4.1章节独立成新版第4章，对ISMS建立的基础进行了调整和明确。
- ISO27001:2005以资产和技术为主体，ISO27001:2013以组织业务关系为主体。
- 在ISMS范围和边界确定上，较ISO27001:2005版更多的考虑到了组织自身及利益相关方的需求，也意味着未来在ISMS建设中，依据组织环境情况对ISMS建设复杂度的剪裁将更灵活和个性化。

# 标准附录A的变化

14个领域



113个控制措施



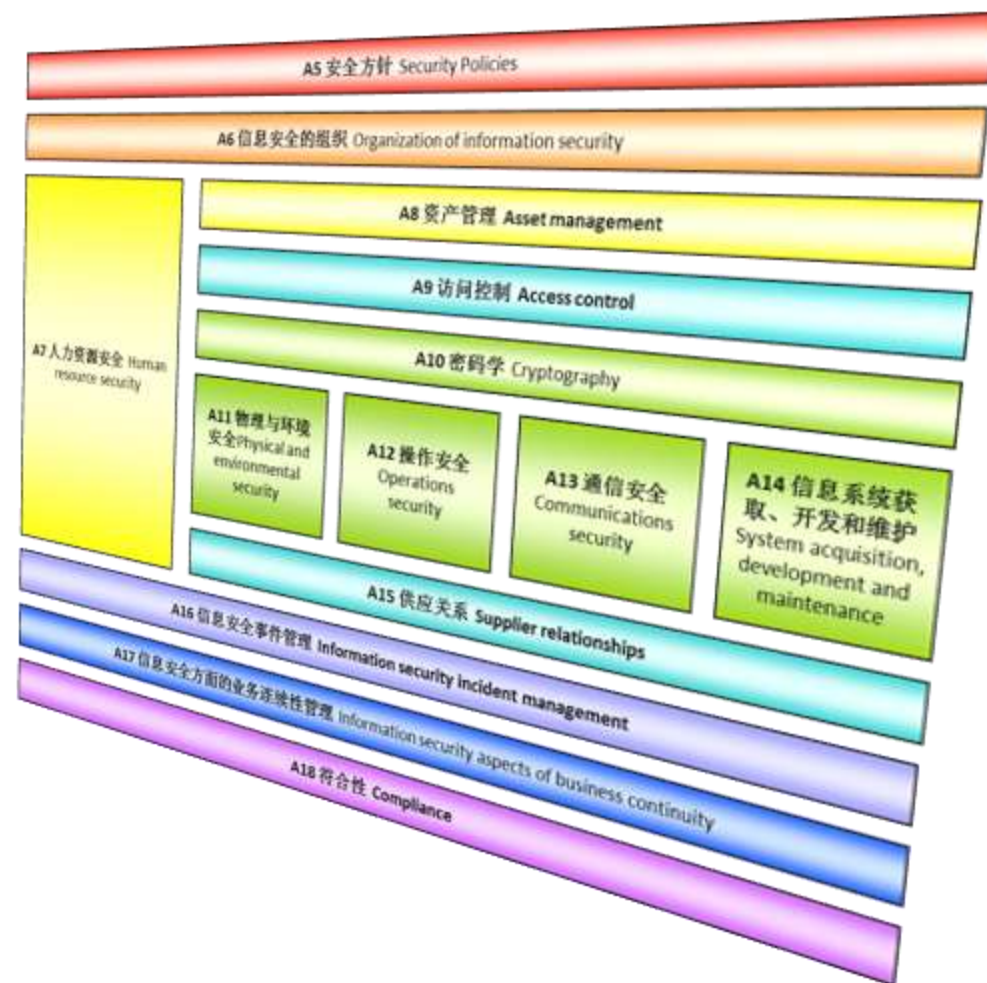
对比ISO27001:2005老版.....

11个领域

133个控制措施

# 附录A控制领域结构

- A.5 安全方针
- A.6 信息安全组织
- A.7 人力资源安全
- A.8 资产管理
- A.9 访问控制
- A.10 密码学
- A.11 物理与环境安全
- A.12 操作安全
- A.13 通信安全
- A.14 信息系统获取、开发和维护
- A.15 供应关系
- A.16 信息安全事件管理
- A.17 信息安全方面的业务连续性管理
- A.18 符合性



# 附录A控制领域的变化

## ISO27001:2005

- A.5 安全方针
- A.6 信息安全组织
- A.7 资产管理
- A.8 人力资源安全
- A.9 物理与环境安全
- A.10 通信与操作管理
- A.11 访问控制
- A.12 信息系统获取、开发和维护
- A.13 信息安全事件管理
- A.14 业务连续性管理
- A.15 符合性

## ISO27001:2013

- A.5 安全方针
- A.6 信息安全组织
- A.7 人力资源安全
- A.8 资产管理
- A.9 访问控制
- A.10 密码学 (新增)**
- A.11 物理与环境安全
- A.12 操作安全 (由旧版A.10 独立出来)**
- A.13 通信安全 (由旧版A.10 分开独立出来)**
- A.14 信息系统获取、开发和维护
- A.15 供应关系 (新增)**
- A.16 信息安全事件管理
- A.17 信息安全方面的业务连续性管理
- A.18 符合性

### Tips :

- 从旧版11个领域更新为14个领域
- 密码学、供应关系成为一个独立领域 ( A10、 A15 )
- 通讯与操作管理被划分到操作安全 ( A12 ) 和通信安全 ( A13 ) 。

# 控制项的增删与调整

新增控制项：

- 14.2.1 安全开发策略（软件和信息系统开发规则）
- 14.2.5 系统开发程序（系统工程的原则）
- 14.2.6 安全的开发环境（建立和保护开发环境）
- 14.2.8 系统安全测试（安全功能的测试）
- 16.1.4 信息安全事件的评估和决策（这是事件管理的一部分）
- 17.2.1 信息处理设施的可用性（实现冗余）

## Tips：

- 新增或调整了一些控制措施，涉及信息系统开发、信息安全事件管理、业务连续性管理等部分；
- 删除了一些旧版中重复的和操作级的控制项；
- 附录A的调整并没有颠覆原有的结构，只是在原有控制项结构的基础上，进行了优化，较旧版来说的确更清晰了，相信这样的变化可以更容易的让组织去实现它们；

删除控制项：

- 6.2.2 处理与顾客有关的安全问题
- 10.4.2 控制移动代码
- 10.7.3 信息处理规程
- 10.7.4 系统文件安全
- 10.8.5 业务信息系统
- 10.9.3 公共可用信息
- 11.4.2 外部连接的用户鉴别
- 11.4.3 网络上的设备标识
- 11.4.4 远程诊断和配置端口的保护
- 11.4.6 网络连接控制
- 11.4.7 网络路由控制
- 11.5.5 会话超时
- 11.5.6 联机时间的限定
- 11.6.2 敏感系统隔离
- 12.2.1 输入数据确认
- 12.2.2 内部处理的控制
- 12.2.3 消息完整性
- 12.2.4 输出数据确认
- 12.5.4 信息泄露
- 14.1.2 业务连续性和风险评估
- 14.1.3 制订和实施业务连续性计划
- 14.1.4 业务连续性计划框架
- 15.1.5 防止滥用信息处理设施
- 15.3.2 信息系统审计工具的保护

# 新标准对已获得认证证书组织的影响

- 新标准的颁布和执行，对已通过ISO27001认证的企业会造成一定影响，在新版公布后的18至24个月的认证转换缓冲期中，原有已取得ISO27001证书的企业最迟需要在2015年10月19日前转换到新版标准。新标的执行需要企业在3方面对现有体系进行调整：

## 1 风险评估工具需升级

随着新标准控制项架构的调整，企业目前使用的风险评估方法将受到一定影响，核心在于信息资产弱点建模及风险处置的控制项选择部分，需要重新构建符合新标准结构的风险评估工具。

## 2 SOA适用性声明及文件体系的升级

新标准的实施，将对SOA适用性声明及企业现有体系文件制度产生较大影响，体系一二级文件将需进行一个较大的内容调整及升级，不过，对三四级文件的影响较小，在三四级文件层面上，仅需根据新标要求进行少量增补即可。

## 3 内部审核工具的升级

受内部管理制度的调整，内部审核的开展方式及使用工具将不可避免受到影响，也需根据新标要求进行升级。





- 关于标准 —— 基本情况
- 关于新版 —— 内容精解
- 关于换证 —— 解决方案

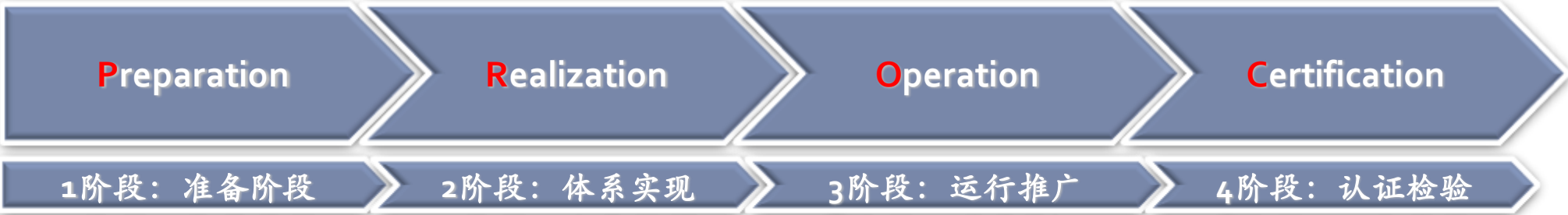
# 新标准认证转换轻量级解决方案

- 企业在新标准认证转换时，可采用基于PROC方法论的轻量级解决方案，可以使组织运转及资源投入实现最精简和最小化。

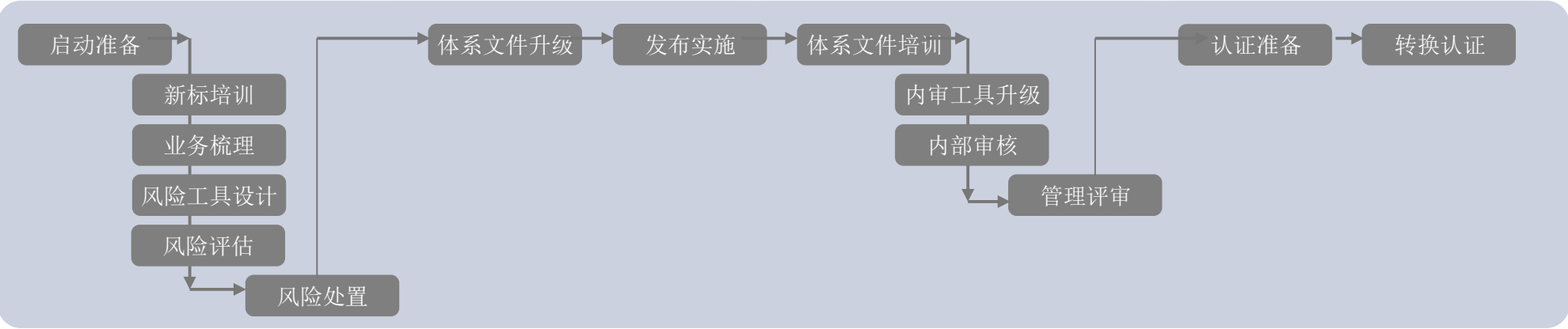
PROC



方法论  
阶段



过程  
活动



# ISMS认证体系管理系统

- 若辅以一些软件工具的使用，可进一步便于体系的管理维护和持续认证管理。
- 系统中固化了符合新版要求的风险评估工具、内审工具等模块，方便易用。



体系文件管理



风险评估管理



内部审核管理



在线教育考试

