ISO 27001：2013
新版标准变化解析

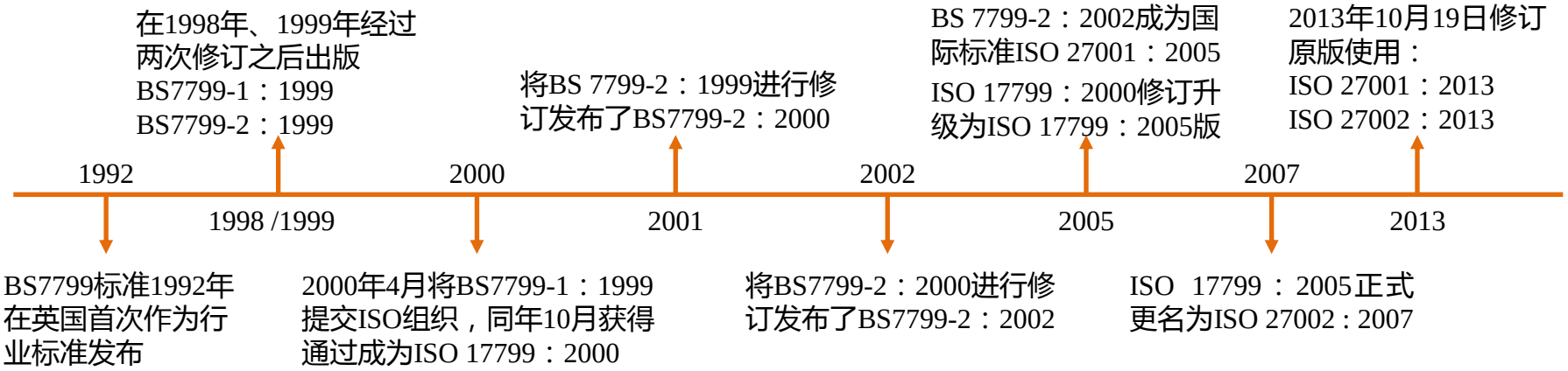
北京谷安天下科技有限公司　李鹏飞

目录
CONTENTS

致力于提升企业安全能力
国内领先的信息安全与IT风险管理服务提供商

- 标准改版背景介绍--Why
- 新版标准内容解析--What
- 认证转换时间安排--When
- 体系换证应对方案--How

ISO 27001/ISO 27002标准发展



标准改版背景

国际标准化组织（ISO组织）遵循所有标准每隔5年必须进行升级的原则。

当前版本的信息安全管理体系标准ISO 27001：2005与ISO 27002：2005已经使用了8年。

ISO 27001：2005与ISO 27002：2005版在体系整合、控制项逻辑性与充分性等方面都有改进的空间。

标准改版特点

管理体系更容易整合：在新版标准中采取Annex SL做结构性要求，使信息安全管理体系更容易与其他管理体系融合。

融入企业面临新安全挑战：对部分控制项进行了合并、删除，并且新增了部分控制项以反映当前信息安全发展趋势。

更多指引延伸参考：新增许多指引供企业参考，组织可以通过不同的面以及风险进行深度的强化。

ISO Guide 83：国际标准未来框架

导则83：
明确了 ISO国际标准未来发展框架及方向

1. Scope
范围

2. Normative Reference
规范性引用文件

3. Terms and Definitions
术语和定义

4. Context of the Organization
组织环境

5. Leadership
领导力

6. Planning
策划

7. Support
支持

8. Operation
运行

9. Performance Evaluation
绩效评价

10. Improvement
改进

ISO 27001 | **ISO 20000** | **ISO 22301** | **….**

管理体系标准新结构和格式

国际标准化组织对管理体系标准在结构、格式、通用短语和定义方面进行了统一。这将确保今后编制或修订管理体系标准的持续性、整合性和简单化，这也将使标准更易读、易懂。

所有管理体系标准将遵循 ISO Supplement Annex SL 的要求，以便整合其他标准文件中的不同主题和要求，如：

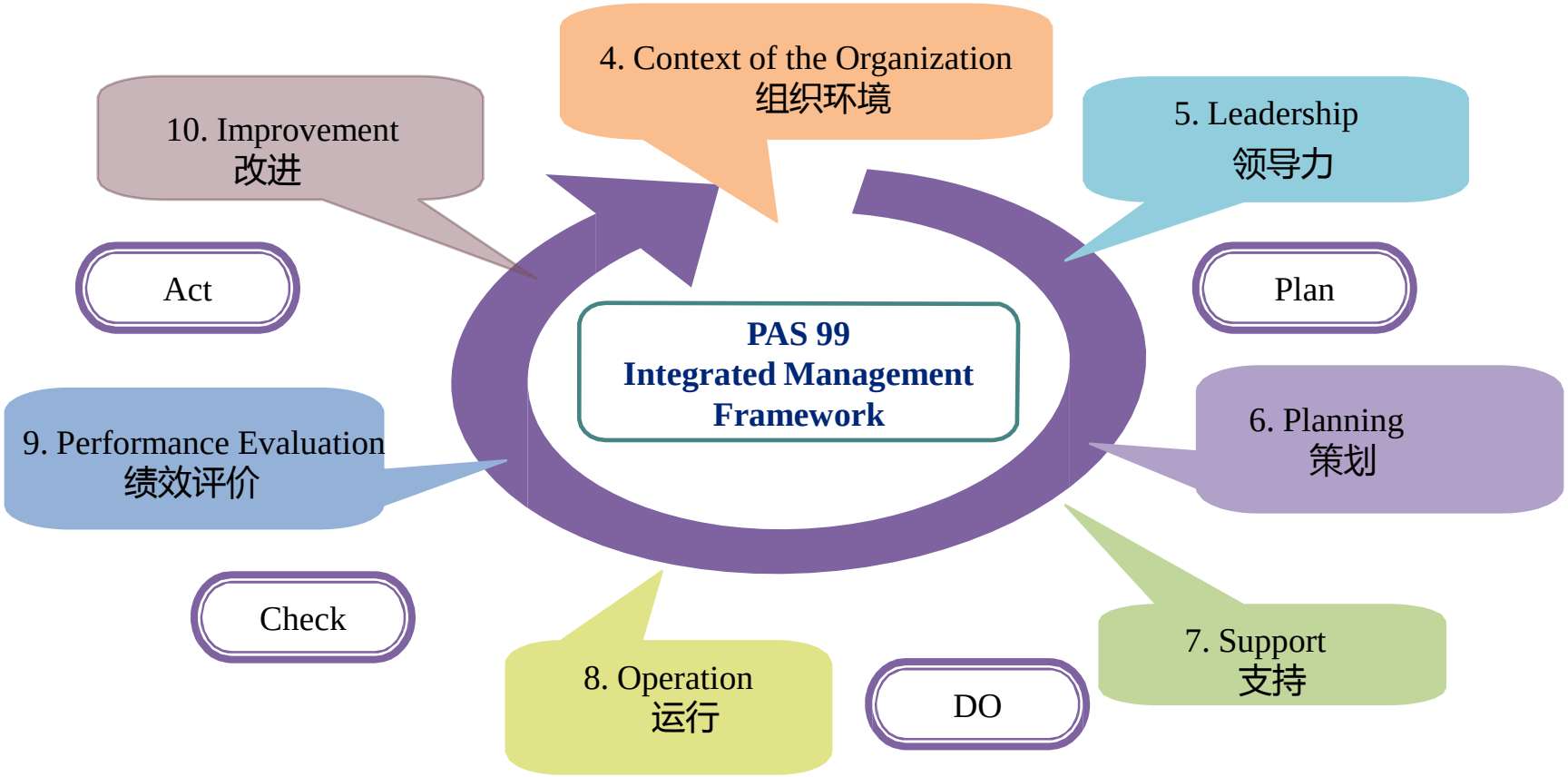
统一定义，如：

组织、相关方、方针、目标、能力、符合性

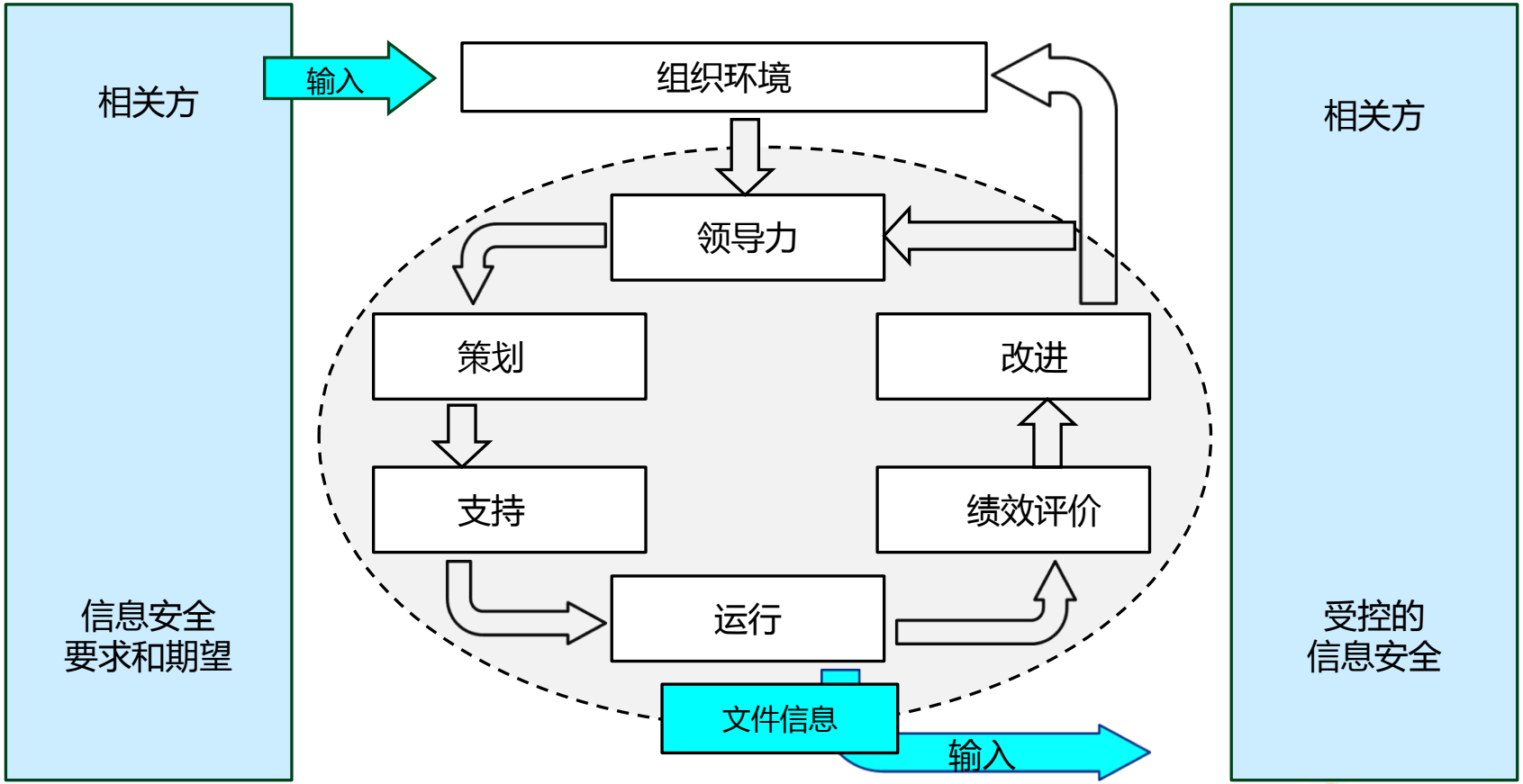
统一的表述，如：

最高管理者应确保组织内的职责、权限得到规定和沟通。

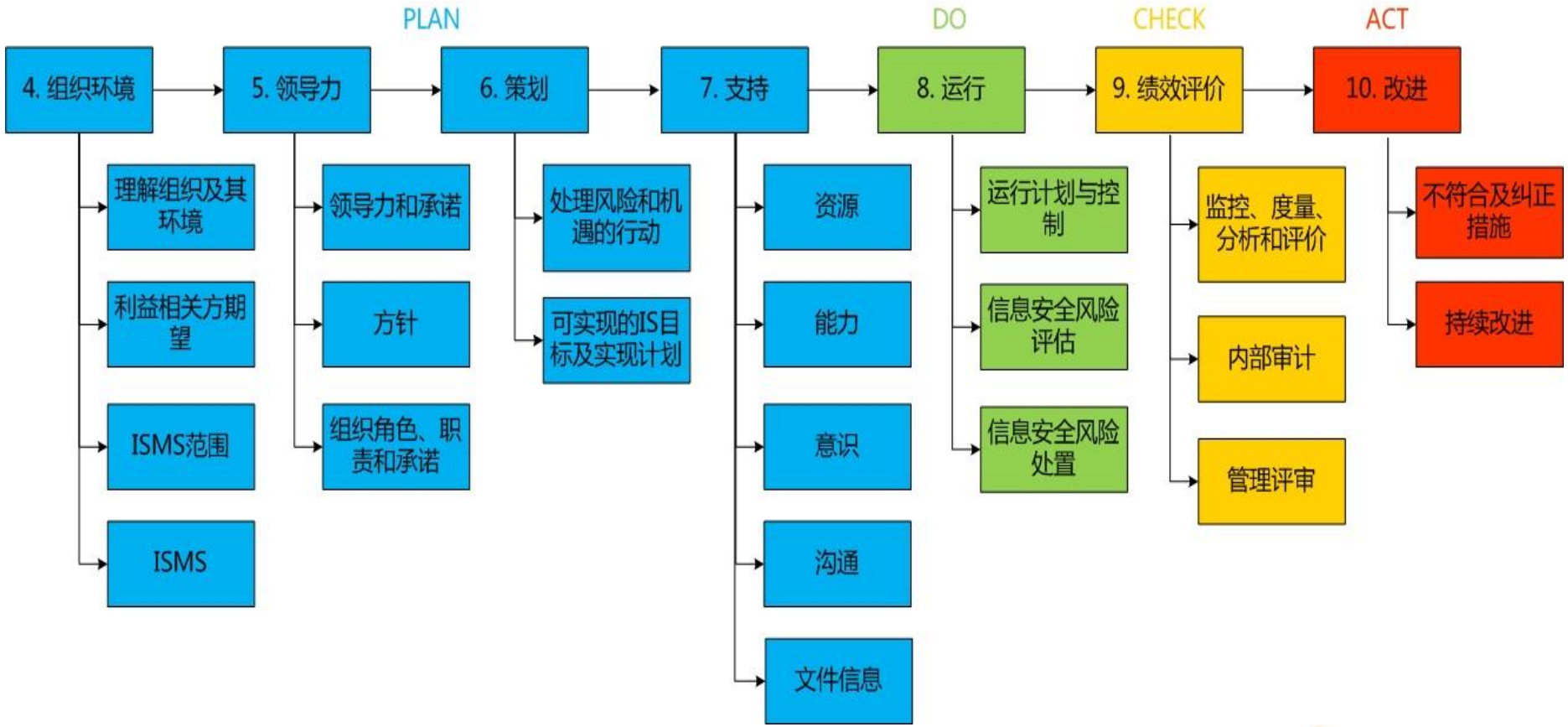
PAS 99：整合管理体系



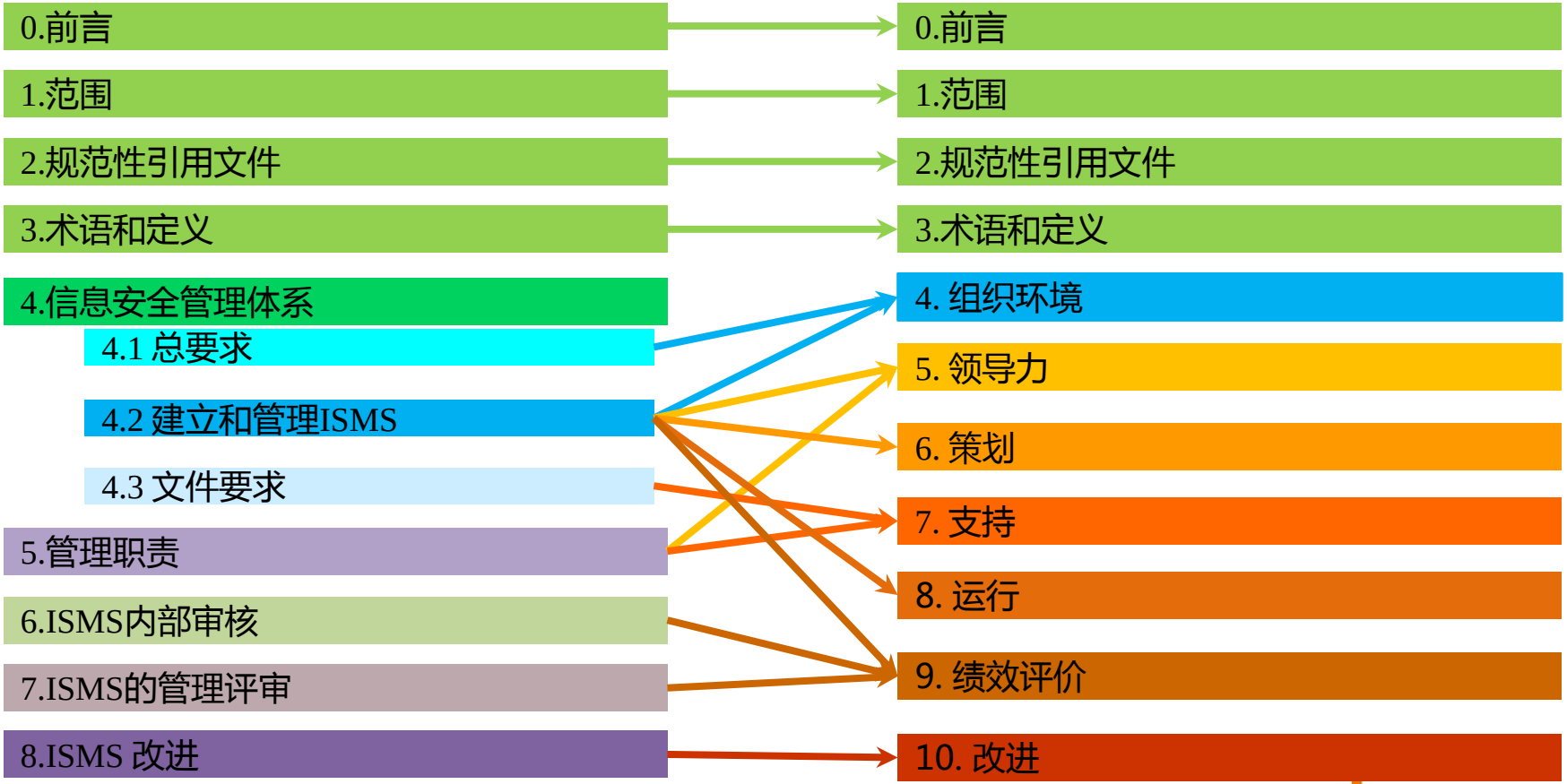
ISO 27001:2013标准结构调整



新标准正文内容结构


PLAN
DO
CHECK
ACT
4. 组织环境
5. 领导力
6. 策划
7. 支持
8. 运行
9. 绩效评价
10. 改进
理解组织及其环境
利益相关方期望
ISMS范围
ISMS
领导力和承诺
方针
组织角色、职责和承诺
处理风险和机遇的行动
可实现的IS目标及实现计划
资源
能力
意识
沟通
文件信息
运行计划与控制
信息安全风险评估
信息安全风险处置
监控、度量、分析和评价
内部审计
管理评审
不符合及纠正措施
持续改进

新标准正文结构变化


0.前言
1.范围
2.规范性引用文件
3.术语和定义
4.信息安全管理体系
4.1 总要求
4.2 建立和管理ISMS
4.3 文件要求
5.管理职责
6.ISMS内部审核
7.ISMS的管理评审
8.ISMS 改进
0.前言
1.范围
2.规范性引用文件
3.术语和定义
4. 组织环境
5. 领导力
6. 策划
7. 支持
8. 运行
9. 绩效评价
10. 改进

新标准正文内容简介

章节	描述
4.组织环境	属于Plan阶段的一个组成部分。 本章介绍了建立适用于组织信息安全管理环境的必要要求，包括需求、要求与范围。 本章涉及了解组织现状及背景、明确建立信息安全管理体系的目的、理解相关方的需求与期望、确定信息安全管理体系范围。
5.领导力	属于Plan阶段的一个组成部分。 本章总结了最高管理层在信息安全管理体系中承担角色的具体要求，以及如何通过一份声明的策略来向组织传达领导层的期望。 本章涉及了领导力和承诺、信息安全方针目标，以及角色、职责和承诺。
6.策划	属于Plan阶段的一个组成部分。 本章介绍了处理风险和机遇的行动，以及可实现的信息安全目标与实现计划。 本章涉及了信息安全风险评估、风险所有者、信息安全风险处置、适用性声明、信息安全目标。
7.支持	属于Plan阶段的一个组成部分。 本章详细叙述了建立、实施、保持和改进一个有效的信息安全管理体系所要求的支持。包括：资源要求、参与人员的能力、意识、与利益相关方沟通、文档化信息。

新标准正文内容简介

章节	描述
8.运行	属于Do阶段的一个组成部分。 本章要求组织计划并控制信息安全要求的运行。 本章涉及运行计划及控制、信息安全风险评估、信息安全风险处置。
9.绩效评价	属于Check阶段的一个组成部分。 本章总结了度量ISMS执行、ISMS与国际标准及管理层期望的符合性、寻求管理层期望反馈的要求。 本章涉及监控、度量、分析和评价，内部审核，管理评审。
10.改进	属于Act阶段的一个组成部分。 本章定义了通过纠正行动来识别和改进不符合项。 本章涉及不符合项与纠正措施、持续改进。

新标准控制域变化

ISO 27001：2005	ISO 27001：2013 DIS
A.5 安全方针	A.5 安全方针
A6 信息安全组织	A.6 信息安全组织
A7 资产管理	A.7 人力资源安全
A8 人力资源安全	A.8 资产管理
A9 物理与环境安全	A.9 访问控制
A10 通信和操作管理	A.10 密码学(新增)
A11 访问控制	A.11 物理与环境安全
A12 信息系统获取、开发和维护	A.12 操作安全(拆分）
A13 信息安全事件管理	A.13 通信安全（拆分）
A14 业务连续性管理	A.14 信息系统获取、开发和维护
A15 符合性	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

2005版原本有11个领域、133项控制措施；新版标准目前调整为14个领域、113个控制措施.
控制措施变化：增加11个、删除26个、合并减少5个，总计减少了20个。

新增控制措施介绍

控制项	描述	说明
A.6.1.4项目管理中的信息安全	信息安全应融入项目管理中，与项目类型无关。	加强项目中的安全管理。
A.12.6.2限制软件安装	应建立规则来控制用户安装软件	控制版权及技术漏洞风险。
A.14.2.1安全开发策略	应制定及应用关于软件和系统的开发规则	加强信息系统生命周期中的信息安全管理，建立安全开发策略、程序与流程。
A.14.2.5系统开发程序	应建立安全系统开发流程，记录，维护并应用到任何信息系统开发工 作	
A.14.2.6安全的开发环境	组织应建立并适当保护开发环境安全，并集成涵盖整个系统开发周期 的工作	
A.14.2.8系统安全性测试	在开发的过程中，必须测试功能的安全性	
A.15.1.3ICT供应链	与供应商的协议应包括解决信息、通信技术服务、产品供应链相关信 息安全风险的要求	控制供应链中断风险。
A.16.1.4信息安全事件的评估和决策	信息安全事件应当被评估与决策，如果他们被归类为信息安全事件。	完善信息安全事件管理生命周期。
A.16.1.5信息安全事故的响应	信息安全事件应依照程序文件响应	
A.17.1.2实现信息安全的连续性	组织应建立、记录、实施并维护流程、程序、控制项，以保证在不利 情况下要求的信息安全连续性的等级。	加强可用性管理，完善原BCM管理的生命周期。
A.17.2.1信息处理设施的可用性	信息处理设施应当实现冗余，以满足可用性需求。	

合并控制措施介绍

ISO 27001：2013 DIS	ISO 27001：2005
A.6.1.1信息安全的角色和 职责	A.6.1.3 信息安全职责的分配 A.8.1.1 角色和职责
A.9.2.1用户注册和注销	A.11.2.1 用户注册 A.11.5.2 用户标识和鉴别
A.9.4.2安全登录程序	A.11.5.1 安全登录规程 A.11.5.5 会话超时 A.11.5.6 联机时间的限定
A.12.4.2管理员和操作员日 志	A.10.10.3 日志信息的保护 A.10.10.4 管理员和操作员日志
A.14.1.2保护公共网络上的应用服务	A.10.9.1 电子商务 A.10.9.3 公共可用信息

删除控制措施介绍

删除控制措施	理由
A.6.1.1信息安全的管理承诺	在ISO 27001正文中管理层承诺中已经包含其内容
A.6.1.2信息安全协调	内容与ISO 27003中关于ISMS建立与实施的内容重复
A.6.1.4信息处理设施的授权过程	在A6.1.1中的一部分，没有必要再单独出现
A.6.2.1与外部各方相关风险的识别	在ISO 27001正文风险评估与处理中已经体现
A.6.2.2处理与顾客有关的安全问题	在ISO 27001正文风险评估与处理中已经体现
A.10.2.1服务交付	没有原因
A.10.7.4系统文件安全	系统文件也属于信息资产，他们如何保护取决于其风险
A.10.8.5业务信息系统	该控制项几乎涉及整个标准，控制效果不明显
A.10.10.2监视系统的使用	是Event Logging（A12.4.1）控制措施的子集
A.10.10.5故障日志	是Event Logging（A12.4.1）控制措施的子集

删除控制措施介绍

删除控制措施	理由
A.11.4.2外部连接的用户鉴别	被相关内容被access control(A.9.1.1)涵盖
A.11.4.3网络上的设备识别	相关内容被 networks control（A.13.1.3）涵盖
A.11.4.4 远程诊断和配置端口的保护	相关内容被 networks control（A.13.1.3）涵盖
A.11.4.6网络连接控制	相关内容被 networks control（A.13.1.3）涵盖
A.11.4.7 网络路由控制	相关内容被 networks control（A.13.1.3）涵盖
A.11.6.2敏感系统隔离	在互联互通的世界这个控制措施的目标很难实现
A.12.2.1输入数据确认	相关内容在System development procedures（A.14.2.5）体现
A.12.2.2内部处理的控制	相关内容在System development procedures（A.14.2.5）体现
A.12.2.3消息完整性	相关内容在 Information transfer policies and procedures（A.13.2.1）体现
A.12.2.4输出数据确认	相关内容在System development procedures（A.14.2.5）体现

删除控制措施介绍

删除控制措施	理由
A.12.5.4信息泄露	相关内容在A.8.3.2/A.11.2.1/A.12.6.2/A.13.2.4和其他区域都有涉及
A.14.1.1 在业务连续性管理过程中包含信息安全	相关控制内容在Implementing information security continuity（A.17.1.2）有体现
A.14.1.3制定和实施包含信息安全的连续性计划	相关控制内容在Implementing information security continuity（A.17.1.2）有体现
A.14.1.4 业务连续性计划框架	相关控制内容在Implementing information security continuity（A.17.1.2）有体现
A.15.1.5防止滥用信息处理设施	该控制内容与英国的一部法律相关
A.15.3.2信息系统审计工具的保护	审计工具也属于信息资产，其保护由其有风险决定

ISO 27000标准系列

序号	标准编号	标准名称	出版年份
1	ISO/IEC 27000	信息技术-安全技术-信息安全管理体系-概述与术语	2009
2	ISO/IEC 27001	信息技术-安全技术-信息安全管理体系-要求	2005
3	ISO/IEC 27002	信息技术-安全技术-信息安全管理实用规则	2005
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
5	ISO/IEC 27004	信息技术-安全技术-信息安全管理-度量	2009
6	ISO/IEC 27005	信息技术-安全技术-信息安全风险管理	2011
7	ISO/IEC 27006	信息技术-安全技术-信息安全管理体系认证机构要求	2007
8	ISO/IEC 27007	信息技术-安全技术-信息安全管理体系审核指南	2011
9	ISO/IEC 27008	信息技术-安全技术-ISMS控制措施的审核员指南	2011
10	ISO/IEC 27010	信息技术-安全技术-部门间和组织间通信的信息安全管理	2012
11	ISO/IEC 27011	信息技术-安全技术-通讯行业基于ISO/IEC 27002的信息安全管理指南	2008

ISO 27000标准系列

序号	标准编号	标准名称	出版年份
12	ISO/IEC 27013	信息技术-安全技术- ISO/IEC 27001与 ISO/IEC 20000-1整合实施指南	2012
13	ISO/IEC 27014	信息技术-安全技术- 信息安全治理架构	2013
14	ISO/IEC 27015	信息技术-安全技术- 金融服务行业信息安全管理指南	2012
15	ISO/IEC 27017	信息技术-安全技术- 信息安全管理-基于ISO/IEC 27002使用云计算服务信息安全控制措施指南	未发布
16	ISO/IEC 27018	信息技术-安全技术- 公共云计算服务数据保护控制措施实用规则	未发布
17	ISO/IEC 27031	信息技术-安全技术-业务连续性信息通信技术准备指南	2011
18	ISO/IEC 27032	信息技术-安全技术-网络安全技术指南	2012
19	ISO/IEC 27033-1	信息技术-安全技术-网络安全-概述与概念	2009
20	ISO/IEC 27033-2	信息技术-安全技术-网络安全-网络安全设计与实施指南	2012
21	ISO/IEC 27033-3	信息技术-安全技术-网络安全-参考网络场景-威胁、设计技术与控制问题	2010

ISO 27000标准系列

序号	标准编号	标准名称	出版年份
22	ISO/IEC 27034-1	信息技术-安全技术-应用安全-应用安全概述与概念	2011
23	ISO/IEC 27034-2	信息技术-安全技术-应用安全-组织规范框架	未发布
24	ISO/IEC 27034-3	信息技术-安全技术-应用安全-应用安全管理流程	未发布
25	ISO/IEC 27034-4	信息技术-安全技术-应用安全-应用安全验证	未发布
26	ISO/IEC 27034-5	信息技术-安全技术-应用安全-协议和应用安全控制数据结构	未发布
27	ISO/IEC 27034-6	信息技术-安全技术-应用安全-特定应用安全指南	未发布
28	ISO/IEC 27035	信息技术-安全技术-信息安全事件管理	2011
29	ISO/IEC 27036	信息技术-安全技术-供应关系信息安全（4部分）	未发布
30	ISO/IEC 27040	信息技术-安全技术-存储安全	未发布
31	ISO/IEC 27044	信息技术-安全技术-安全信息与事态管理指南	未发布

ISO 27000标准系列

序号	标准编号	标准名称	出版年份
22	ISO/IEC 27034-1	信息技术-安全技术-应用安全-应用安全概述与概念	2011
23	ISO/IEC 27034-2	信息技术-安全技术-应用安全-组织规范框架	未发布
24	ISO/IEC 27034-3	信息技术-安全技术-应用安全-应用安全管理流程	未发布
25	ISO/IEC 27034-4	信息技术-安全技术-应用安全-应用安全验证	未发布
26	ISO/IEC 27034-5	信息技术-安全技术-应用安全-协议和应用安全控制数据结构	未发布
27	ISO/IEC 27034-6	信息技术-安全技术-应用安全-特定应用安全指南	未发布
28	ISO/IEC 27035	信息技术-安全技术-信息安全事件管理	2011
29	ISO/IEC 27036	信息技术-安全技术-供应关系信息安全（4部分）	未发布
30	ISO/IEC 27040	信息技术-安全技术-存储安全	未发布
31	ISO/IEC 27044	信息技术-安全技术-安全信息与事态管理指南	未发布

新标准认证转换时间安排

2013年6月-7月

日前ISO27001:2013 DIS版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。

发布DIS最终版

2013年10月19日

ISO组织公布的正式版本的颁布时间为2013年10月19日。

发布正式版

2015年10月19日前

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。

完成认证转换

体系认证换证方案

Plan → Do → Check → Action

法律法规

监管要求

国际国内标准

最佳实践

谷安安全实践

项目准备	现状调研	风险评估	体系建设	体系运行	认证审核
1.项目资源准备	1.体系文件评审	1.评估方法更新	1.体系整合设计	1.体系运行跟踪	1.宣传培训
2.项目计划编制	2.现场访谈走查	2.信息资产更新	2.文件架构更新	2.运行工具更新	2.文件审核
3.实施工具准备	3.安全技术评估	3.安全风险分析	3.制度文件编写	3.体系内部审核	3.现场审核
4.项目启动大会	4.新版差距分析	4.安全风险处置	4.制度文件评审	4.体系管理评审	4.审核整改
5.新版标准培训	5.现状调研总结	5.风险评估总结	5.制度文件发布	5.体系持续改进	5.宣传展示

获得新版证书

课堂培训、共同实施、资料交付、知识转移

Thanks!

谷安天下

国内领先的信息安全与IT风险管理服务提供商

T +86 01 51626887
F +86 01 51626887-816
E market@gooann.com

A-806.Digital Tower,No.2,South Street ZhongGuanCun,
Haidian District,Beijing
北京海淀区中关村南大街2号
数码大厦A座806
www.gooann.com