等级保护体系与ISO27001信息安全管理体系的区别和联系

目录

- 等级保护体系与ISO27000体系对比
- 等级保护工作与ISO27000实施时存在的难点
- 等级保护工作与ISO27000相互补充融合的意义

等级保护政策发展过程

1999

计算机系统安全保护等级划分思想提出

2002

等级保护工作试点启动

2004

等级保护相关政策文件颁布

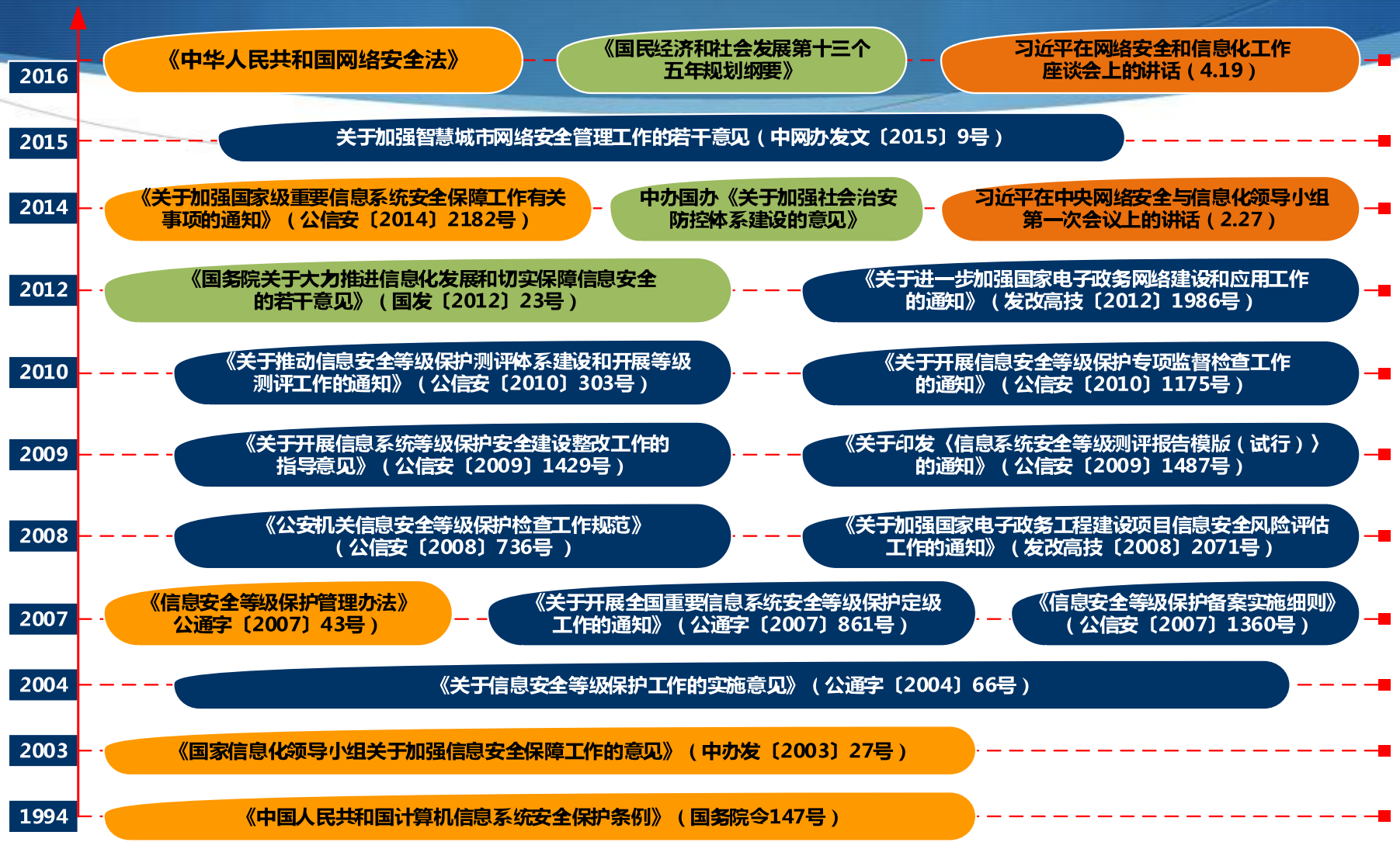
2008

等级保护相关标准发布

2016

《网络安全法》将等级保护制度作为基本国策

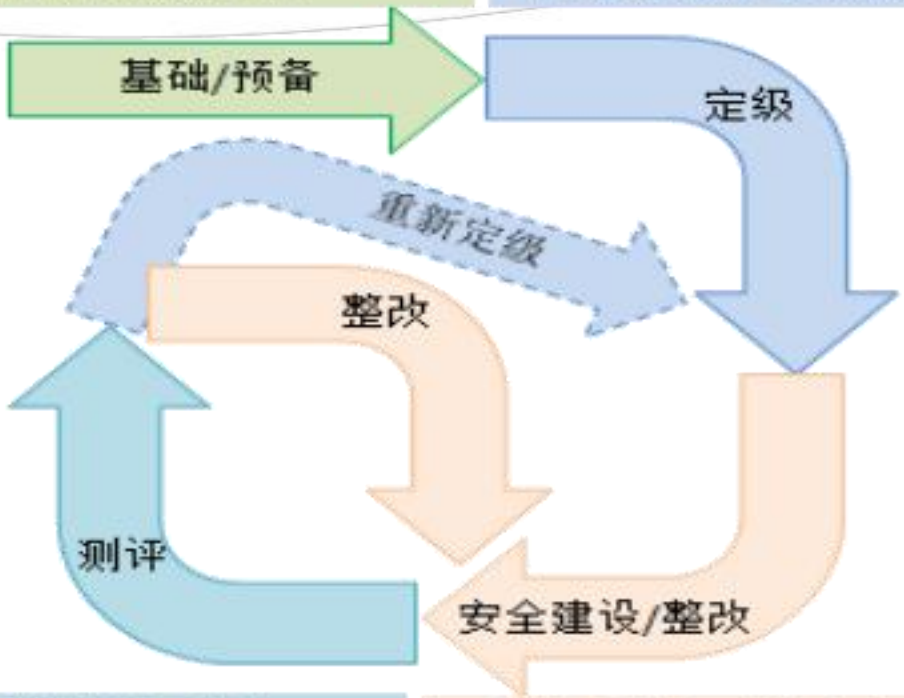
等级保护政策发展过程


2016
《中华人民共和国网络安全法》
《国民经济和社会发展第十三个五年规划纲要》
习近平在网络安全和信息化工作座谈会上的讲话（4.19）
2015
关于加强智慧城市网络安全管理工作的若干意见（中网办发文〔2015〕9号）
2014
《关于加强国家级重要信息系统安全保障工作有关事项的通知》（公信安〔2014〕2182号）
中办国办《关于加强社会治安防控体系建设的意见》
习近平在中央网络安全与信息化领导小组第一次会议上的讲话（2.27）
2012
《国务院关于大力推进信息化发展和切实保障信息安全的若干意见》（国发〔2012〕23号）
《关于进一步加强国家电子政务网络建设和应用工作的通知》（发改高技〔2012〕1986号）
2010
《关于推动信息安全等级保护测评体系建设和开展等级测评工作的通知》（公信安〔2010〕303号）
《关于开展信息安全等级保护专项监督检查工作的通知》（公信安〔2010〕1175号）
2009
《关于开展信息系统等级保护安全建设整改工作的指导意见》（公信安〔2009〕1429号）
《关于印发〈信息系统安全等级测评报告模版（试行）〉的通知》（公信安〔2009〕1487号）
2008
《公安机关信息安全等级保护检查工作规范》（公信安〔2008〕736号）
《关于加强国家电子政务工程建设项目信息安全风险评估工作的通知》（发改高技〔2008〕2071号）
2007
《信息安全等级保护管理办法》公通字〔2007〕43号）
《关于开展全国重要信息系统安全等级保护定级工作的通知》（公通字〔2007〕861号）
《信息安全等级保护备案实施细则》（公信安〔2007〕1360号）
2004
《关于信息安全等级保护工作的实施意见》（公通字〔2004〕66号）
2003
《国家信息化领导小组关于加强信息安全保障工作的意见》（中办发〔2003〕27号）
1994
《中国人民共和国计算机信息系统安全保护条例》（国务院令147号）

现行信息安全等级保护标准体系

《计算机信息系统安全保护等级划分准则》
《信息系统安全等级保护实施指南》
GB 17859-1999
GB/T 25058-2010

《信息系统安全保护等级定级指南》
GB/T 22240-2008



GB/T 22239-2008
GB/T 25070-2010
GB/T 20271-2006
GB/T 20269-2006
GB/T 20282-2006

《信息系统安全等级保护测评要求》
《信息系统安全等级保护测评过程指南》
GB/T 28448-2012
GB/T 28449-2012

《信息系统安全等级保护基本要求》
《信息系统等级保护安全设计技术要求》
《信息系统通用安全技术要求》
《信息系统安全管理要求》
《信息系统安全工程管理要求》

网络安全等级保护制度
进入2.0时代

- 一是网络安全法第二十一条明确要求：国家实行网络安全等级保护制度。
- 二是中央关于加强社会治安防控体系建设的意见要求“健全完善信息安全等级保护制度”。
- 三是习近平总书记等中央领导批示要求：健全完善以保护国家关键信息基础设施安全为重点的网络安全等级保护制度。

等级保护对象的演变

1994

计算机信息系统

保护重点没有变，但复杂度提高

2003

基础信息网络

重要信息系统

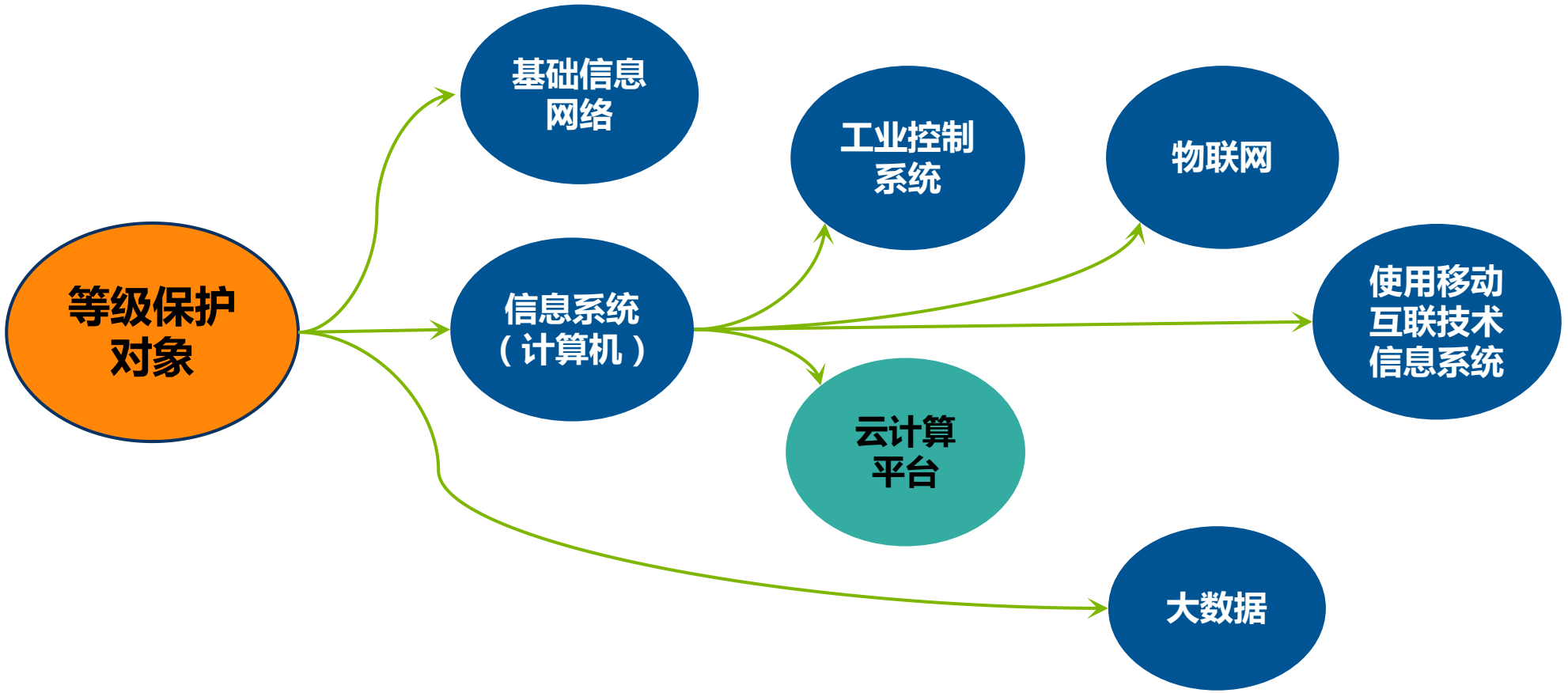
重点

2017

重要**网络设施**

重要信息系统

等级保护2.0保护对象展现形态



《网络安全法》明确

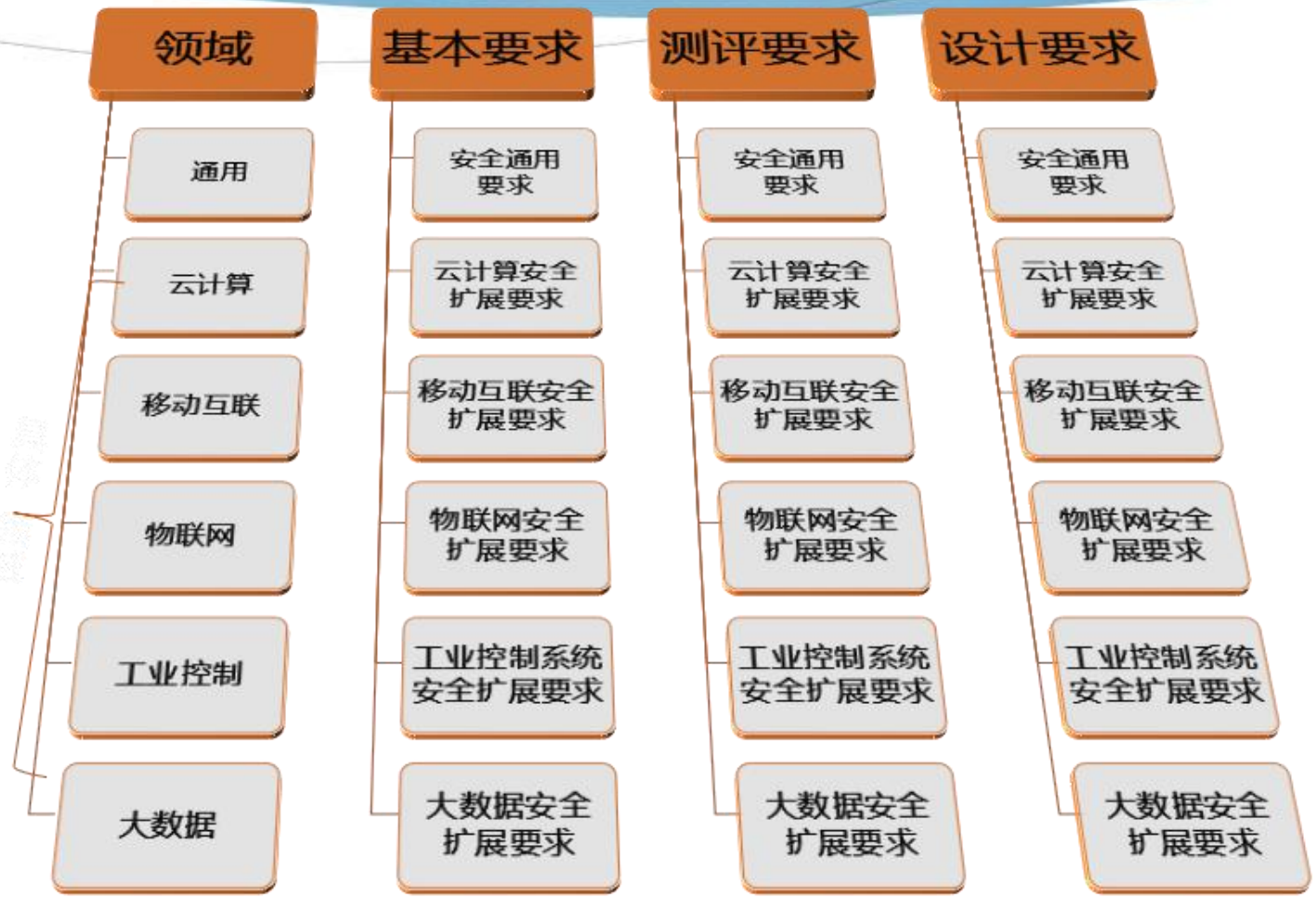
- 第二十一条　**国家实行网络安全等级保护制度**。网络运营者应当按照网络安全等级保护制度的要求，履行下列安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改。**（法律明确　基本国策　基本制度）**

- 第三十一条　国家对公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务等重要行业和领域，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的**关键信息基础设施**，在网络安全**等级保护制度的基础上，实行重点保护（新的阶段任务）**

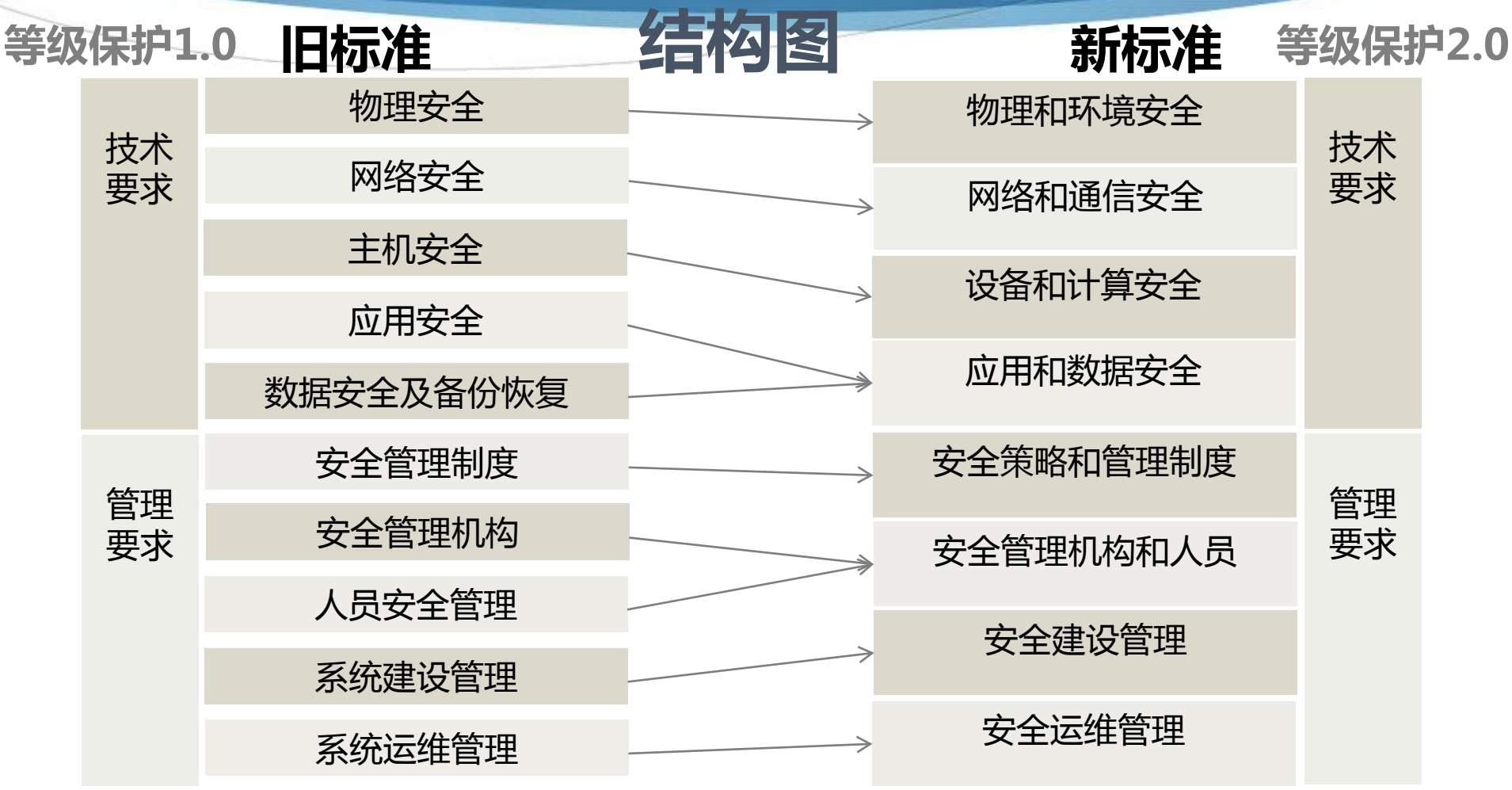
等保2.0定级指南

侵害客体	对客体的侵害程度		
	一般损害	严重损害	特别严重损害
公民、法人和其他组织的合法权益	第一级	第二级	第三级
社会秩序、公共利益	第二级	第三级	第四级
国家安全	第三级	第四级	第五级

等保2.0要求体系变化


领域
基本要求
测评要求
设计要求
通用
云计算
移动互联
物联网
工业控制
大数据
安全通用要求
云计算安全扩展要求
移动互联安全扩展要求
物联网安全扩展要求
工业控制系统安全扩展要求
大数据安全扩展要求
安全通用要求
云计算安全扩展要求
移动互联安全扩展要求
物联网安全扩展要求
工业控制系统安全扩展要求
大数据安全扩展要求
安全通用要求
云计算安全扩展要求
移动互联安全扩展要求
物联网安全扩展要求
工业控制系统安全扩展要求
大数据安全扩展要求

等级保护基本要求结构变化



等级保护控制点变化

基本要求大类1.0	基本要求子类	信息系统安全等级保护级别	
		等保二级	等保三级
技术要求	物理安全	10	10
	网络安全	6	7
	主机安全	6	7
	应用安全	7	9
	数据安全	3	3
管理要求	安全管理制度	3	3
	安全管理机构	5	5
	人员安全管理	5	5
	系统建设管理	9	11
	系统运维管理	12	13
合计	/	66	73

基本要求大类2.0	基本要求子类	信息系统安全等级保护级别	
		等保二级	等保三级
技术要求	物理和环境安全	10	10
	网络和通信安全	7	8
	设备和计算安全	6	6
	应用和数据安全	9	10
管理要求	安全策略和管理制度	4	4
	安全管理机构和人员	9	9
	安全建设管理	10	10
	安全运维管理	14	14
合计	/	69	71

等级保护要求项变化

基本要求大类1.0	基本要求子类	信息系统安全等级保护级别	
		等保二级	等保三级
技术要求	物理安全	19	32
	网络安全	18	33
	主机安全	19	32
	应用安全	19	31
	数据安全	4	8
管理要求	安全管理制度	7	11
	安全管理机构	9	20
	人员安全管理	11	16
	系统建设管理	28	45
	系统运维管理	41	62
合计	/	175	290

基本要求大类2.0	基本要求子类	信息系统安全等级保护级别	
		等保二级	等保三级
技术要求	物理和环境安全	15	22
	网络和通信安全	16	33
	设备和计算安全	17	26
	应用和数据安全	22	34
管理要求	安全策略和管理制度	6	7
	安全管理机构和人员	16	26
	安全建设管理	25	34
	安全运维管理	30	48
合计	/	147	230

等保2.0《基本要求》标准结构

- 1　范围
- 2　规范性引用文件
- 3　术语和定义
- 4　缩略语
- 5　网络安全等级保护概述
  - 5.1　等级保护对象
  - 5.2　不同级别的安全保护能力
  - 5.3　安全通用要求和安全扩展要求

等保2.0《基本要求》标准结构

- 6 第一级安全要求
  - 6.1 安全通用要求
  - 6.2 云计算安全扩展要求
  - 6.3 移动互联安全扩展要求
  - 6.4 物联网安全扩展要求
  - 6.5 工业控制系统安全扩展要求

《基本要求》标准结构3

- 附录D：云计算应用场景说明
- 附录E：移动互联应用场景说明
- 附录F：物联网应用场景说明
- 附录G：工业控制系统应用场景说明
- 附录H：大数据应用安全扩展要求

安全通用要求和安全扩展要求的使用场合

- 安全通用要求针对共性化保护需求提出，等级保护对象无论以何种形式出现，必须根据安全保护等级实现相应级别的安全通用要求
- 安全扩展要求针对个性化保护需求提出，需要根据安全保护等级和使用的特定技术或特定的应用场景实现安全扩展要求

等级保护2. 对0测评要求提升

- ✓ 功能、机制符合
- ✓ 策略、配置符合
- ✓ 文档、记录符合

- ✓ 保护目标达成
- ✓ 措施取得成效
- ✓ 效果能够持续

- ✓ 自动配置检查和判断
- ✓ 状态信息自动收集
- ✓ 数据分析和评估

等保2.0《测评要求》标准结构

- 6 第一级安全要求
  - 6.1 安全测评通用要求
  - 6.2 云计算安全测评扩展要求
  - 6.3 移动互联安全测评扩展要求
  - 6.4 物联网安全测评扩展要求
  - 6.5 工业控制系统安全测评扩展要求

等保2.0《安全设计要求》标准结构

网络安全等级保护安全设计技术要求（GB/T 25070）

前言

引言

1 范围

2 规范性引用文件

3 术语和定义

4 缩略语

5 网络安全等级保护安全技术设计概述

5.1 通用等级保护安全技术设计框架

5.2 云计算等级保护安全技术设计框架

5.3 移动互联等级保护安全技术设计框架

5.4 物联网等级保护安全技术设计框架

5.5 工业控制等级保护安全技术设计框架

6 第一级系统安全保护环境设计

6.1 设计目标

6.2 设计策略

6.3 设计技术要求

7 第二级系统安全保护环境设计

7.1 设计目标

7.2 设计策略

7.3 设计技术要求

8 第三级系统安全保护环境设计

8.1 设计目标

8.2 设计策略

8.3 设计技术要求

9 第四级系统安全保护环境设计

9.1 设计目标

9.2 设计策略

9.3 设计技术要求

10 第五级系统安全保护环境设计

11 定级系统互联设计

11.1 设计目标

11.2 设计策略

11.3 设计技术要求

8 第三级系统安全保护环境设计

8.1 设计目标

8.2 设计策略

8.3 设计技术要求

8.3.1 安全计算环境设计技术要求

8.3.1.1 通用安全计算环境设计技术要求

8.3.1.2 云安全计算环境设计技术要求

8.3.1.3 移动互联安全计算环境设计技术要求

8.3.1.4 物联网系统安全计算环境设计技术要求

8.3.1.5 工业控制系统安全计算环境设计技术要

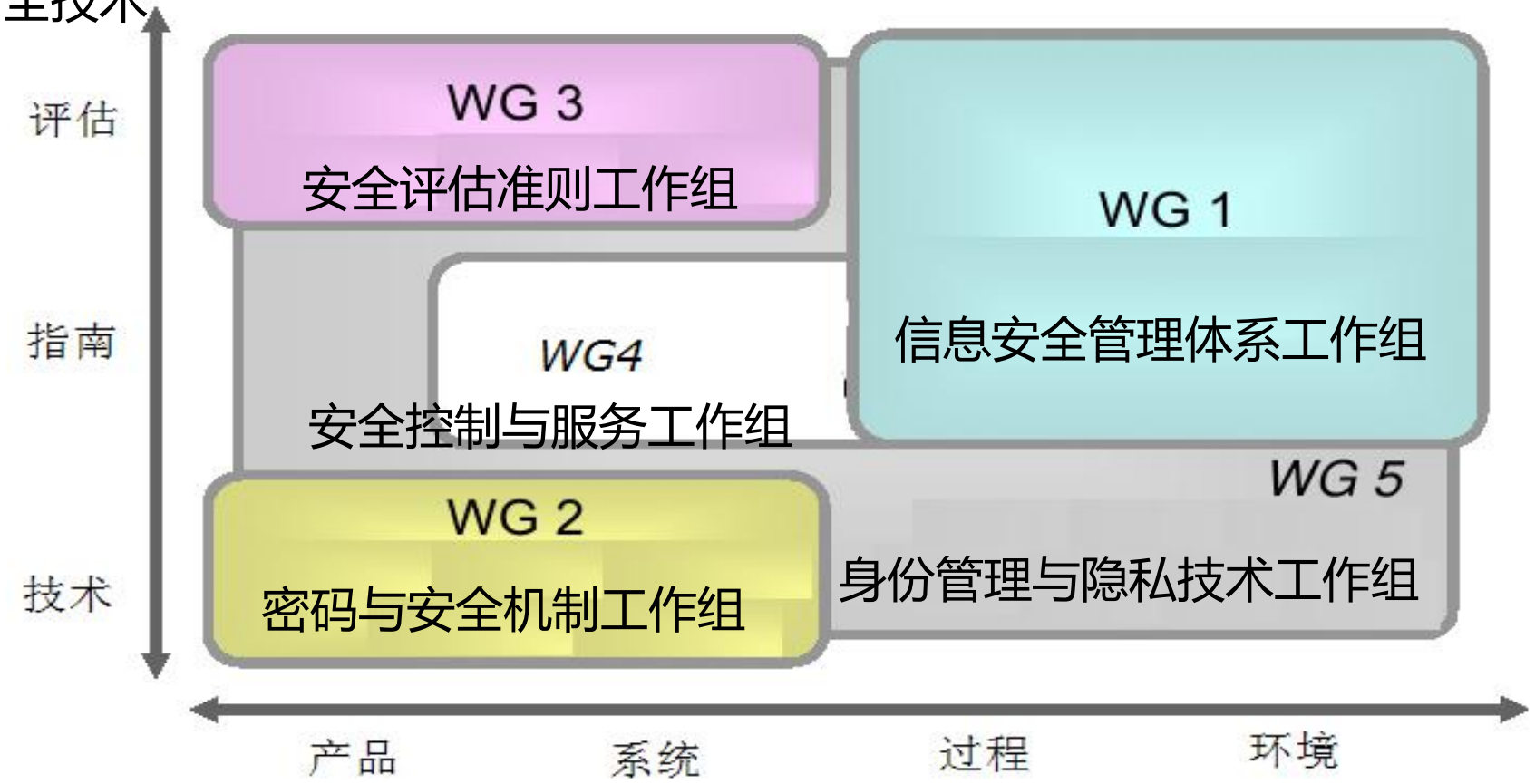
8.3.2 安全区域边界设计技术要求

8.3.3 安全通信网络设计技术要求

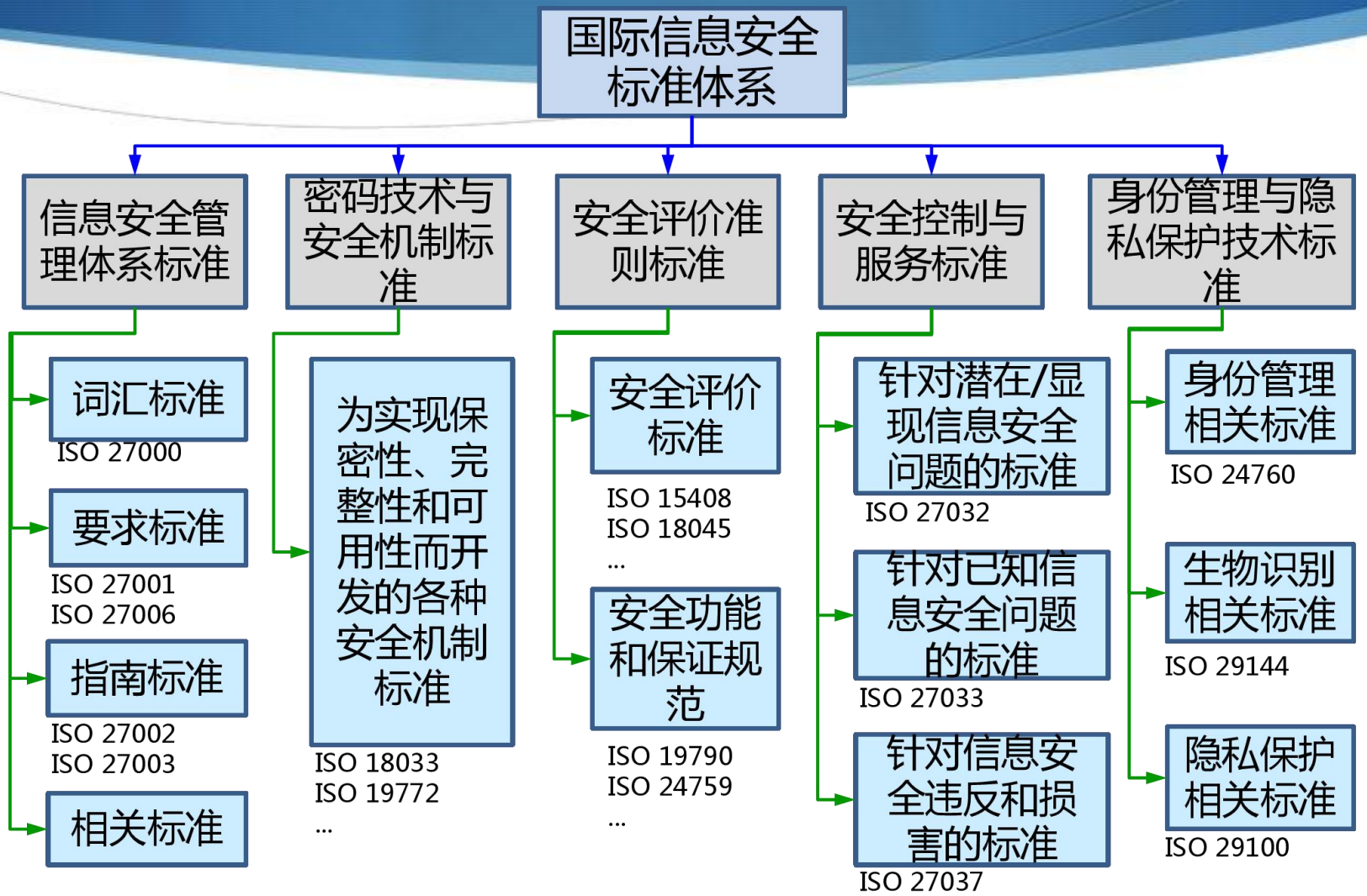
8.3.4 安全管理中心设计技术要求

国际信息安全标准化组织

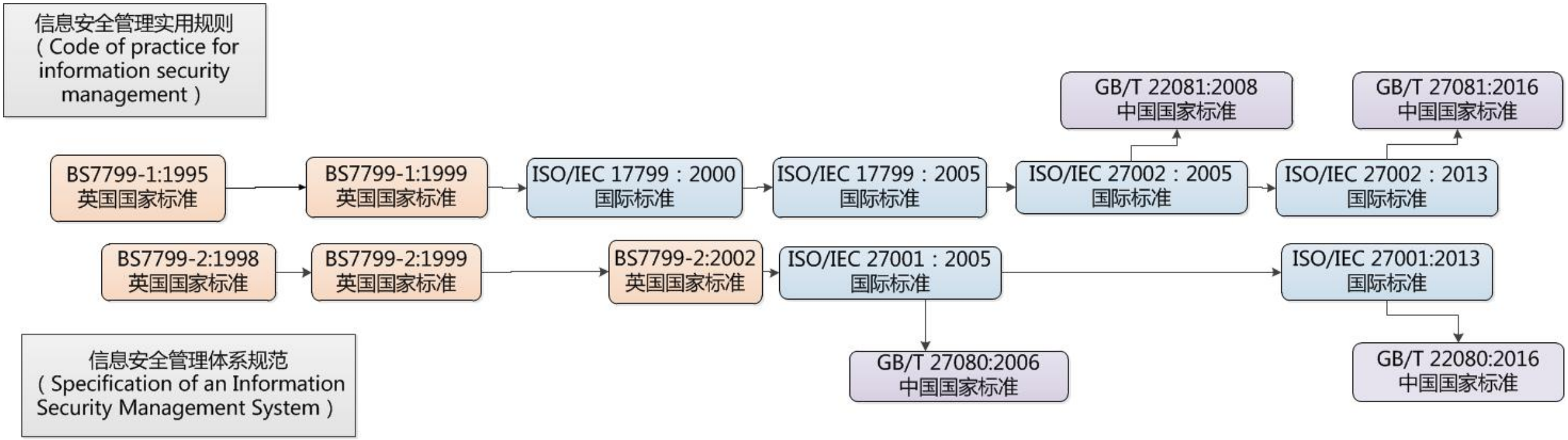
- ISO/IEC JTC1 SC27
  - 信息技术 安全技术



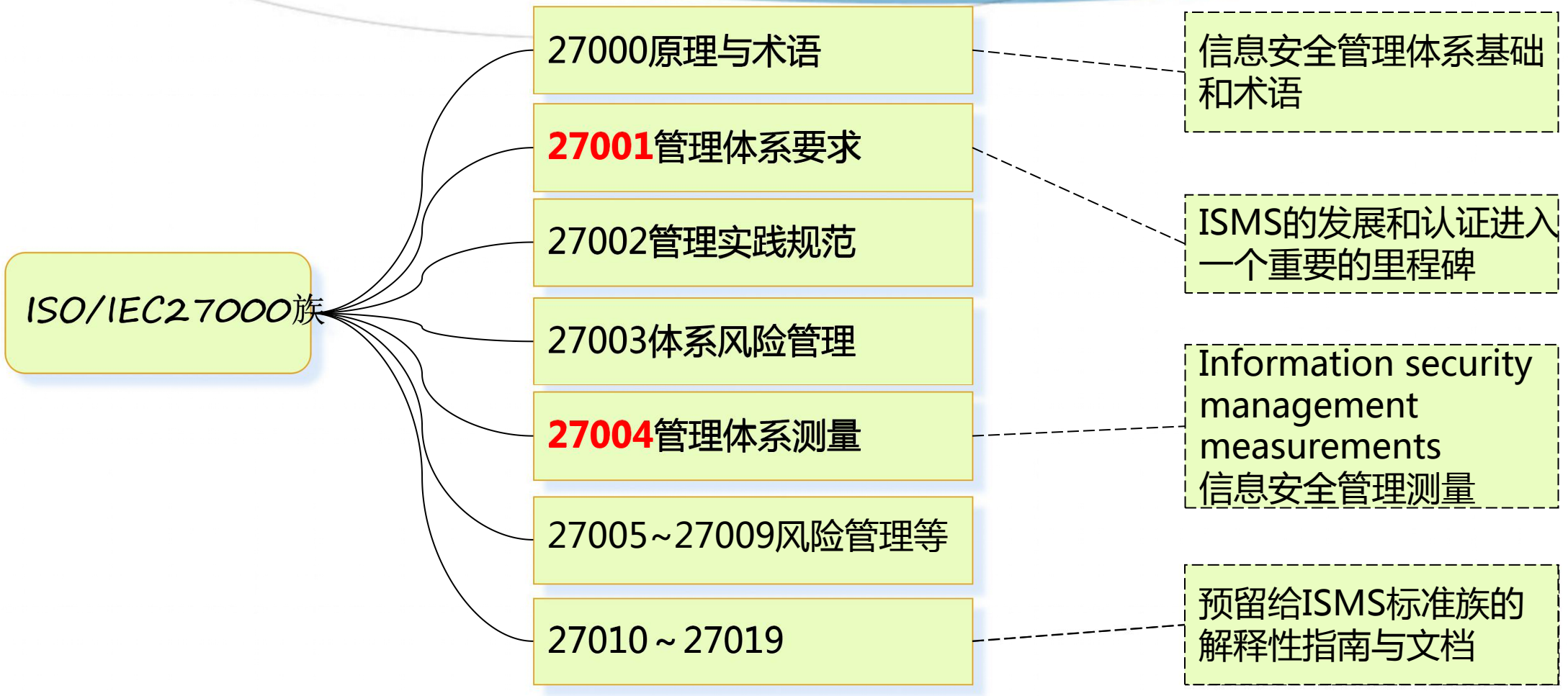
国际信息安全标准体系


国际信息安全标准体系
信息安全管理体系标准
密码技术与安全机制标准
安全评价准则标准
安全控制与服务标准
身份管理与隐私保护技术标准
词汇标准
ISO 27000
要求标准
ISO 27001
ISO 27006
指南标准
ISO 27002
ISO 27003
相关标准
为实现保密性、完整性和可用性而开发的各种安全机制标准
ISO 18033
ISO 19772
...
安全评价标准
ISO 15408
ISO 18045
...
安全功能和保证规范
ISO 19790
ISO 24759
...
针对潜在/显现信息安全问题的标准
ISO 27032
针对已知信息安全问题的标准
ISO 27033
针对信息安全违反和损害的标准
ISO 27037
身份管理相关标准
ISO 24760
生物识别相关标准
ISO 29144
隐私保护相关标准
ISO 29100

ISO27000发展


信息安全管理实用规则
(Code of practice for information security management)
BS7799-1:1995
英国国家标准
BS7799-1:1999
英国国家标准
ISO/IEC 17799：2000
国际标准
ISO/IEC 17799：2005
国际标准
ISO/IEC 27002：2005
国际标准
GB/T 22081:2008
中国国家标准
ISO/IEC 27002：2013
国际标准
GB/T 27081:2016
中国国家标准
BS7799-2:1998
英国国家标准
BS7799-2:1999
英国国家标准
BS7799-2:2002
英国国家标准
ISO/IEC 27001：2005
国际标准
ISO/IEC 27001:2013
国际标准
GB/T 27080:2006
中国国家标准
GB/T 22080:2016
中国国家标准
信息安全管理体系规范
(Specification of an Information Security Management System)

ISMS标准体系—ISO/IEC27000族介绍



ISO/IEC 27001

ISO/IEC 27000
Overview and vocabulary

ISO/IEC 27002

ISO/IEC 27003
ISMS implementation guide

ISO/IEC 27004
Information security measurements

ISO/IEC 27005
ISMS risk management

ISO/IEC 27006
Requirements for bodies providing audit and certification of ISMSs

/IEC 27007
ditor guidelines

New and Future Developments

ISMS for other sector specific areas

Information security management for inter-sctor communications (ISO/IEC 27010)

Newly Approved Project

ISO/IEC 27011
Telecoms ISMS requirements

ISMS for e-gov (ISO/IEC 27012)

Newly Approved Project

ISMS for the service sector (ISO/IEC 27013)

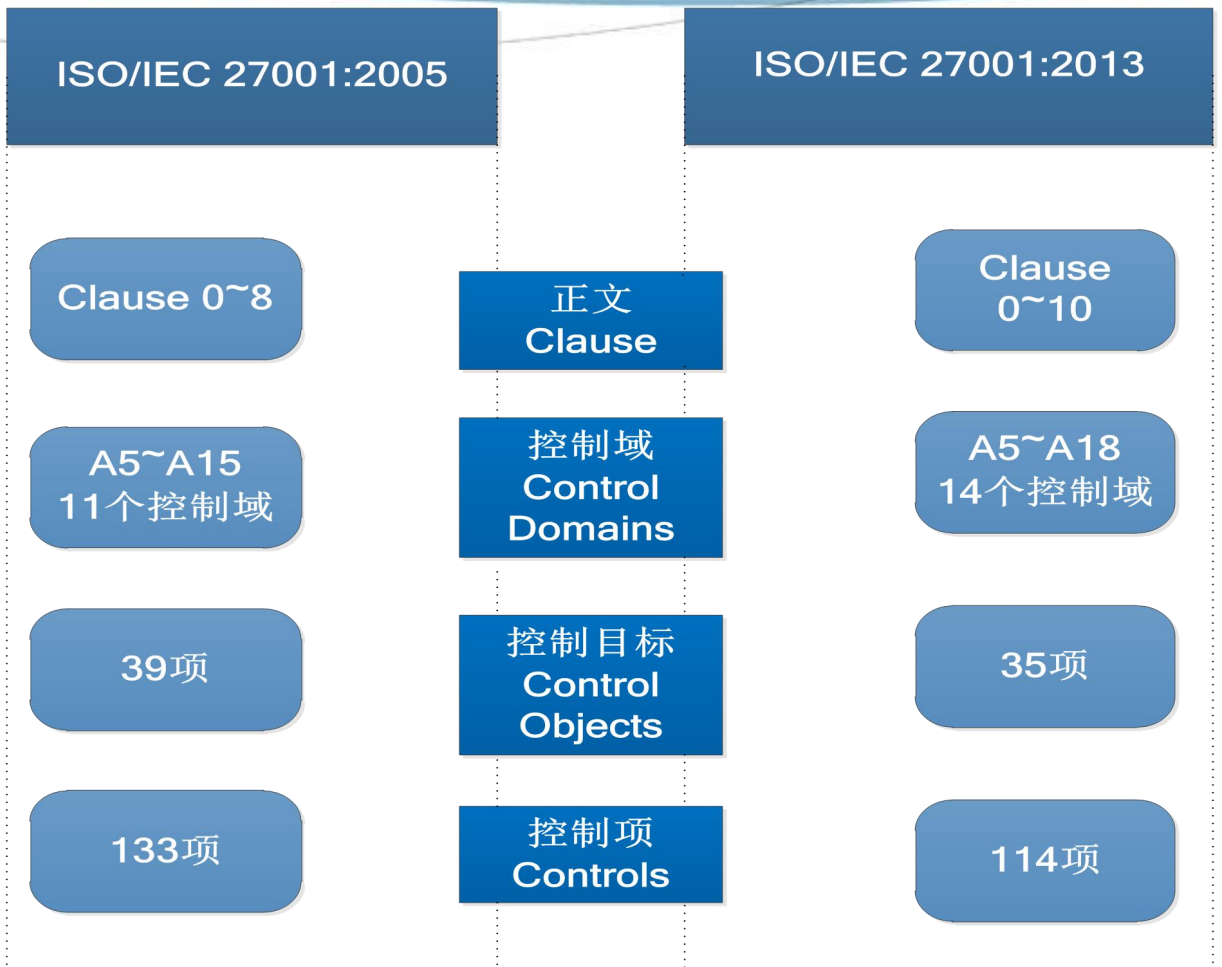
Proposed

Information security governance (ISO/IEC 27014)

ISMS for financial and insurance sectors (ISO/IEC 27015)

Proposed

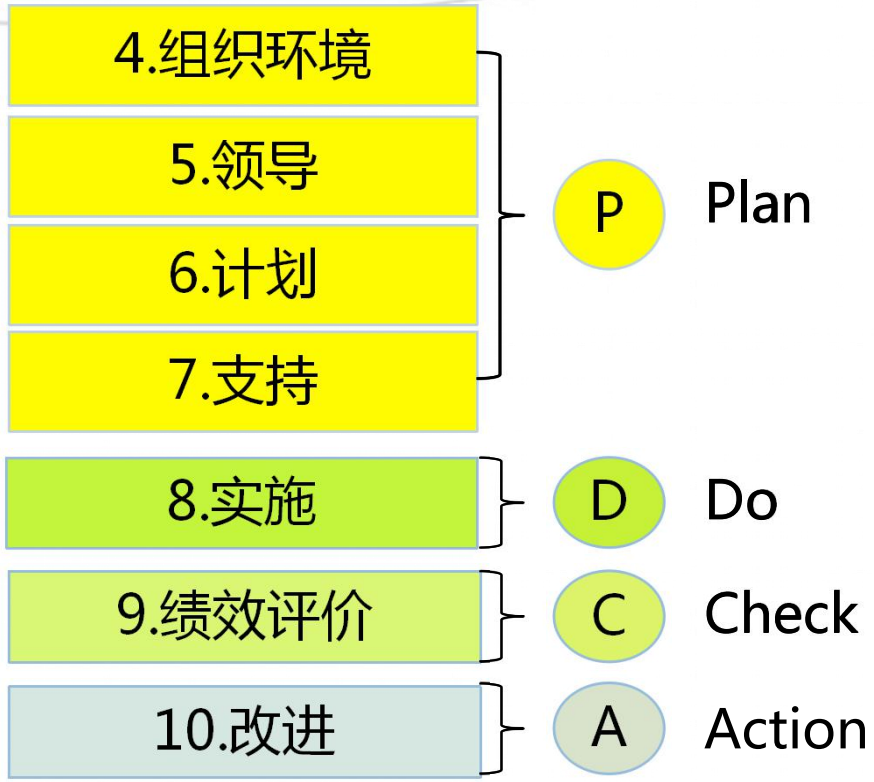
新旧27002标准结构对比



信息安全管理体系持续改进的PDCA循环过程

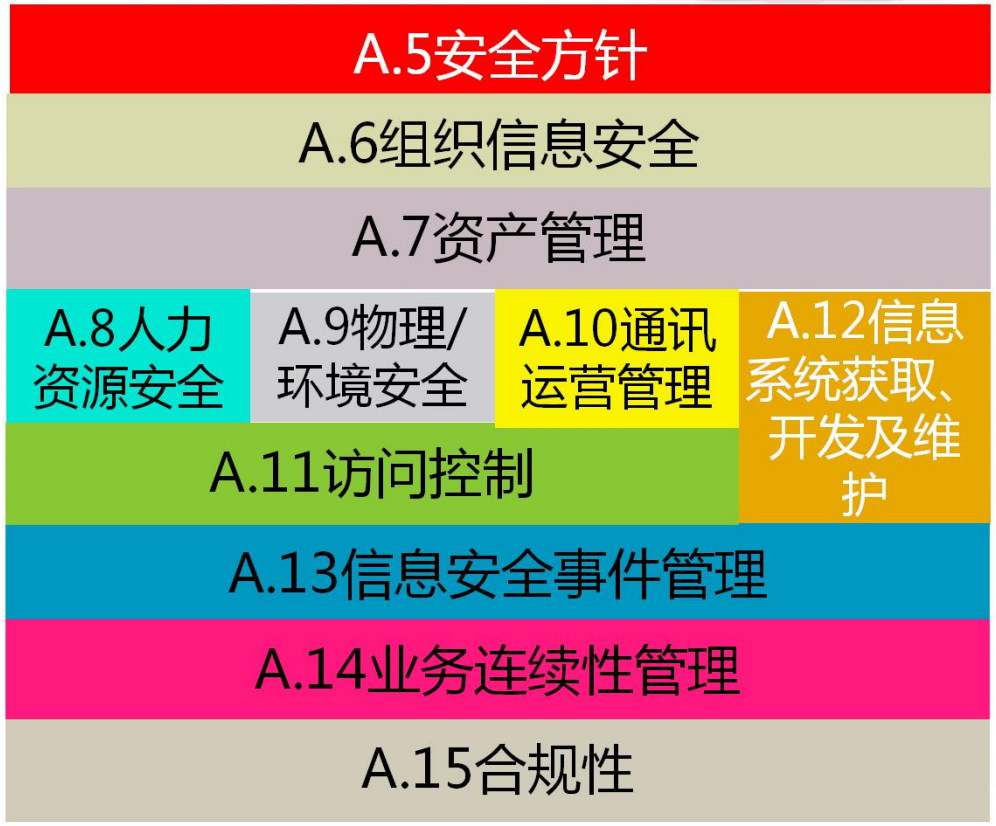
- 信息安全管理体系是PDCA动态持续改进的一个循环体

新27001标准对应PDCA

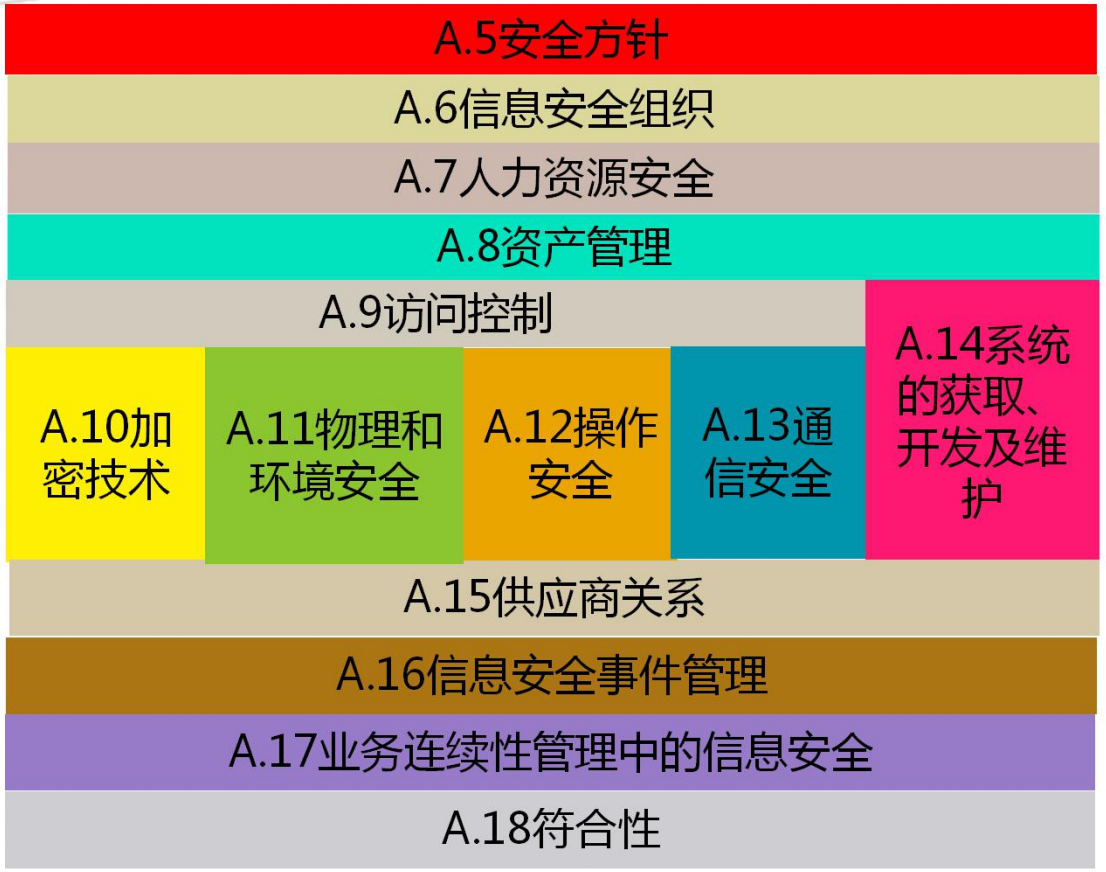


ISO/IEC27001:2013 文件结构与PDCA

新27002标准体系



旧27002



新27002

等级保护体系与ISO27001不同点

出发点不同

等级保护

- 保护国家安全、社会秩序和公共利益
- 指导全国安全工作
- 构建国家整体安全保障体系

ISO27000

- 保证组织业务连续性
- 缩减业务风险
- 最大化投资收益

出发点不同

等级保护

- 合规性要求
- 政策性要求
- 基本安全要求

ISO27000

- 承诺相对安全
- 内生性需求
- 额外安全要求

分级标准差异

等级保护

- 首先定级
- 根据级别提出安全要求
- 等级保护分等级考虑三方面影响：公民法人及其他组织合法权益社会秩序、公共利益、国家安全
- 按影响程度分为5个级别
- 以组织外部影响为依据

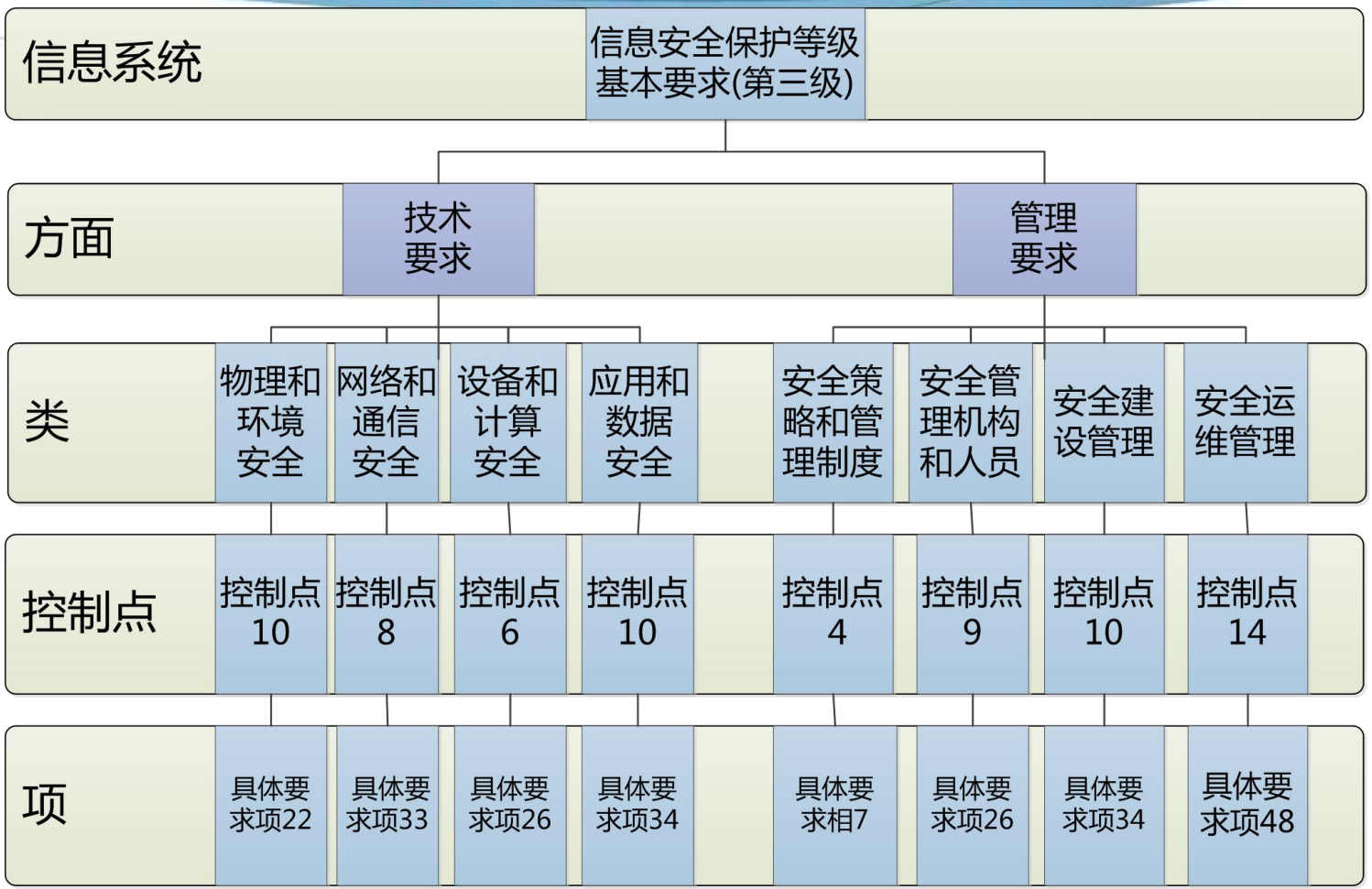
ISO27000

- 首先进行风险评估
- 根据资产、威胁、脆弱性、现有安全控制措施
- 定量或定性分级
- 由组织自行决定风险评估可接受程度
- 以组织内部业务影响为依据

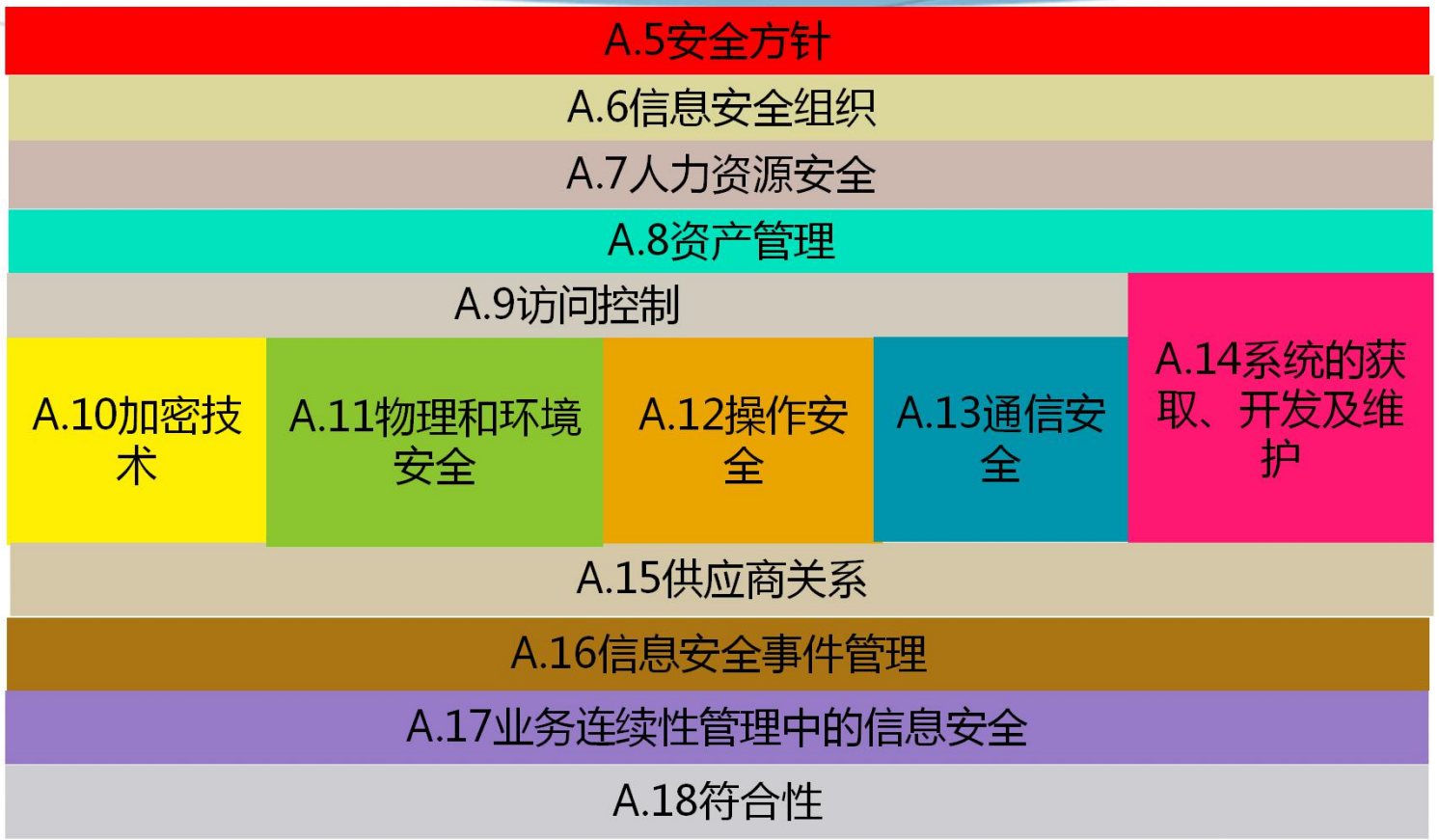
安全控制项、控制点差异

体系	目的	控制项	控制点
ISO/IEC27001	建立适合企业实际情况的信息安全管理体系	14个	35个控制项，114个控制点
等级保护	保障国家、人民、社会的信息安全	8个	二级69个控制点147个具体要求 三级71个控制点230个具体要求

等级保护基本要求组织形式

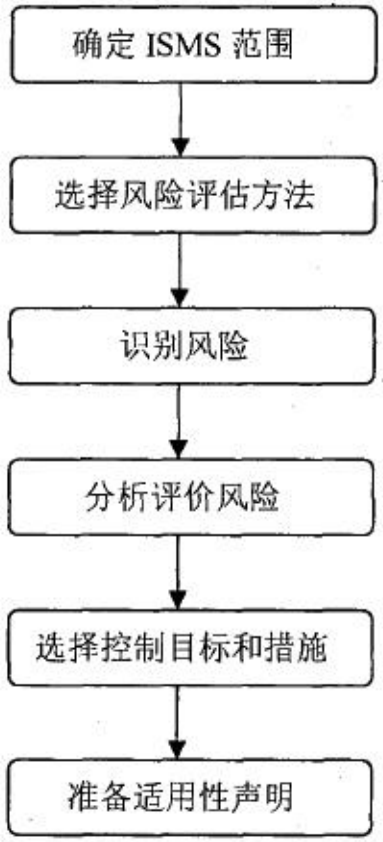


ISO/IEC27000标准体系要求

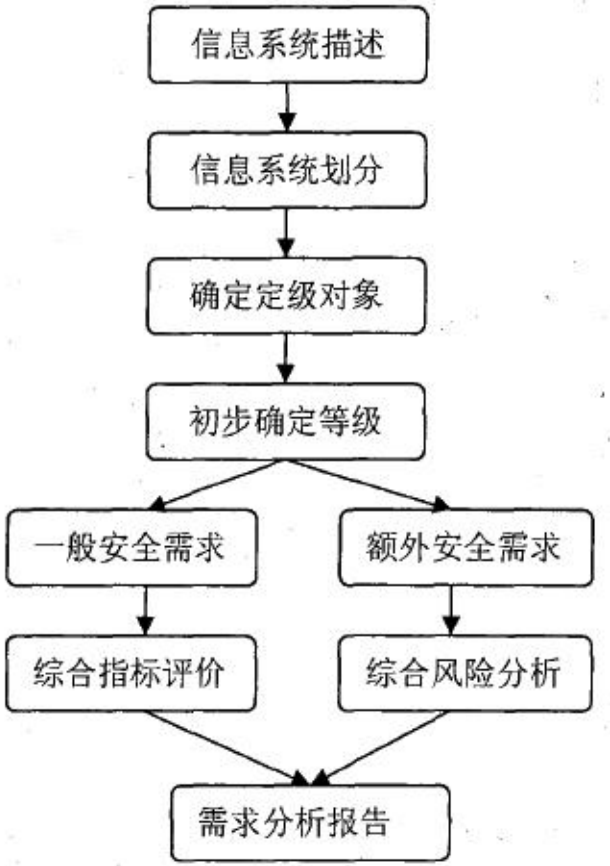


注：14个控制域，35个控制目标，114个控制措施

安全需求分析流程差异



ISO27000

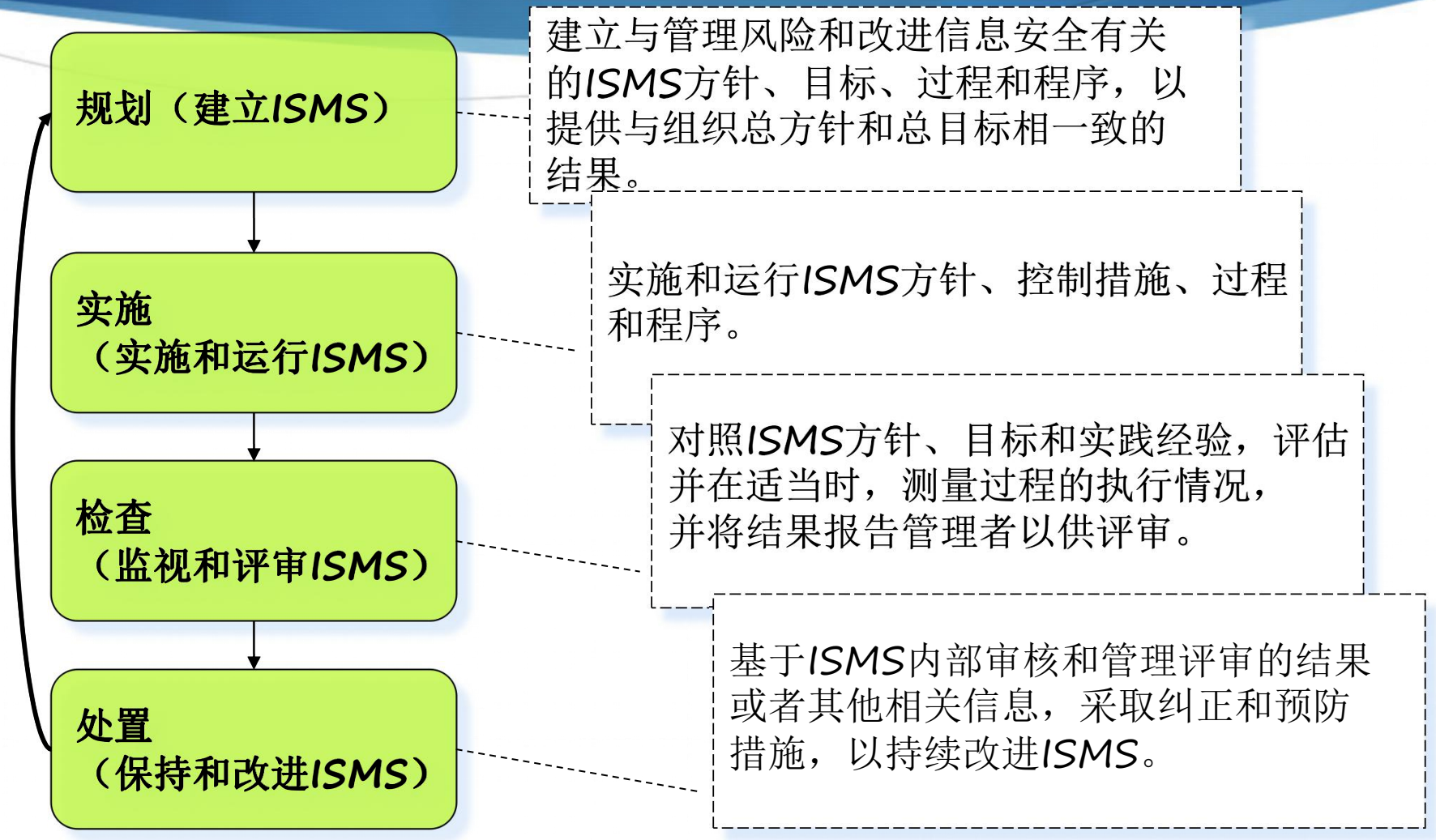


等级保护

等级保护实施流程


局部调整
总体规划
统
定
级
信
安全需求分析
安全总体设计
安全建设规划分析
安全保护等级确定
设计实施
安全方案详细设计
等级保护管理实施
等级保护技术实施
安全运维
运行管理和控制
变更管理和控制
安全状态监控
安全事件处置与应急预案
安全检查和持续改进
等级保护安全测评
信息系统备案
等级保护监督检查
系统终止
信息转移、暂存或清除
设备迁移或废弃
存储戒指的清除或销毁
重大变更

ISO27000体系实施流程



等级保护与ISO27001相似点

风险处理思想相同

安全是相对的，不安全是绝对的！

- 不追求百分之百的安全，目标是达到低于可接受风险的相对安全

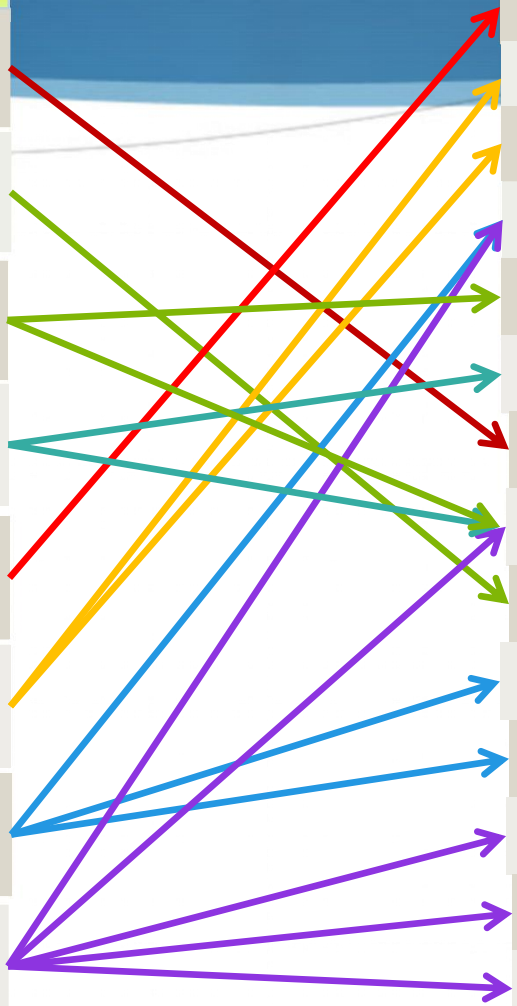
实施前强调分级分类，找出信息安全保护重点、要点

把有限的资源投入到关键部位

- 木桶原理：保护木桶最短的几块木板
- 不再“眉毛胡子一把抓”！

安全分类共同点

等级保护2.0 8个域
物理和环境安全
网络和通信安全
设备和计算安全
应用和数据安全
安全策略和管理制度
安全管理机构和人员
安全建设管理
安全运维管理



ISO/IEC27002的14个域
信息安全策略
信息安全组织
人力资源安全
资产管理
访问控制
密码学
物理和环境安全
操作安全
通讯安全
系统的获取、开发及维护
供应商关系
信息安全事件管理
业务连续性管理的信息安全方面
符合性

宏观与微观相辅相成

- 两个体系均认识到：
  - 信息系统分布于各个组织内部
  - 组织内部的信息安全是国家整体安全基础
  - 国家整体安全体现在各个组织微观能力上
  - 组织的风险同时来自于内部和外部
  - 没有国家宏观信息安全也没有组织内部信息安全

覆巢之下岂有完卵！

等级保护与ISO27000实施问题

ISO27000实施难点

- 风险评估方法选择困难、实施难度大、耗时长、成本高
- 如何选择控制措施困难，如何有重点针对性的选择控制措施更难

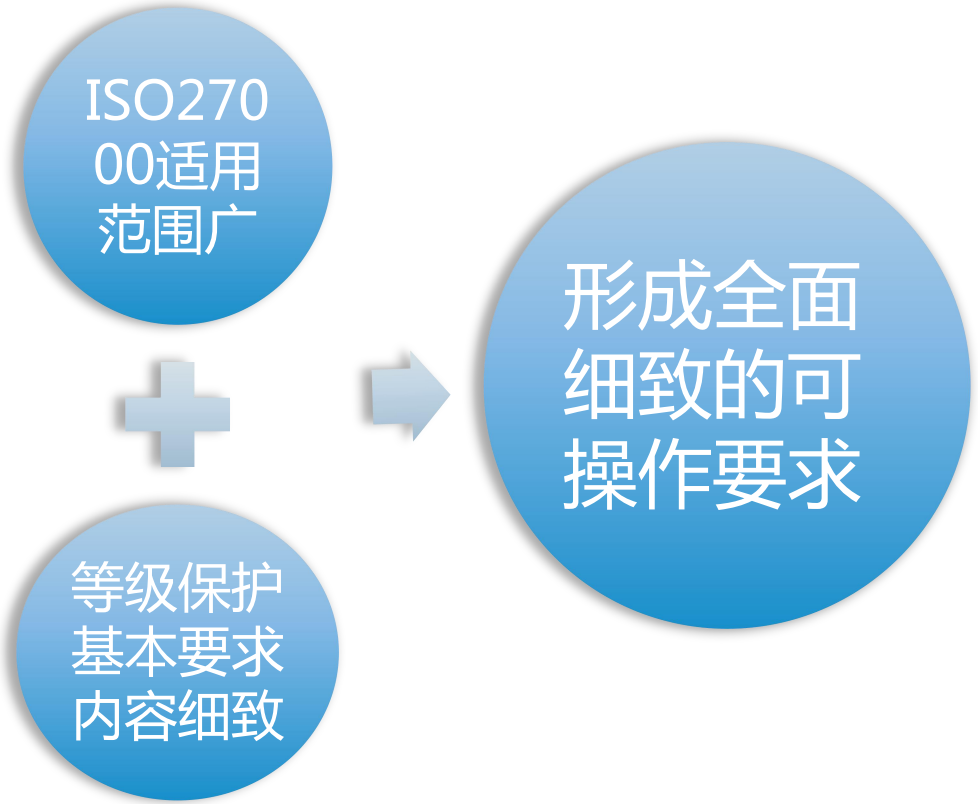
等级保护实施过程不足

- 虽预留特殊安全保护需求，但对大型系统，宏观分级无法细化到具体要求
- 以国家安全、社会秩序和公共利益为出发点，对特定行业单位内生性需求未考虑，导致管理者对推动等保落地的意愿不足

等级保护与ISO27000互相补充促进

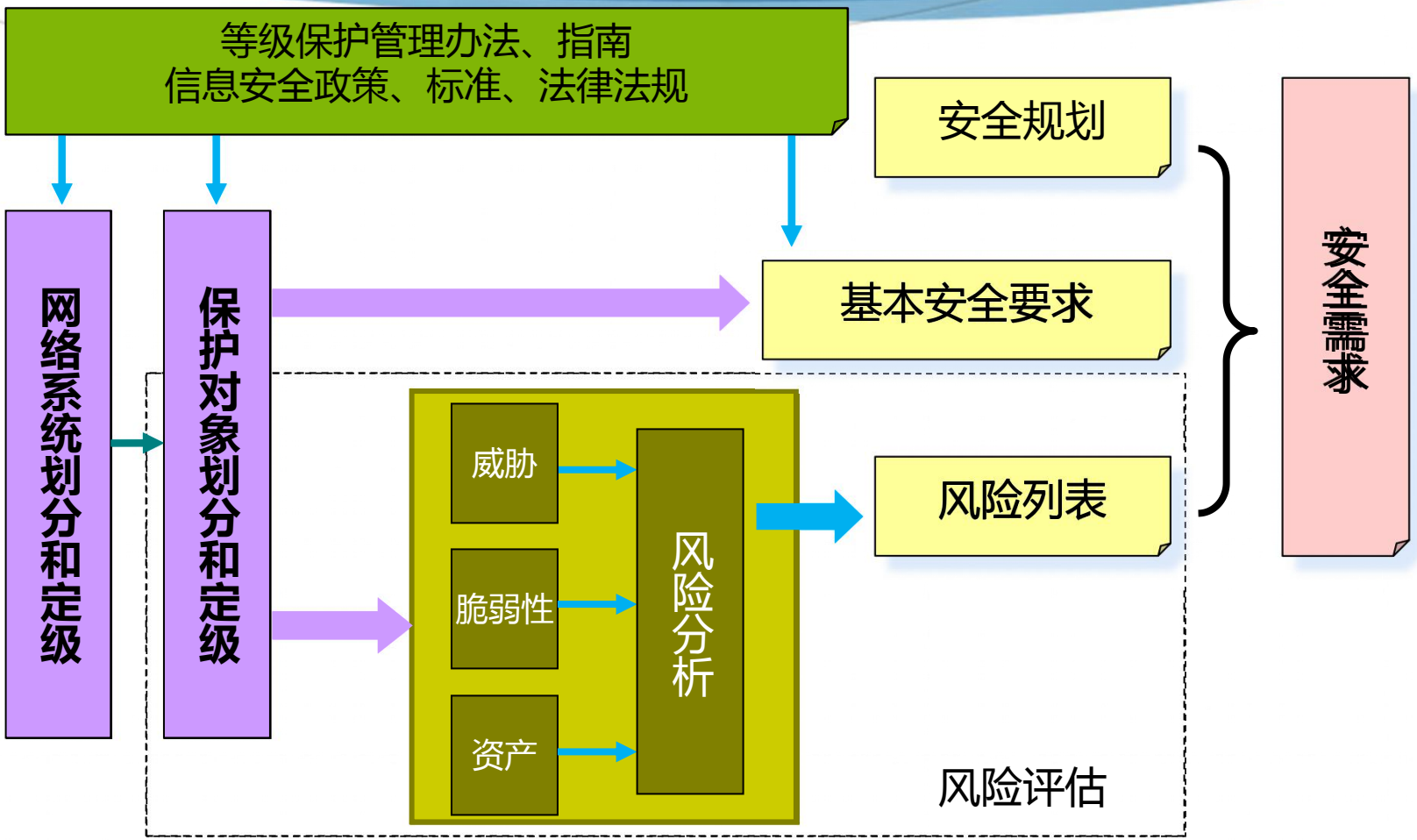
内容的相互补充

两体系融合形成全面细致要求

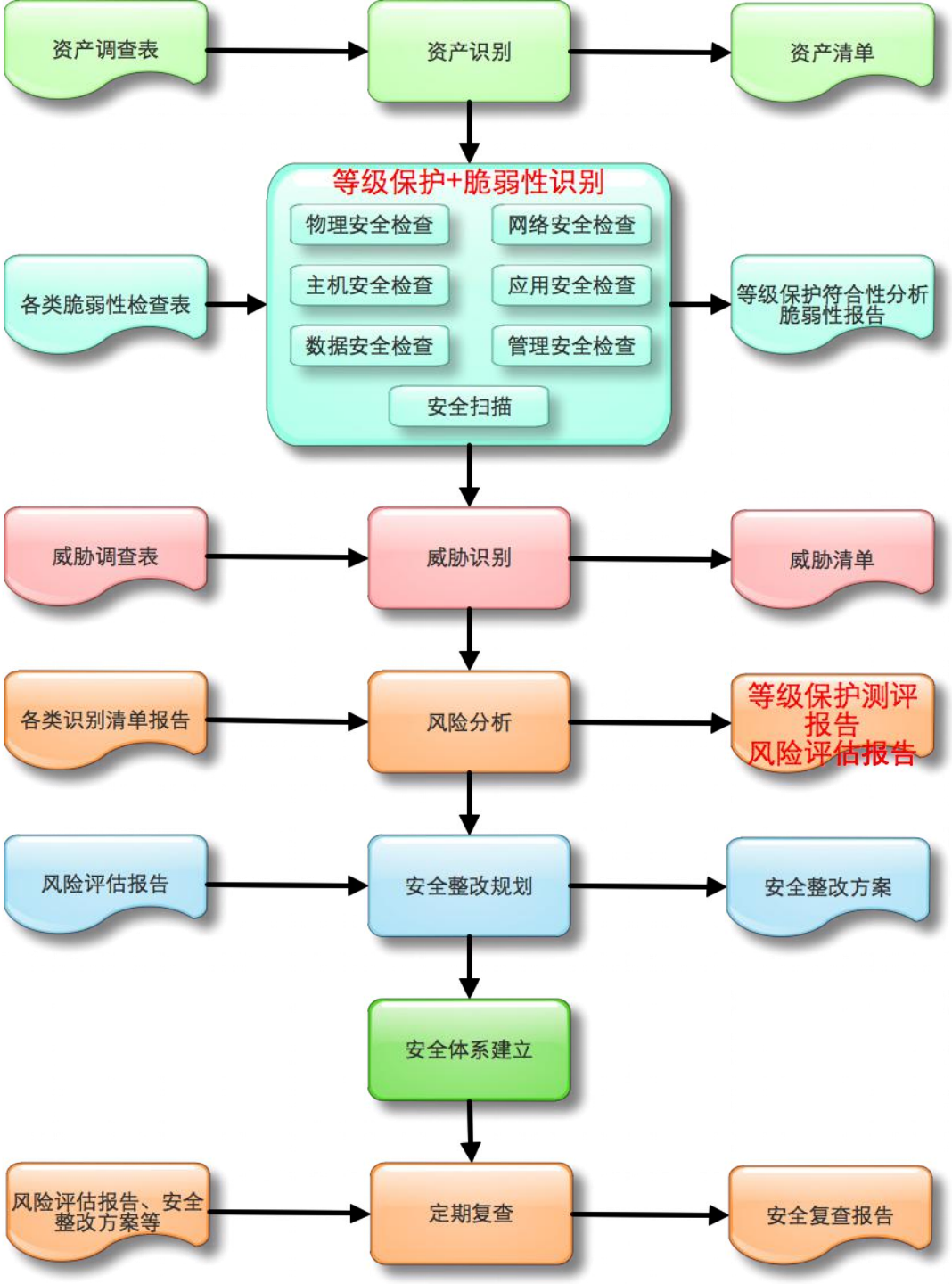


两体系互补形成新控制集合

实施过程的融合


等级保护管理办法、指南
信息安全政策、标准、法律法规
网络系统划分和定级
保护对象划分和定级
安全规划
基本安全要求
风险列表
安全需求
威胁
脆弱性
资产
风险分析
风险评估

融合等级保护测评与风险评估的实施过程



结合等级保护测评的风险评估流程

策划阶段

- 进行系统定级、明确SOA范围
- 制定安全方针，实施风险评估
- 从整合控制措施集合选择控制措施
- 制定风险处置计划，形成体系文件

实施阶段

- 按风险处置计划实施控制措施
- 进行安全意识、技能培训
- 进行各类技术管理安全整改

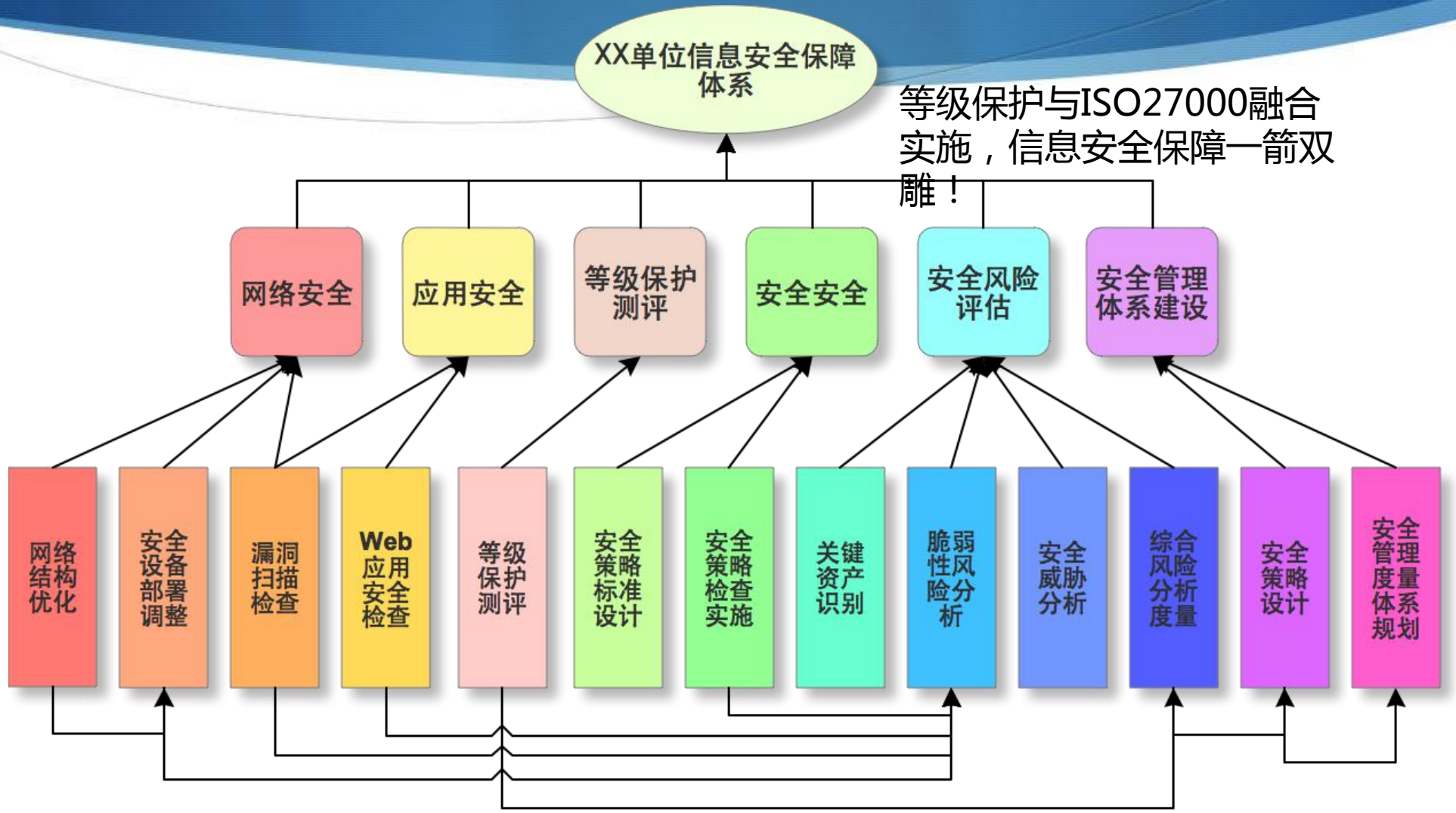
检查阶段

- 执行内部审核，检查等级保护目标和ISO27001符合性
- 实施管理评审，评审等级保护措施和体系有效性
- 识别可改进之处，保证体系适宜性、充分性和有效性

处置阶段

- 实施各类改进措施
- 进行预防和纠正措施
- 持续改进安全保证能力

结论



等级保护与ISO27000融合实施，信息安全保障一箭双雕！

谢谢