高校信息安全管理体系实践与思考

中国科学技术大学
信息安全测评中心
蒋凡

信息化需要管理。这种管理不是对信息化的单个要素进行碎片式的管理，而是要重注管理好各个要素之间的关系。信息化本身是一个有机的整体，互联网是信息化的重要基础设施，只有把互联网的管理放在信息化的大视野中看待，才能找到更加合适的管理手段和方式。

自我介绍

蒋凡
中国科学技术大学计算机科学与技术学院教授
中国科学技术大学信息安全测评中心主任
ISO/IEC JTC 1/SC6 WG9 中国专家组成员
ISO/IEC JTC 1/SWG 5 中国专家组成员
信息安全等级保护高级测评师

主要研究方向：测试与测试控制语言（TTCN），信息安全

电子邮箱；fjiang@ustc.edu.cn

目录

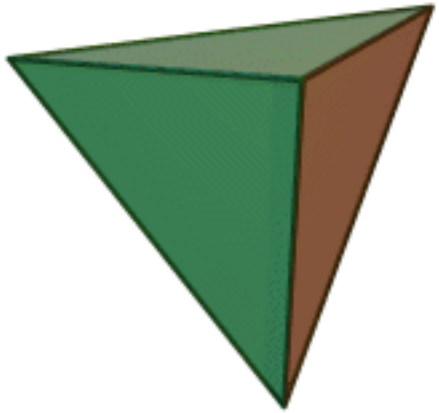
本讲义取材主要来源于上海天帷企业管理咨询公司的丁劲松先生，在此表示感谢！

信息安全管理体系基础

1) 信息安全管理基本术语与概念

2) 如何确定信息安全管理的目标与关注焦点

3) ISO27001对信息安全管理目标的要求

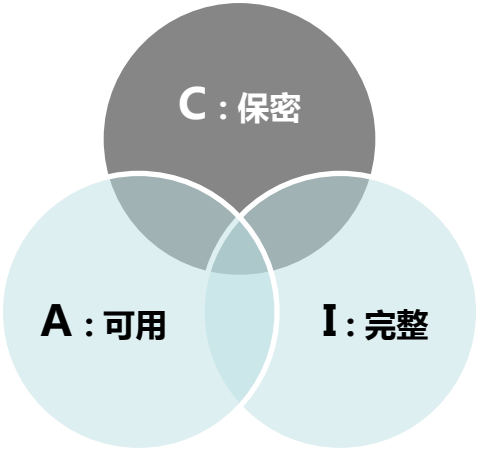


信息安全的基本术语

保密性（Confidentiality ）

完整性（Integrity ）

可用性（Availability ）



真实性（Truth）

可核查性（accountability ）

不可否认性（non-repudiation）

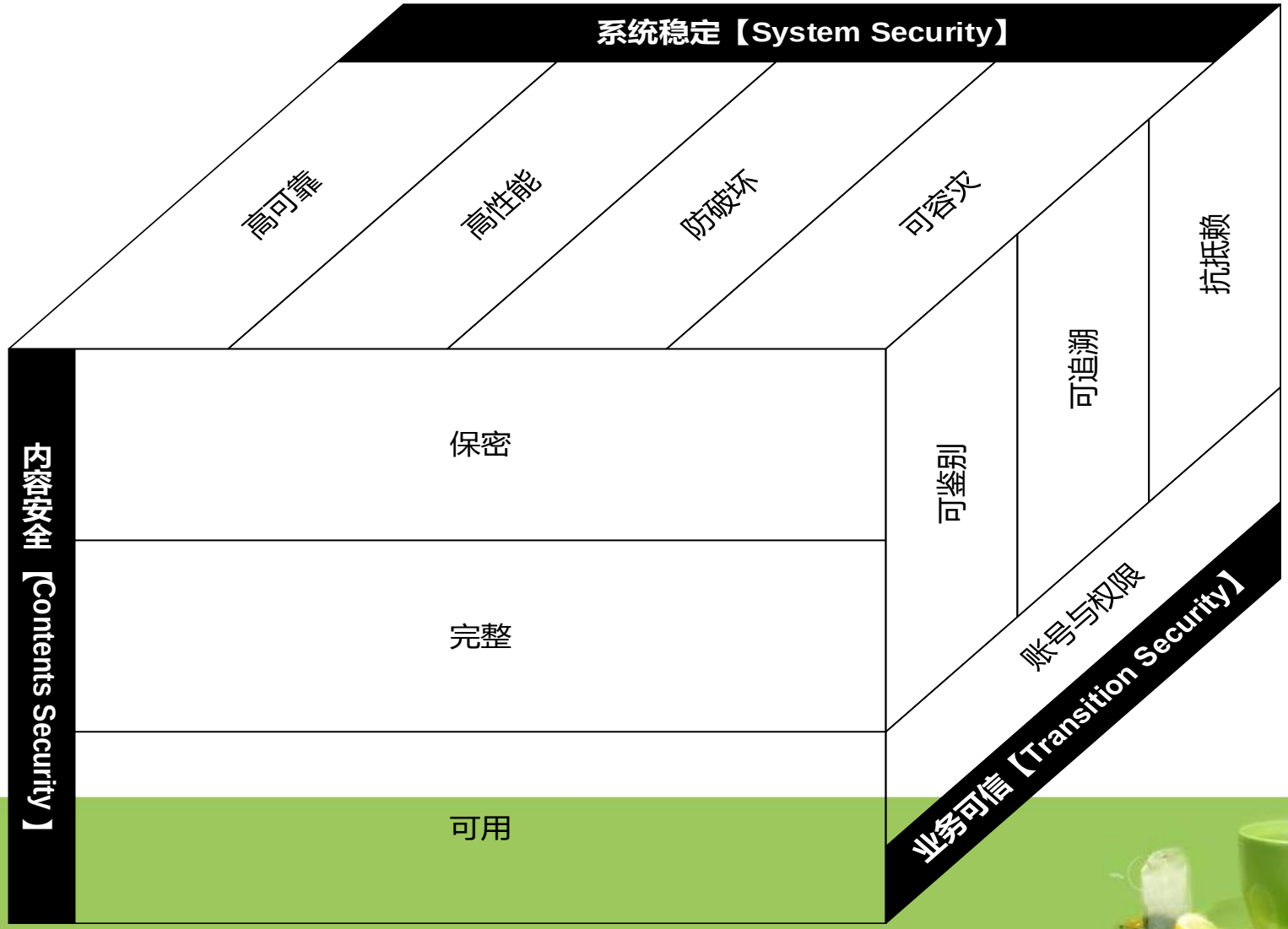
可靠性（ dependability，availability,reliability,maintainability ）等

---：ISO/IEC 27000:2012

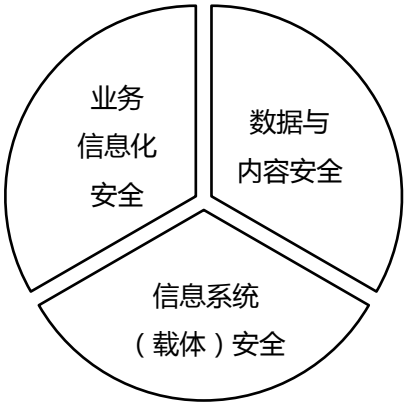
信息安全管理的关注点

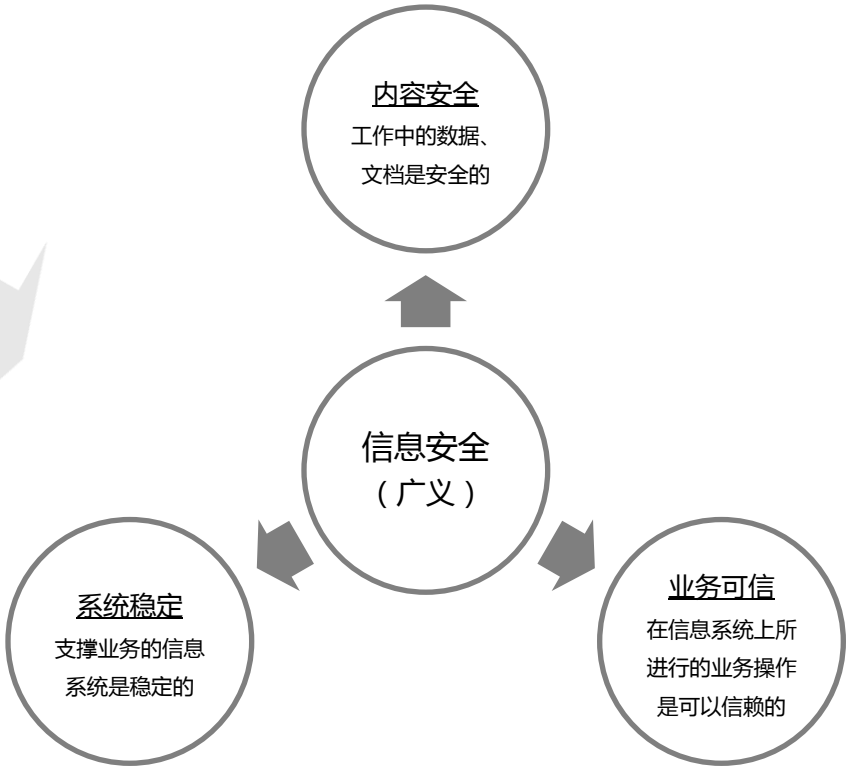
- 业务数据会不会出问题？
  - 会不会泄密或被人窃取？
  - 会不会被人篡改？
  - 会不会有无法恢复的损失和丢失？
- 信息系统内所进行的业务操作会不会有问题
  - 会不会有人冒名操作？
  - 会不会不认账？
- 信息系统会不会出问题？
  - 系统会不会中病毒？
  - 系统会不会停机？
  - 系统会不会遭到破坏和攻击？

信息安全目标模型(CTS)



信息安全保护的对象


业务
信息化
安全
数据与
内容安全
信息系统
（载体）安全


内容安全
工作中的数据、
文档是安全的
信息安全
（广义）
系统稳定
支撑业务的信息
系统是稳定的
业务可信
在信息系统上所
进行的业务操作
是可以信赖的

ISO2700X系列标准的概要介绍

1) ISO27001标准概要介绍

2) ISO2700X系列标准概要介绍

以信息或信息流为中心

ISO27001是以信息为中心（而不是以信息系统或信息载体为中心）的安全管理标准，重点关注与C、I、A相关的风险。

ISO/IEC 27001:2013 6.1.2 c) ：应利用信息安全风险评估过程，以识别ISMS范围内的信息丧失保密性、完整性和可用性的风险

等级保护是以信息系统为中心的安全管理标准，重点关注的是信息系统可能遭受的攻击和破坏（系统稳定）。

ISO/IEC 27001的三大构成要素

从组织的整体业务风险的角度，为建立、实施、运行、监视、评审、保持和改进文件化的ISMS规定了要求。

❶持续改进的框架 - 戴明循环 /过程方法

❷风险管理的理念

❸来自行业的最佳实践

持续改进框架

4. 组织背景
- 理解组织现状及背景
- 确理解利益相关方的期望
- 定ISMS的范围
- 建立ISMS

5. 领导作用
- 领导作用和承诺
- 方针
- 角色、责任和授权

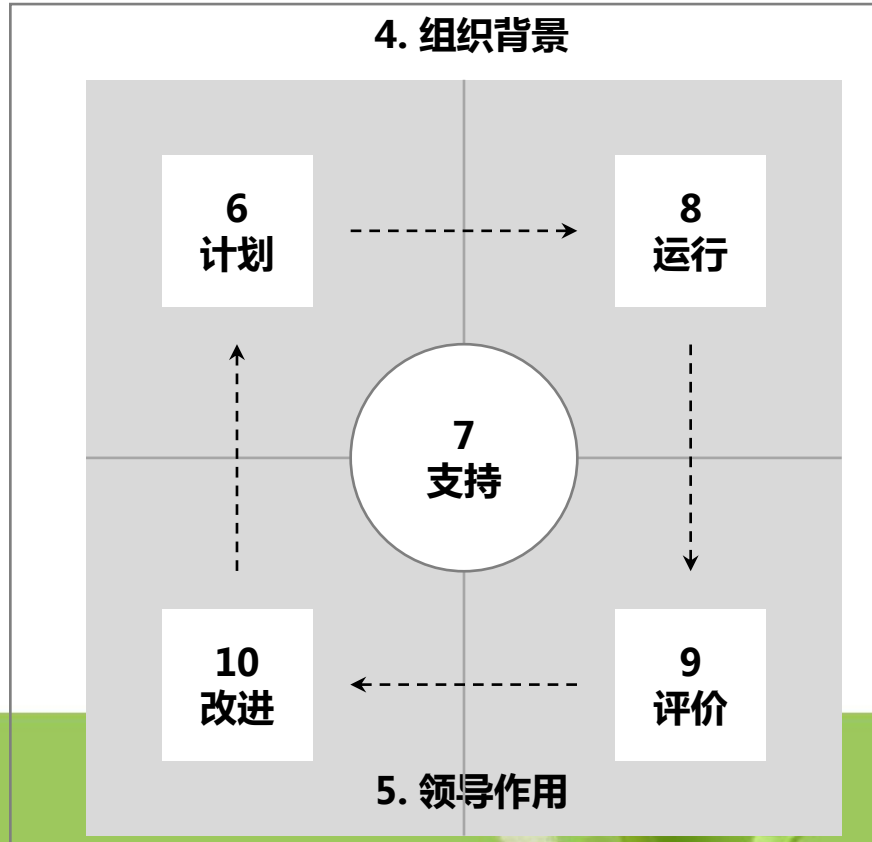
6. 计划
- 处理风险和机会的行动
- 信息安全目标及达成计划

7. 支持
- 资源
- 能力
- 意识
- 沟通
- 文件花信息

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

9. 绩效评价
- 监控、度量分析和评价
- 内部审核
- 管理评审

10.改进
- 不符合及纠正措施
- 持续改进

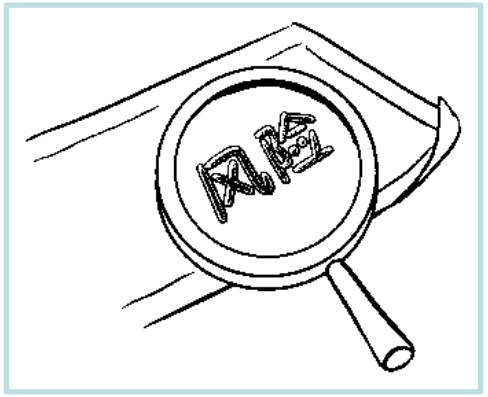


风险评估的概念

- 风险

  事态的概率及其结果的组合

  [ISO Guide 73：2002]



- 风险管理

  指导和控制一个组织相关风险的协调活动

  注：风险管理一般包括风险评估、风险处置、风险接受和风险沟通

  [ISO Guide 73：2002]

14个控制域

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

27001及其相关标准

ISO/IEC 27001:2013 Information security management systems -- Requirements		
• ISO/IEC 27000:2014 • ISO/IEC 27002:2013 • ISO/IEC 27003:2010 • ISO/IEC 27004:2009 • ISO/IEC 27005:2011 • ISO/IEC 27013:2012 • ISO/IEC 27014:2013 …	• ISO/IEC 27006:2011 • ISO/IEC 27007:2011 • ISO/IEC TR 27008:2011 • …	• ISO/IEC 27010:2012 • ISO/IEC 27011:2008 • ISO/IEC TR 27015:2012 • ISO/IEC TR 27016:2014 • ISO/IEC DR 27017:2014（云计算） • ISO/IEC TR 27019:2013 • …
Supporting Guideline	**Accreditation Requirements and Auditing Guidelines**	**Sector Specific Requirements and Guidelines**

如何策划信息安全管理体系框架？

1) 策划信息安全管理体系要考虑哪些要素？

2) 有哪些可以选择的体系框架实现方式？

3) 如何实现管理措施（标准）与技术措施（技术标准的融合?

4) 如何实现多标准的融合?

5) 如何实现与等级保护多个监管要求的融合

1. 策划信息安全管理体系要考虑哪些要素？

- 物理安全
- 设备安全
- 逻辑安全
- 网络安全
- 系统安全
- 人员安全
- 开发安全
- 建设安全
- 运维安全
- 安全管理
- 安全治理
- 安全技术
- 病毒防范
- 攻击防范
- 防火墙
- 防毒墙
- 访问控制
- 身份管理
- 权限管理
- 应用安全
- 网站安全
- 数据安全
- 主机安全
- 商业秘密保护

…

1. 策划信息安全管理体系要考虑哪些要素？

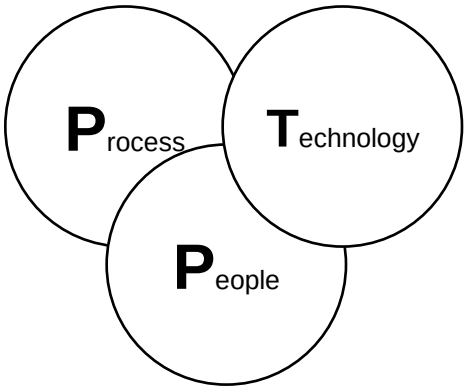
- **安全措施的预期目标**
  - ✓ 哪些安全目标是我们需要重点考虑的？
- **安全管理措施全面性的问题**
  - ✓ 需要实施哪些措施，才能确保安全控制措施不会存在缺项？
- **控制措施之间的关联关系的问题**
  - ✓ 如何实现管理措施、技术措施、人员职责之间的有机结合？
- **体系融合的问题**
  - ✓ 多种体系的融合，ISO27001/CMMi/ITIL？
- **体系落地的问题**
  - ✓ 如何与日常的工作结合？
- **合规要求的问题**
  - ✓ 多种监管要求：等级保护、科技风险、外包、数据中心、应急？
  - ✓ 如何确保减少重复的工作？

1. 策划信息安全管理体系要考虑哪些要素？

---- 摘自ISO/IEC 27002:2005

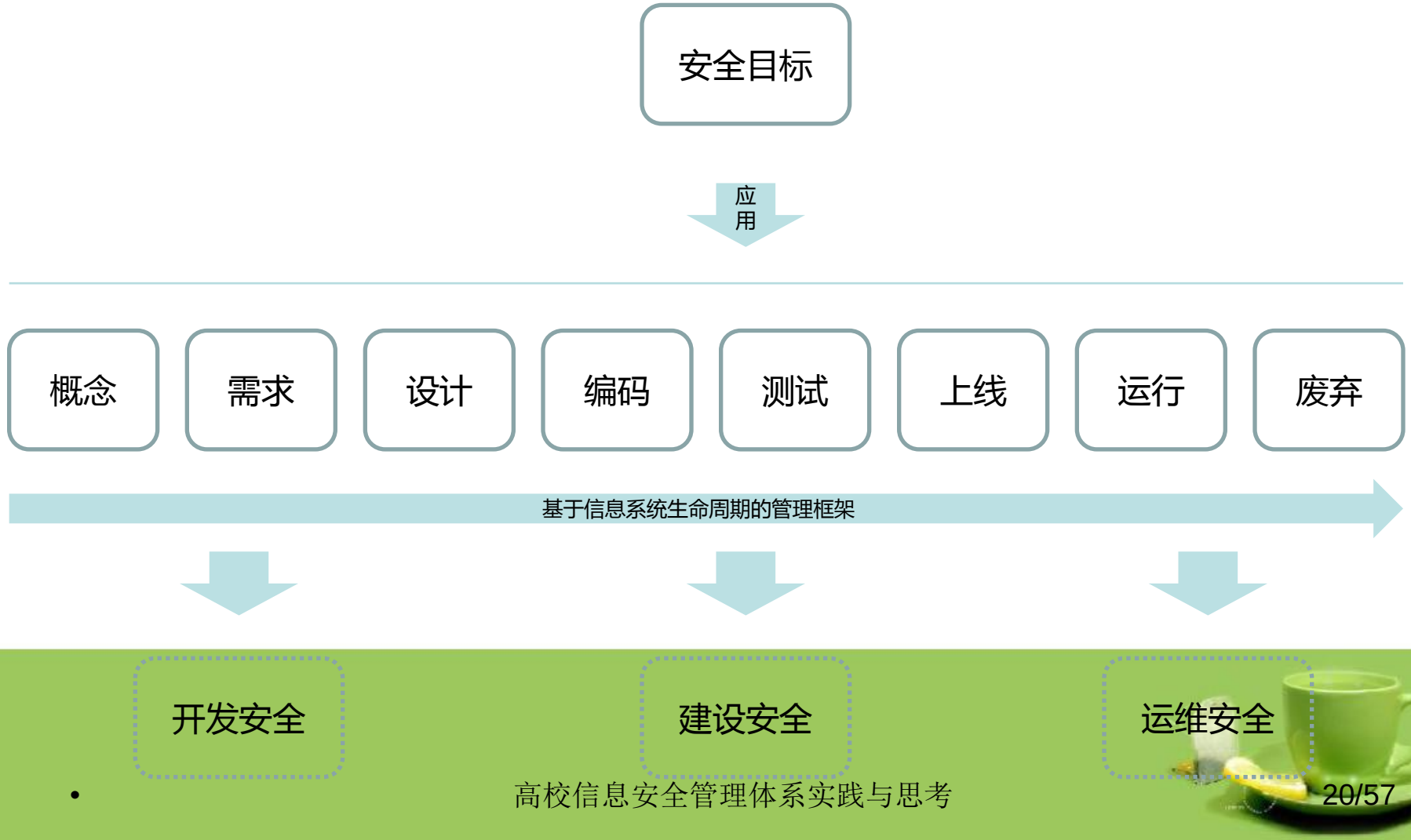
通过实施一系列的控制措施来达到安全的效果，包括方针策略

- ✓过程和程序
- ✓组织结构
- ✓软件和硬件功能



2. 如何实现管理措施与技术措施的融合

- 管理措施与实际工作流程的整合



技术体系与管理体系的融合

技术规范

技术基线

应用

应用

建设期

运维期

概念 | 需求 | 设计 | 编码 | 测试 | 上线 | 运行 | 废弃

基于信息系统生命周期的管理框架

产生

技术方案

3. 有哪些可以选择的体系框架实现方式？

- 基于标准条款

✓ 以管理要求为核心，按照ISO/IEC 27001:2005的管理要求，制定相应的管理规章和制度

- 基于管理对象

✓ 以管理对象为核心，按照资产的类别，如数据/应用/主机/网络/环境（数据中心）等，制定针对特定对象的管理规章和制度

- 基于工作流程

✓ 以日常工作流程或工作内容为核心，制定相应的日常运活动的管理规章和制度

3. 有哪些可以选择的体系框架实现方式？

基于标准条款

- 优点
  - 便于实现ISO27001的要求，
  - 实施方便/快捷/简单
- 缺点
  - 不利于融合其他标准要求
  - 不利于落实到日常工作中

3. 有哪些可以选择的体系框架实现方式？

基于标准条款

- 优点
  - 便于实现ISO27001的要求，
  - 实施方便/快捷/简单
- 缺点
  - 不利于融合其他标准要求
  - 不利于落实到日常工作中

3. 有哪些可以选择的体系框架实现方式？

基于日常流程

- 优点
  - 便于将来的落实
  - 理解简单
- 缺点
  - 不利于考虑技术性风险，主要关注人员操作所带来的风险

3. 有哪些可以选择的体系框架实现方式？

基于管理对象： 以管理对象为核心，按照资产的类别，如数据/应用/主机/网络/环境（数据中心）等，制定针对特定对象的管理规章和制度

▪优点

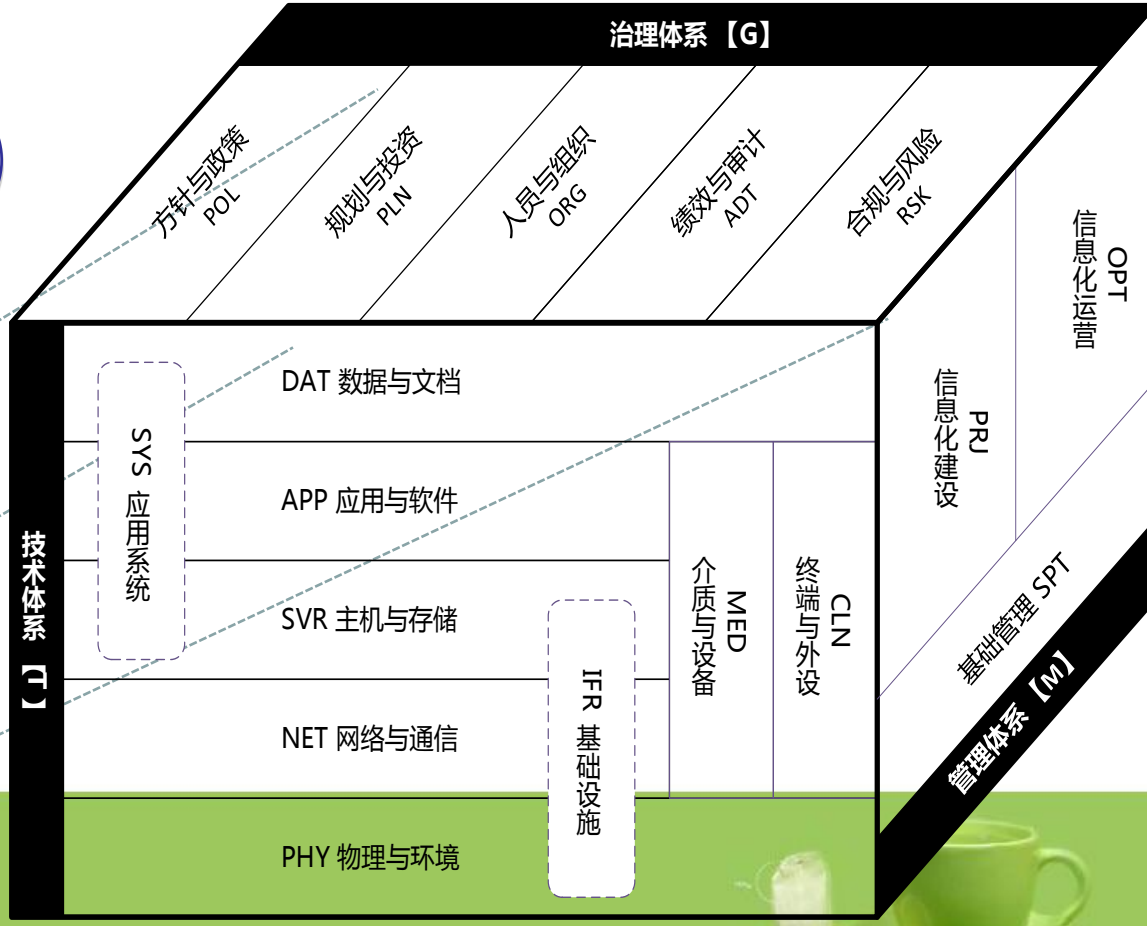
- 便于技术措施的落实
- 理解简单

▪ 缺点

- 缺乏对流程及管理性风险的考虑

3. 有哪些可以选择的体系框架实现方式？（TMG）

通过对300多项信息安全管理标准和技术标准（包括等级保护、工控安全等）的研究和分析，将安全控制措施划分为治理、管理、技术3大领域，18个模块。



把管理措施融合到基础管理工作中

把管理措施融合到技术设施与架构中

把管理措施融合到系统生命周期中

基于TMG模型的实现方式

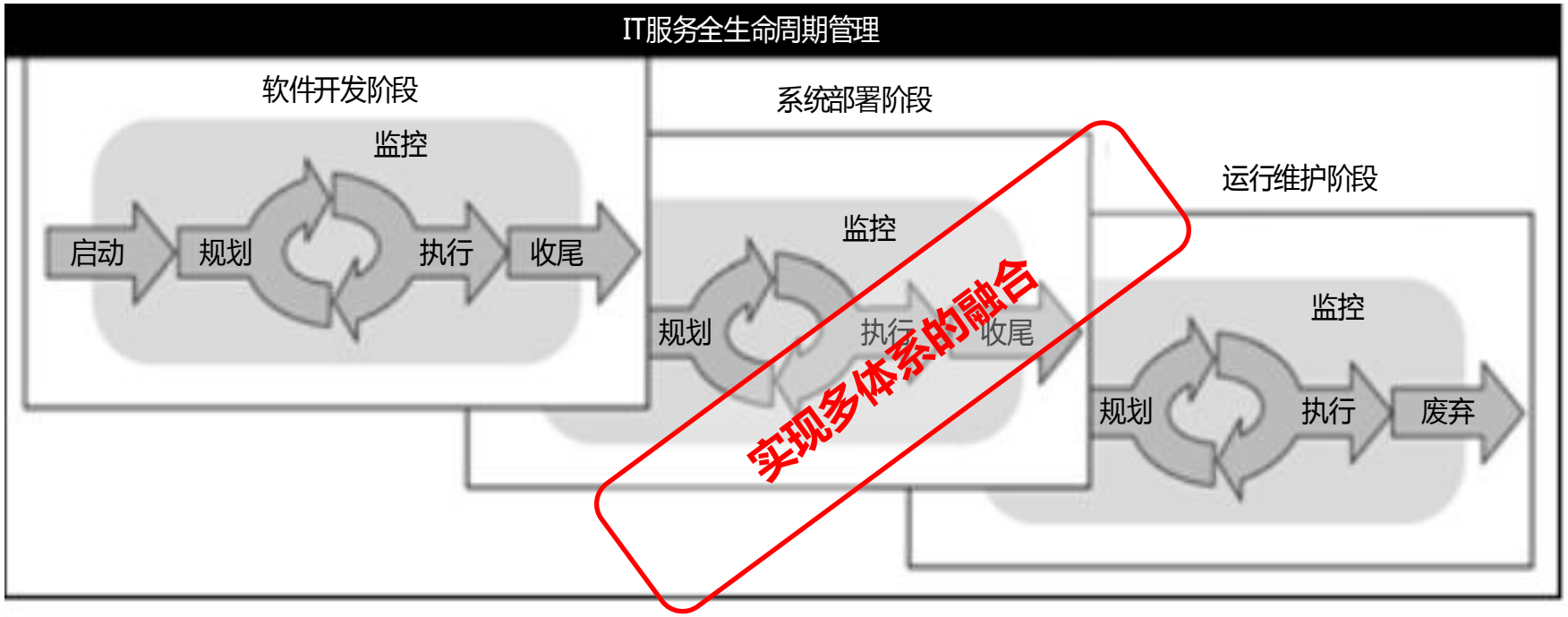
● 优点

- 符合日常管理的习惯和思维，日常管理习惯于按照技术职能（对应相应的产品和设备）来进行管理的
- 有利于与工作岗位的匹配，使得在管理措施落地时，能够和工作岗位和职责相融合
- 有利于不同管理标准以及技术标准（如等级保护/科技风险管理指引/数据中心风险管理等）相关标准的融合
- 符合以资产核心的信息安全风险管理理念
- 有利于与安全技术产品的融合，目前多数安全产品都是基于纵深防御的理念推出的，多是针对特定管理对象的
- 有利于管理在一定时间段内的稳定，不会应为标准要求发生变化（或岗位调整），而需要大规模调整

● 缺点

- 对规划设计人员要求高，设计规划工作量大

4、如何实现多标准的融合？



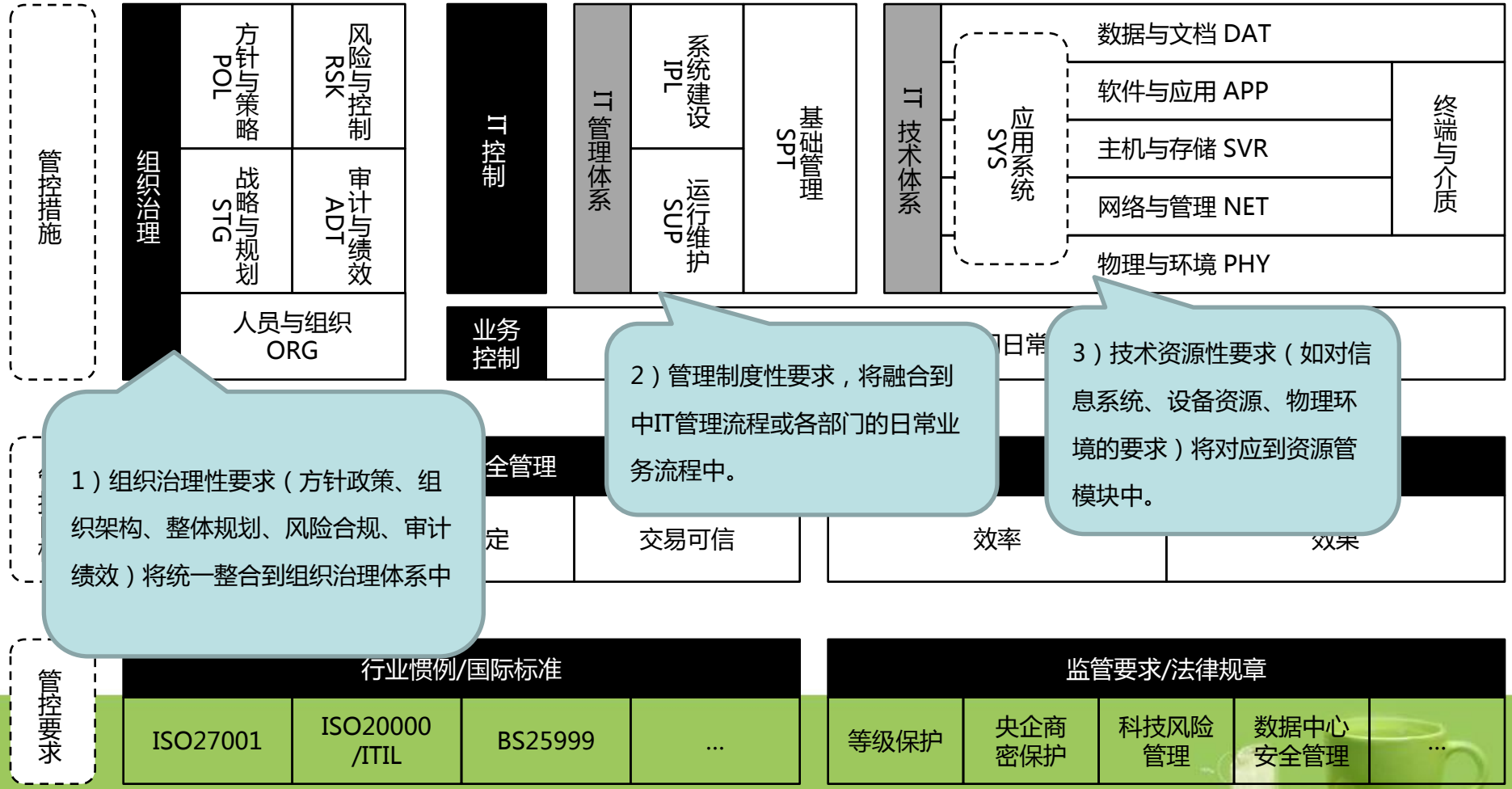
CMMi（软件开发）的范畴

ISO 20000（IT运维服务）的范畴

ISO 9001（质量管理的领域）

ISO 27001（信息安全管理）的范畴

5. 如何实现与等级保护多个监管要求的融合
（安全管理的整合框架（ROC）：整合管控目标、管控措施、管理要求）



实施信息安全管理体系的大概流程？

1. 项目的整体流程

转变管理（持续沟通 + 培训）

评估规划	体系建立	体系运行	项目结项
1) 启动准备 2) 理念导入 3) 调研评估 4) 体系规划	1) 建立组织治理体系 2) 建立管理制度体系 3) 建立技术措施体系	1) 实施规划 2) 实施指导 3) 优化改进	1) 内部审核 2) 管理评审 3) 外部审核 4) 项目结项

项目管理

2. 评估规划 - 项目启动

项目启动阶段：主要目的

确定业务需求及初步的职责分配，完成项目前期的普及性宣讲和信息安全管理理念导入，做好知识准备，完成统一认识，使项目组人员到位并进入项目角色。

好的开始，是成功的一半

2. 评估规划 - 项目启动

项目启动阶段：工作内容

基本调研

为后续的包括风险评估等相关工作能够有序和有效的进行，需要对当前的基本信息和管理现状进行基本的了解。

成立项目组

为确保体系更好的符合业务运转的要求以及与日常工作的结合（同时也标准实施的基本要求），按照标准要求需要成立：**信息安全领导小组**（信息安全管理委员会）和**信息安全工作小组**。领导小组由公司管理层与各相关部门领导构成，信息安全工作小组由各部门派出代表构成。

理念导入培训

为了对以后阶段工作提供便利和好的基础，提高公司领导层和员工的信息安全意识，以便在项目实施过程中能够得到大家的积极配合和有效支持，在本阶段分别对领导层和员工进行相关安全理念的培训。

信息安全理念培训： 主要针对管理层与项目其他干系人

信息安全管理标准（ISO27001)培训：主要针对信息安全管理体系实施项目组的成员

明晰项目计划

根据基本调研的结果，明晰项目工作计划

项目启动

为确保项目在后续能够得到各相关部门的支持，在项目启动阶段得到领导层的支持非常重要。

2. 评估规划 - 项目启动

项目启动阶段：关注事项

信息安全工作小组成员的理想人选：

- 在部门内部具有一定的资历和威望
- 善于激励别人
- 执行能力强和追求结果
- 希望对现状进行改进（对现状感到不满意或持有怀疑的态度）

最担心的问题：

- 谁有空， 交给谁
- 对本部门的工作不太熟悉
- 在其部门内无法推动工作的开展

2. 评估规划 - 项目启动

项目启动阶段：主要成果

1. 《项目领导小组与工作小组成员》
2. 《信息安全基本理念培训》
3. 《信息安全管理体系标准讲解》
4. 《项目实施工作计划》

2. 评估规划 - 调研评估

调研评估阶段：主要目的

现状调研与风险评估阶段的主要目标：

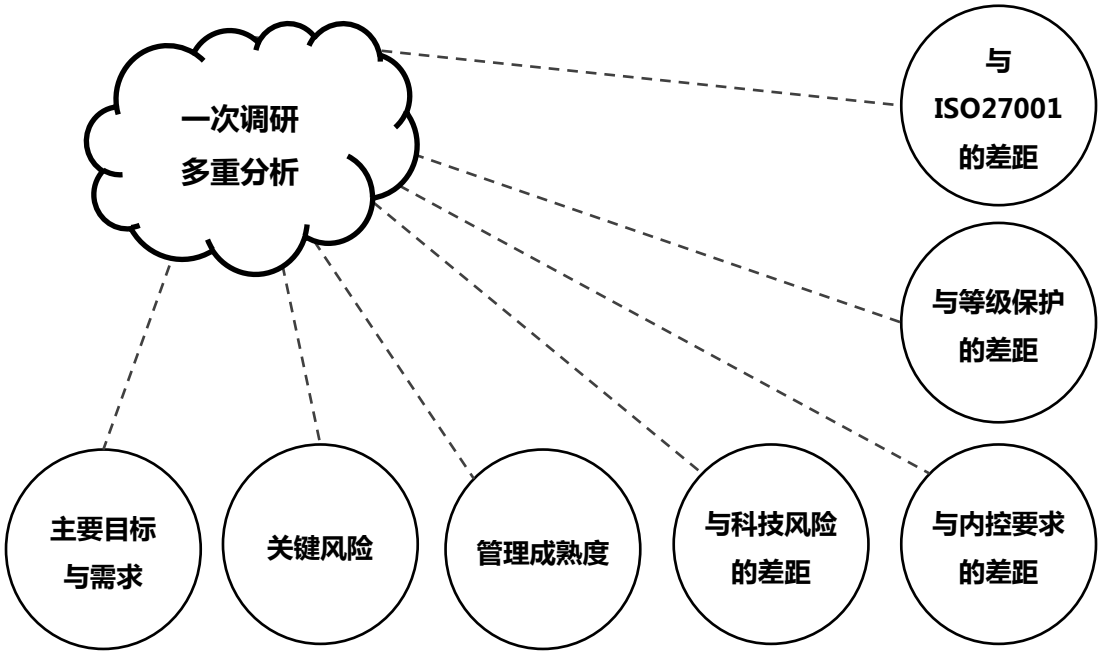
1. 了解现状
2. 明晰需求
3. 分析差距
4. 确认风险

1. 现状是什么？可能发生什么（事件）？为什么发生？
2. 产生的后果是什么？对目标的影响有多大？
3. 这些后果发生的可能性有多大？
4. 是否存在可以减轻风险后果、降低风险可能性的因素？
5. 风险等级是否是可容忍或可接受的？是否需要进一步应对？

现状调研与风险评估阶段需解决的五个问题：

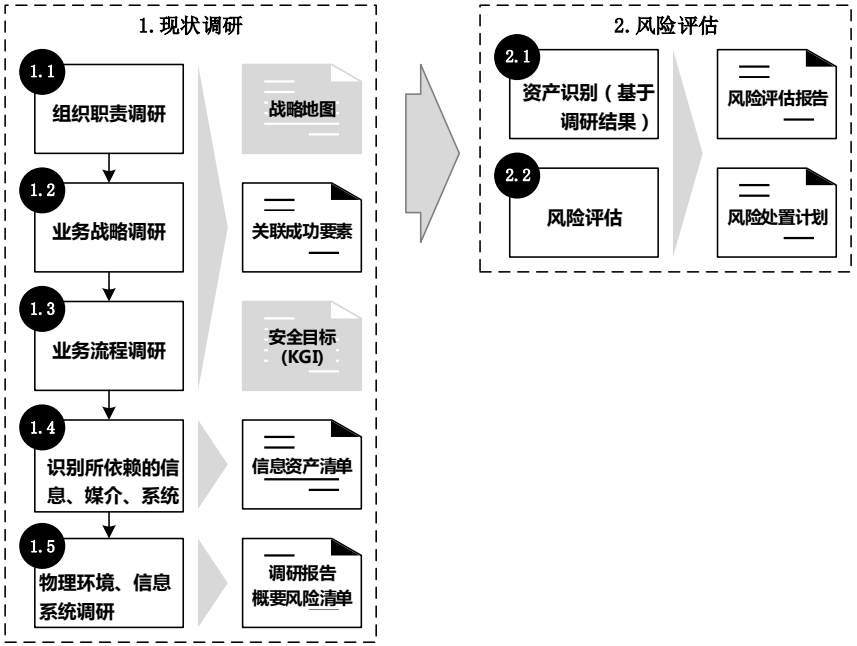
2. 评估规划 - 调研评估

调研评估阶段：工作思路



2. 评估规划 - 调研评估

调研评估阶段：工作内容



安全现状的调研主要包括对系统、网络的配置、操作、管理等内容，采用问卷调研、技术工具评估及现场访谈等方式，其中问卷调研、技术工具评估可以在项目涉及范围内广泛展开，现场访谈选择一些有代表性的单位进行，可能包括：

✓ 组织架构及职责的调研/业务战略调研/业务流程调研

✓ 物理环境调研/网络安全系统调研/系统主机调研/系统数据调研/业务应用调研/初步风险识别

风险评估是依据国际最新风险评估标准ISO27005作为基础方法论，同时结合ISO13335，国标《信息安全风险评估指引》等标准和规范，结合客户当前的自身特点，设计风险评估模型并对信息资产面临的信息安全风险进行评估，主要内容包括：

✓ 风险评估模型的确定/风险分析风险计算风险的处置

2. 评估规划 - 风险评估

调研评估阶段：工作方法

基于资产分类的头脑风暴法

优点：

- 易于客户理解，实施简单，耗时少

缺点

- 资产识别可能不全
- 资产之间的关联关系不能体现
- 不宜关注信息全生命周期的风险
- 流程性风险不被关注

基于业务流程的过程识别法

优点：

- 重要资产不宜遗漏、能够识别客户整个业务流中和整个信息生命周期的信息安全风险

缺点

- 客户理解困难，对客户当前管理水平要求较高， 实施困难，耗时长（特别是当客户各部门没有文档化的流程时）。

2. 评估规划 - 调研评估

调研评估阶段：主要成果

《现状调研报告》

1. 各部门的主要业务与信息资产
2. 各部门的信息安全管理现状
3. 各部门的主要信息安全风险

《差距分析报告》

1. 信息安全管理现状与信息安全管理体系的差距分析
2. 信息安全管理现状与科技风险管理指引的差距分析
3. 信息安全管理现状与等级保护要求的差距分析

《风险评估报告》

1. 信息及信息资产所面临的风险
2. 与风险相对应的控制措施与处置计划

2. 评估规划 - 调研评估

调研评估阶段：成果参考

- 技术调研报告
- 报告0：信息安全管理现状调研总报告-v1.0
- 报告1：ISO27001差距分析报告-V1.0
- 报告2：等级保护差距分析报告-v1.0
- 报告3：商业秘密保护现状调研报告-V1.1
- 报告4：电力二次系统防护现状调研报告-v1.2
- 报告5：IT服务管理现状调研报告-v1.0
- 江苏核电-ISO27001差距分析问卷-v1.0
- 江苏核电-等级保护差距分析调查问卷-v.0
- 江苏核电-信息安全管理现状调研总报告-v1.0
- 总目录

- 【ISMS】信息资产风险管理表@20120224
- 【ISMS】【风险评估-4】信息系统资产清单@20120301
- 【ISMS】【风险评估-3】信息系统类资产@20120229
- 【ISMS】【风险评估-2】非系统类资产@20120301
- 【ISMS】【风险评估-1】业务与信息@20120301
- 【ISMS】【风险管理】流程说明 - V1.1@20120302
- 【ISMS】【风险管理】风险评估报告- V1.1@20120302

2. 评估规划 - 体系规划

体系规划阶段：主要工作

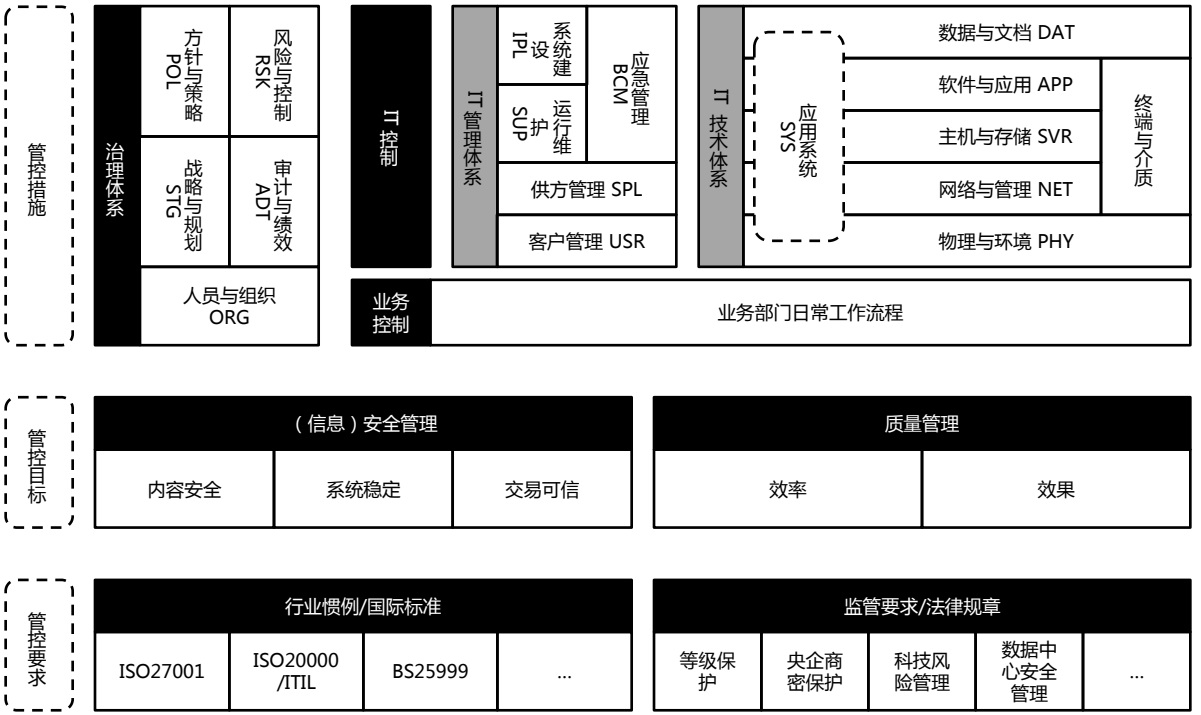
根据调研及风险评估的结果，依据行业最佳实践，从管理和技术层面，系统设计和构建未来3年的信息安全规划，提出实施路线图、预算和投资计划。

2. 评估规划 - 体系规划

体系规划阶段：主要思路

体系规划阶段的主要思路：

- ✓ 融合多方要求
- ✓ 融合多种体系
- ✓ 融合日常工作



2. 评估规划 - 体系规划

体系规划阶段：主要成果

梳理当前信息安全管理的总体需求，提出1 - 3年信息安全管理的总体架构策略性建议，提出信息安全管理总体架构策略性实施路线图：

1. 《信息安全管理规划整体建议》
2. 《信息安全治理体系整体框架》
3. 《信息安全管理体系整体框架》
4. 《信息安全技术体系整体框架》
5. 《信息安全技术建议实施方案》

2. 评估规划 - 体系规划

体系规划阶段：成果参考

3. 体系建立

体系建立阶段：主要工作

制定管理制度：

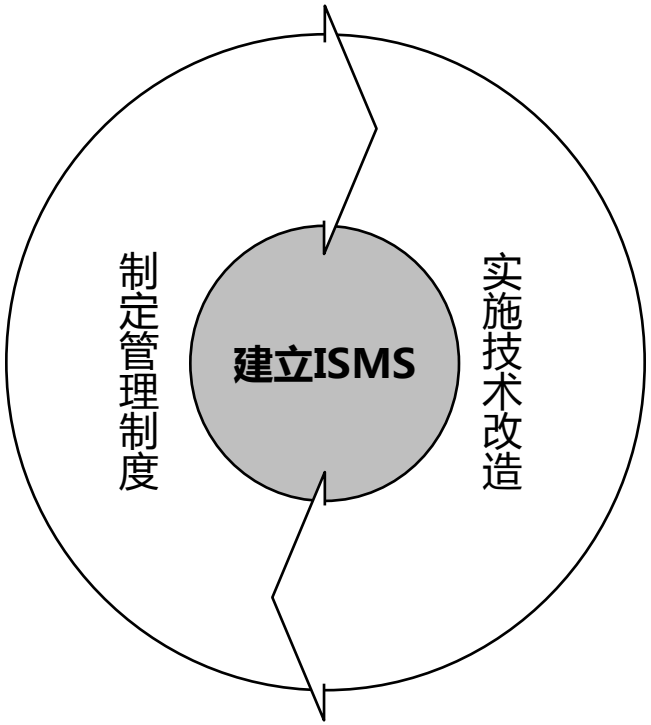
通过TMG模型， 融合多标准/规范以及当前管理措施的要求，

覆盖27001及等级保护的相关管控要求

实施技术改造：

提供风险指处置计划的执行的指导、监督和检查，协助技术措施

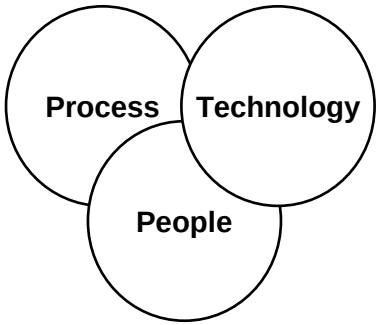
的实现



3. 体系建立

体系建立阶段：工作思路

在风险处置过程中所输出的众多信息安全管控措施可能是相互独立的，缺乏统一规划，并且缺少各项控制措施之间的相互作用。
信息安全管理体系拥有为数众多的文档化的方针、策略、规范、制度，并在体系运行的过程中将产生大量的记录，如何对这些文件进行分门别类的管理，并且很好的对其中的逻辑性与一致性进行控制，这对于体系设计和维护人员来讲是一个不大不小的难题。



管理架构 / 管理对象	责任人 PEOPLE	管理制度 (POLIY)	管理规程 (PROCESS)	技术产品/措施 (PRODUCTS/Techonology)	安全测量 (PROOF/Metrics)

3. 体系建立

体系建立阶段：工作思路

基于推进实施考虑的流程表单化设计

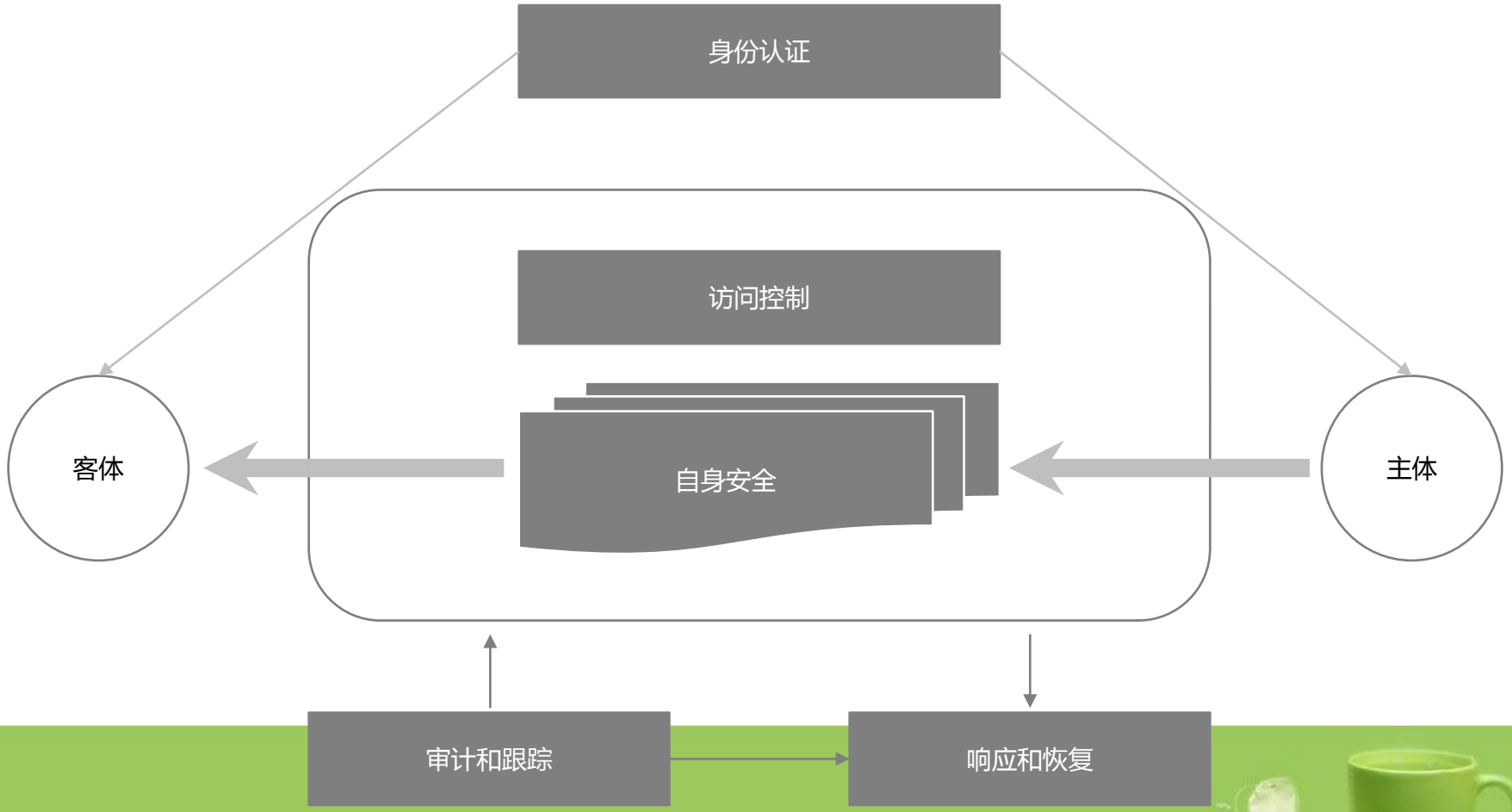
系统变更申请表	版本号	V2.2
	发布日期	2010/11/30

2. 变更风险评估

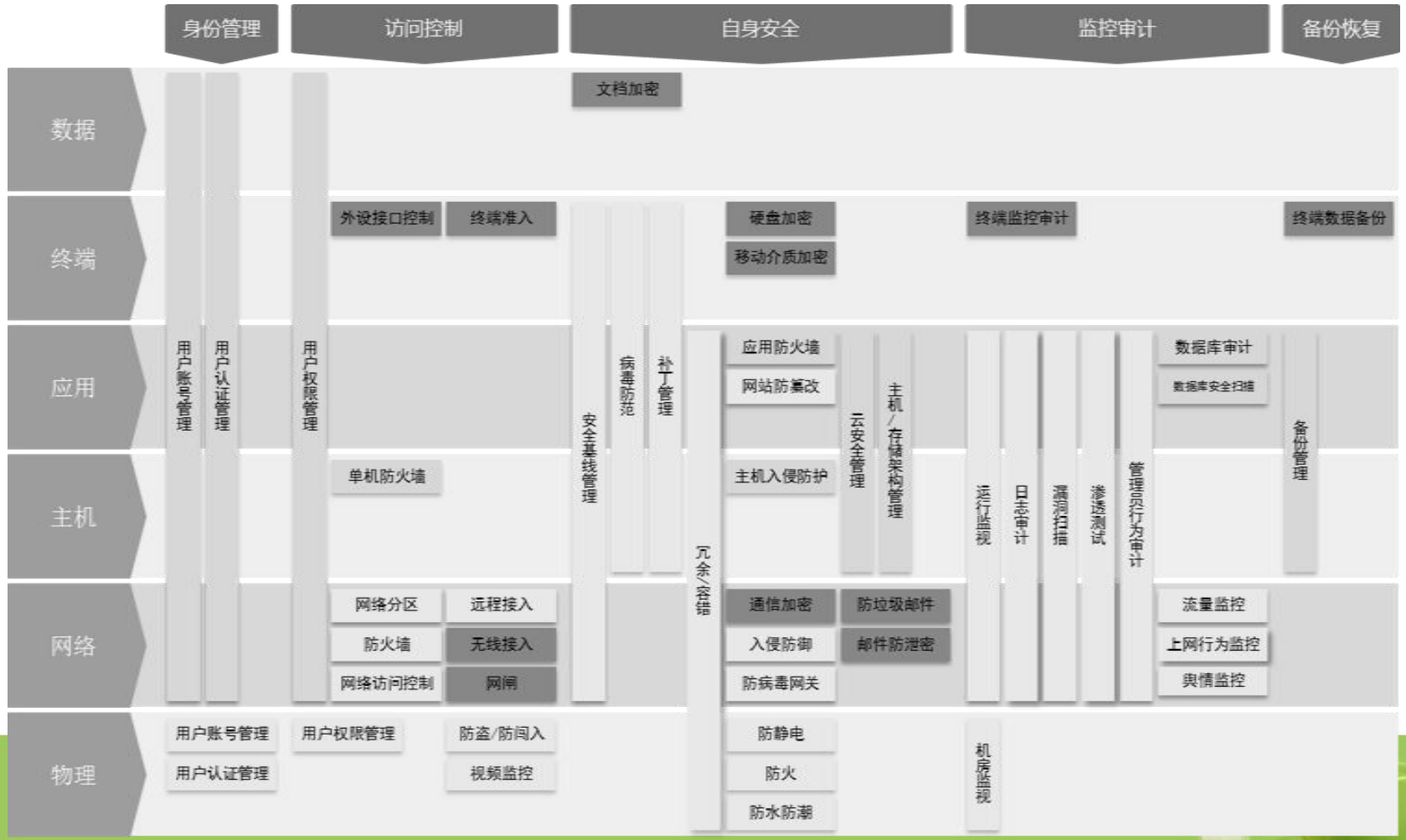
2.1 风险水平计算：

评估因素	状态	分数	选择
变更实施或回退影响的用户总数	>150	5	
	50-150	4	
	10-49	3	
	<10	2	
	N/A（例如:没有服务影响)	1	
准备或实施变更所需要的资源 例如:变更包括了生产支持团队和数据库支持团队,因而将被计为2分	5 个或者更多支持团队	5	
	4 个支持团队	4	
	3 个支持团队	3	
	2 个支持团队	2	

3. 体系建立

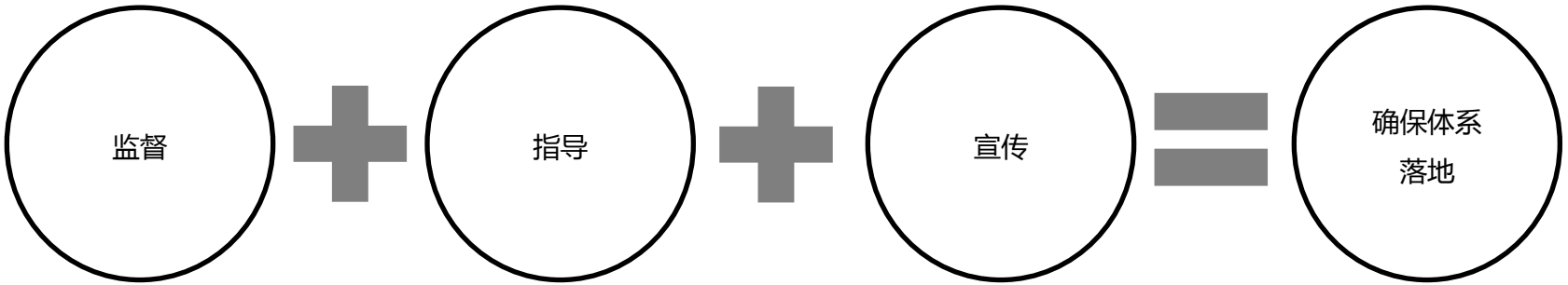


3. 体系建立


身份管理
访问控制
自身安全
监控审计
备份恢复
数据
终端
应用
主机
网络
物理
文档加密
外设接口控制
终端准入
硬盘加密
移动介质加密
终端监控审计
终端数据备份
用户账号管理
用户认证管理
用户权限管理
单机防火墙
安全基线管理
病毒防范
补丁管理
冗余/容错
应用防火墙
网站防篡改
主机入侵防护
云安全管理
主机/存储架构管理
运行监视
日志审计
漏洞扫描
渗透测试
管理员行为审计
数据库审计
数据库安全扫描
备份管理
网络分区
远程接入
防火墙
无线接入
网络访问控制
网闸
通信加密
防垃圾邮件
入侵防御
邮件防泄密
防病毒网关
流量监控
上网行为监控
舆情监控
用户账号管理
用户认证管理
用户权限管理
防盗/防闯入
视频监控
防静电
防火
防水防潮
机房监视

4. 体系运行

体系运行阶段：工作内容



4. 体系运行

监控管理	张三	使用性能监控系统进行实时监控	技术部每天应对服务器的性能进行监控，监控的范围包括：带宽使用情况、CPU、内存使用情况、服务器硬盘容量。
		使用日志监控系统	技术部系统管理员每月应对重要服务器进行日志监控，重点检查错误记录及告警记录，并对发现的情况进行跟踪调查。
数据备份管理	李四	《备份策略明细表》	技术部根[illegible]提出的备份需求及各部门业务的实际情况，制定《备份策略明细[illegible]的数据、备份的方式及周期。
		《备[illegible]	[illegible]统后对备份情况进行检查，并将备份的检查结果记[illegible]备份未成功或异常时应立即排除故障并在适当
		[illegible]	[illegible]数据所属部门依据备份策略规定的恢复测试频率，对备份数据进行[illegible]，并填写《备份数据恢复测试记录表》
变更管[illegible]		[illegible]计划表 变更验收报告	技术部依据公司实际情况制定《变更分类策略明细表》，明确公司的变更事项的分类，变更类别分日常、一般和重大三种类别。当涉及重大变更时启动公司变更流程，对日常和一般两个级别的变更只要求保留变更记录即可。详见《信息系统变更管理程序》。
	王五	《开发、测试环境管理规定》	[illegible]适用于公司及所有分公司业务中的开发、测试环境、人员以及职责，每项业务的使用者都应该遵守该规章制度。 1）开发、测试人员通过OA系统提交申请。 2） 技术部接到申请后，建立测试环境，并将相应权限交给开发、测试人员，结束申请流程。

总实施策略 | 每天 | 每周 | 每月 | 每季度 | 每半年 | 每年 | 触发

规章制度的**岗位化**：每个岗位每天需要进行的工作？遵循哪些要求？

3.2 各流程入口说明

序号	业务场景	接口流程
1	监控告警（监控室通过监控发现的系统故障）	事件流程
2	业务申告（业务部门无法解决的系统故障）	事件流程
3	OA 系统转单的故障（办公应用及设备部分或全部功能不能正常使用的报障）	事件流程
4	运维人员发现的系统故障	[illegible]程
5	与业务支撑系统相关的[illegible]	
6	办公[illegible]	[illegible]件流程
	[illegible]	事件流程
	[illegible]	事件流程
	[illegible]	事件流程
	[illegible]询统计	事件流程
1[illegible]	系统处理逻辑咨询	事件流程
12	业务开通配合	事件流程
13	前台账务操作配合	事件流程

规章制度的**场景化**：在发生这种情形时，应该遵循哪些要求？

4. 体系运行

体系运行阶段：工作思路

管理与技术相结合

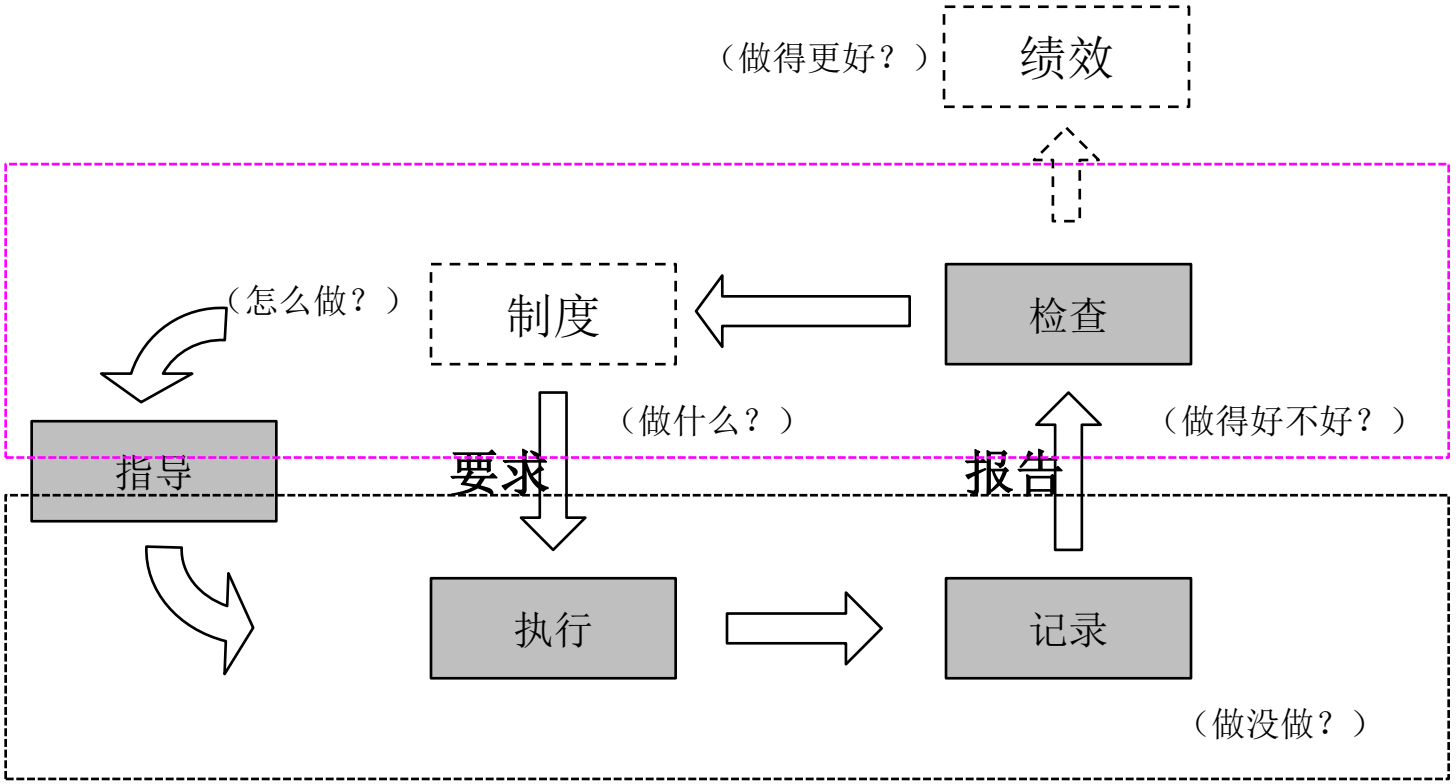
提高人员意识，实现

易拉宝、海报

视频短片

- 电影剪辑
- FLASH动画
- 信息安全管理内刊
- 信息安全标准集锦
- 信息安全管理知识库
- 信息安全管理白皮书
- 流程小手册
- 台历、鼠标垫、小贴士
- 展板、海报、易拉宝
- 屏保、电脑背景
- 会议条幅等

4. 体系运行



5. 认证结项

认证结项：主要工作

内部审核：

内部审核，是为了检查与确认体系各要素的实施效果是否按照计划有效实现，它是对体系运行是否达到了规定的目标所作的系统的、独立的检查和评价。

管理评审：

管理评审，是组织最高管理者亲自对体系的现状是否有效地适应方针要求，以及体系变化后确定的新目标是否合适等所作的综合评价。它是在体系审核的基础上进行的。

外部审核：

外部认证机构按照标准要求所进行的发证审核

6. 实施信息安全管理体系大概需要多长时间？

序号	起止时间	阶段目标
1	**评估规划** **（1-2个月）**	本阶段的主要工作将包括项目启动、理念导入、现状评估、差距分析、风险评估、体系规划等相关工作。 主要目的出通过现状评估、差距分析以及风险评估，识别当前存在的风险，以及考[illegible]公司当前的建设现状和未来业务发展的需要，对安全管理体系的建[illegible]技术和保障的相互结合进行规划。
2	**体系建立** **（3-5个月）**	以风险[illegible]基础，按照信息安全管理体系标准ISO27001 、[illegible]企业/组织的管理现状与业务需求，建立一套文件化的管[illegible]方针、策略、程序文件，操作手册等。
3	**体[illegible]** **（3个[illegible]**	[illegible]已建立的体系为基础，在实际工作中进行推行，配合响应的宣传和指导，确保体系的落地以及通过体系的试运行发现体系设计层面和体系层面的问题。通过对所发现问题的分析与处理，使得体系得到有效的落实。
4	**认证结项** **（1个月）**	在体系通过运行得到验证及优化后就，提请相关外部认证机构进行评估和认证。

根据工作实际推进的配合程度，进度可能有所调整，一般建议为8-10个月