国佳基业
GORGEOUS

信息安全管理体系培训

ISO/IEC27001

内容介绍

一，信息安全管理体系简介

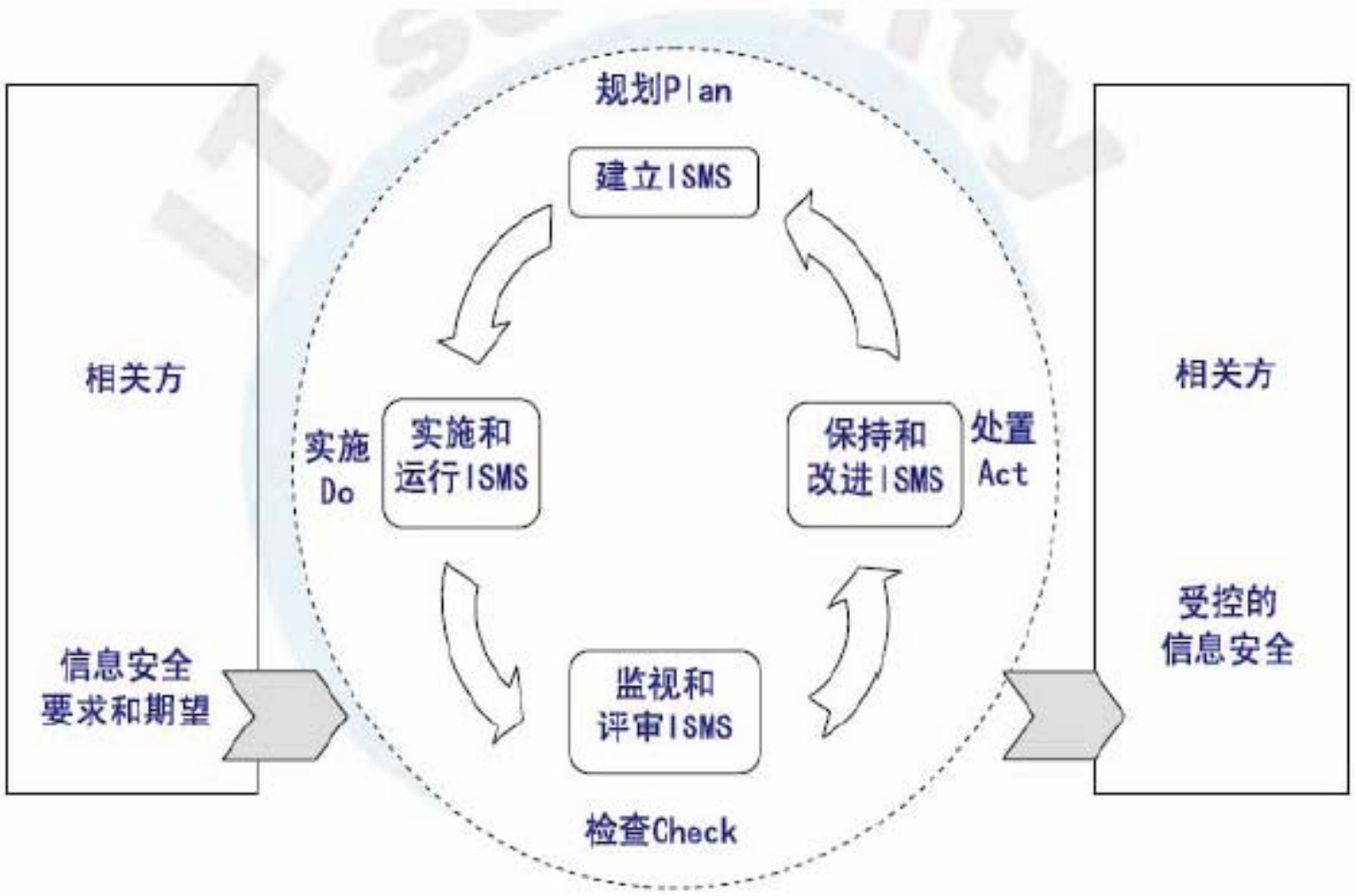
二，信息安全管理体系详解

一，信息安全管理体系简介

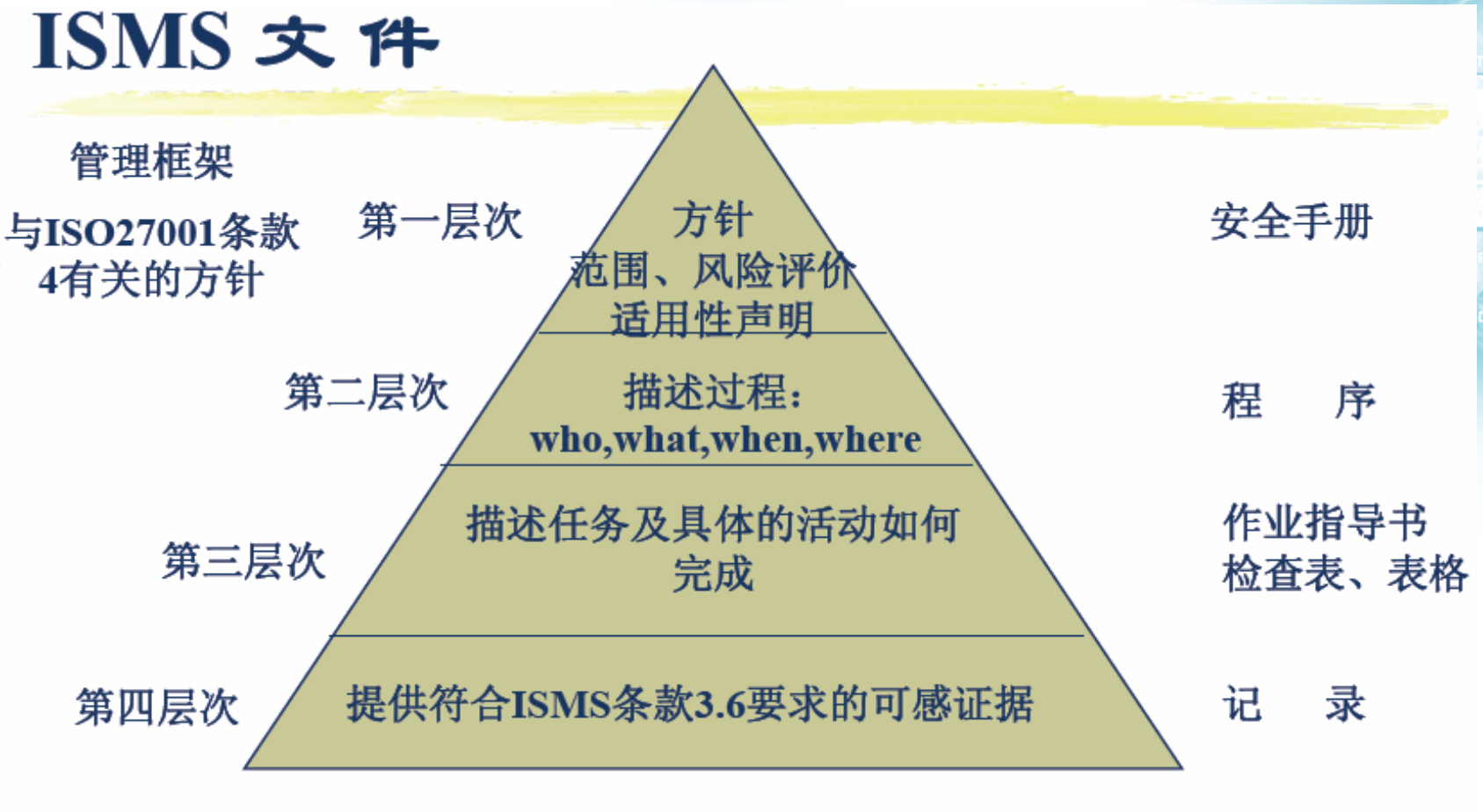
ISO/IEC27001管理体系的发展历史

ISO/IEC是由英国标准BS7799转换而来的。BS7799在1993年由英国贸易工业部立项，于1995年英国首次出版BS7799—1:1995《信息安全管理实施细则》。2000年12月，BS7799—1:1999《信息安全管理实施细则》通过国际标准化组织ISO认证，正式成为ISO/IEC7799—1：2000《信息技术—信息安全管理实施细则》，后来升版为ISO/IEC17799：2005。2002年9月5日，BS7799—2：2002发布。2005年BS7799—2：2002正式转版为ISO/IEC27001：2005.

ISO/IEC27001 信息安全管理模式

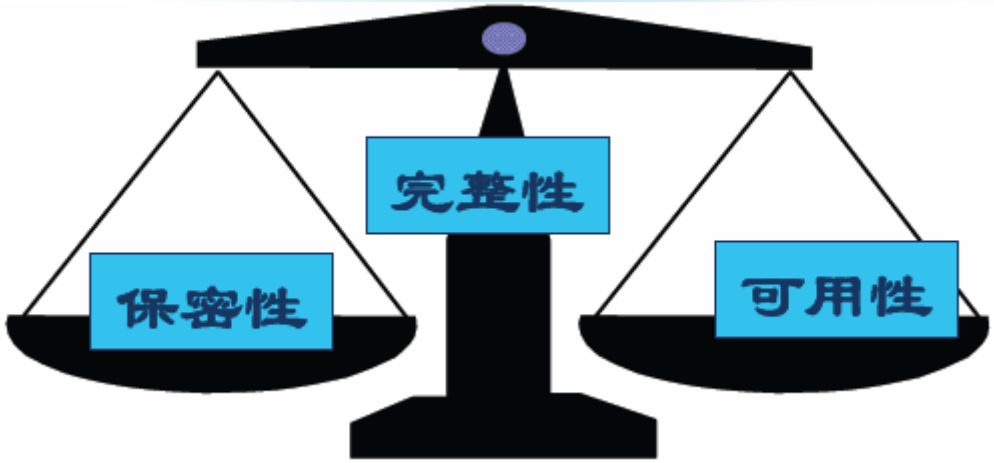


ISO/IEC27001管理层次



ISO/IEC 27001中信息安全的定义:

保持信息的保密性、完整性、可用性；另外，也包括其他属性，如：真实性（身份识别）、可核查性（日志）、不可否认性（数字签名）和可靠性（MTBF）。



ISO/IEC 27001中信息安全三元组CIA:

☆保密性Confidentiality:

信息不能被未授权的个人、实体或者过程利用或知悉的特性。例如，重要配方的保密。

☆完整性Integrity

保护资产的准确和完整的特性。例如，财务信息的完整性。

☆可用性Availability:

根据授权实体的要求可访问和利用的特性。例如，供应商资料库的及时更新。

二，信息安全管理体系详解

ISO 27001的内容

- 前言
- 0 引言
- 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(ISMS)**
- **5 管理职责**
- **6 ISMS内部审核**
- **7 ISMS的管理评审**
- **8 ISMS改进**
- 附录A (规范性附录)控制目标和控制措施
- 附录B (资料性附录)OECD原则和本标准
- 附录C (资料性附录)9001、14001和本标准之间的对照

引言

0.1 总则

描述了标准的用途及应用对象

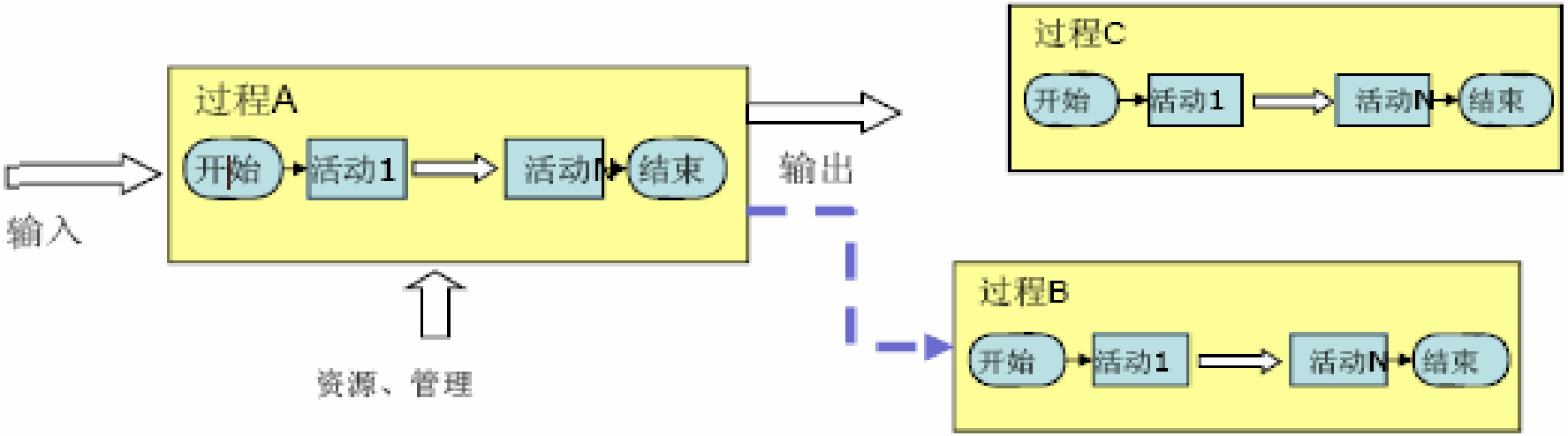
- 提供一个模型，用于建立、实施、运行、监视、评审、保持和改进信息安全管理体系(ISMS)
- 适用对象：一个组织
- 可被组织内部或外部相关方用来进行一致评估
- 组织ISMS的设计和实践受影响的因素：
  - 业务需要和目标
  - 安全要求
  - 所采用的过程
  - 规模和结构

引言

0.2 过程方法

描述了过程、过程方法、及贯穿于本标准的**PDCA模型**

- 过程：通过使用资源和管理，将输入转化为输出的活动
- 过程方法：组织内诸过程的系统的应用，连同这些过程的识别和相互作用及其管理。



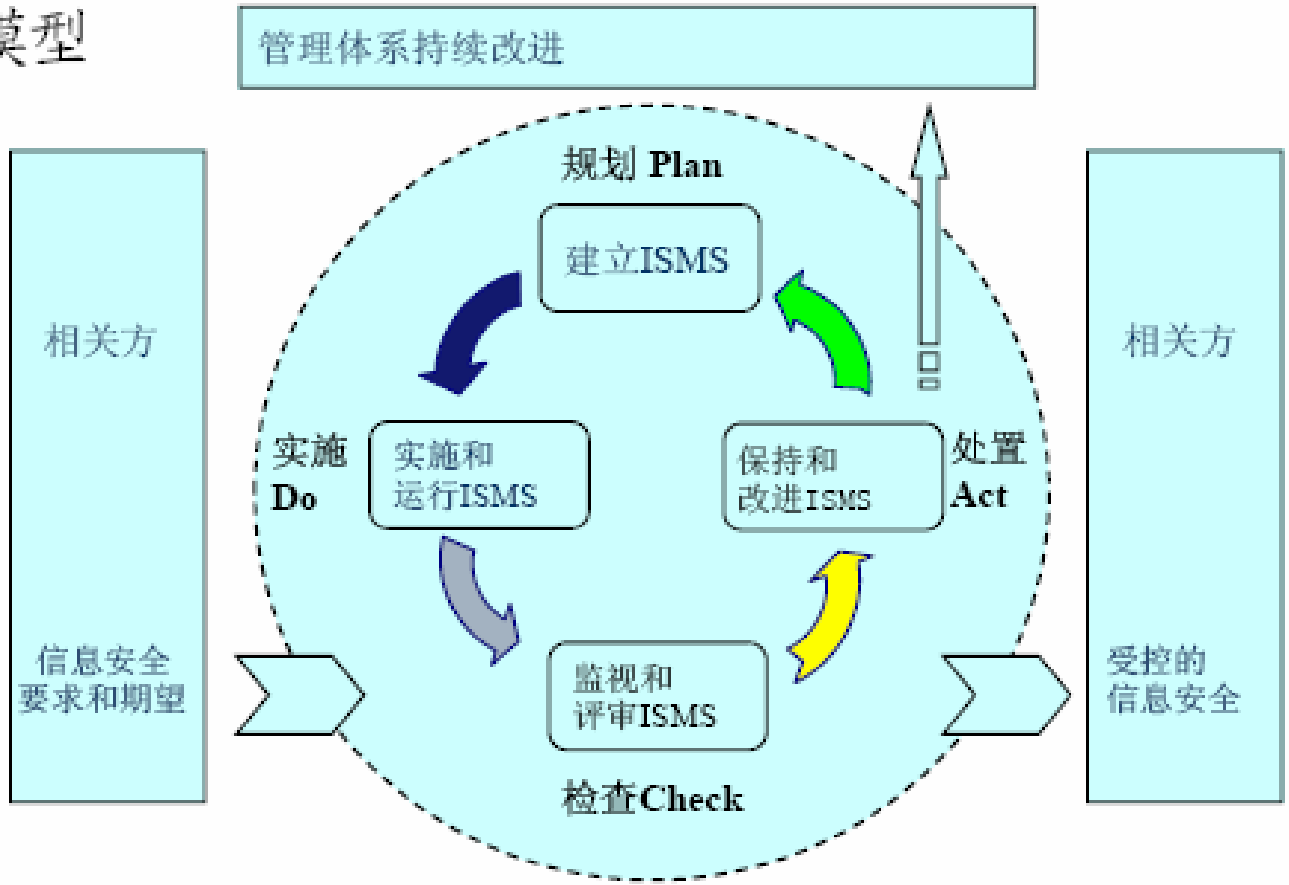
引言

了解过程方法：

- 适用性
  - 组织中需要重复执行的系列活动，并贯穿多个角色
  - 通过过程的组织，可更有效地实现预期的结果或目的
  - 保证活动的实施和结果的一致性
  - 通过对过程的改进，可实现更佳的效果
- 在信息安全管理中的使用场景
  - 信息安全风险管理
  - 信息安全事件管理

引言

PDCA模型


管理体系持续改进
相关方
信息安全
要求和期望
规划 Plan
建立ISMS
实施
Do
实施和
运行ISMS
保持和
改进ISMS
处置
Act
监视和
评审ISMS
检查Check
相关方
受控的
信息安全

PDCA说明

PDCA各阶段	内　容	对应标准条款
P-规划 建立ISMS	建立与管理风险和改进信息安全有关的ISMS方针、目标、过程和规程，以提供与组织总方针和总目标相一致的结果。	4.1；4.2.1； 4.3；5
D-实施 实施和运行 ISMS	实施和运行ISMS方针、控制措施、过程和规程。	4.2.2
C-检查 监视和评审 ISMS	对照ISMS方针、目标和实践经验，评估并在适当时测量过程的执行情况，并将结果报告管理者以供评审。	4.2.3； 6；7
A-处置 保持和改进 ISMS	基于ISMS内部审核和管理评审的结果或者其他相关信息，采取纠正和预防措施，以持续改进ISMS。	4.2.4；8

引言

0.3 与其它管理体系标准的兼容性

说明ISMS与其它管理体系的兼容性问题

- 与ISO 9001、14001等管理体系标准一致
- ISMS可与其它相关的管理体系整合并运行

–如,ISO 20000 IT服务管理体系

1 规范

1.1 总则

●本标准适用于所有类型的组织（例如，商业企业、政府机构、非赢利组织）。

●本标准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。

●规定了为适应不同组织或其部门的需要而定制的安全控制措施的实施要求。

●是ISMS的设计应确保选择适当和相宜的安全控制措施，以充分保护信息资产并给予相关方信心。

1 范围

1.2 应用

- 本标准规定的要求是通用的，适用于各种类型、规模和特性的组织。
- 对本标准内容删减的规定
  - 组织声称符合本标准时，对于4、5、6、7和8章的要求不能删减；
  - 对附录A中所提供的控制措施的任何删减都必须被证明是合理的；
  - 需要提供证据证明相关风险已被负责人员接受；
  - 删减不影响组织满足由风险评估和适用法律法规要求所确定的安全要求的能力和/或责任。
- 控制措施删减的原因
  - 组织的业务需求和目标不同；
  - 所采用的过程以及规模和

2 规范性引用文件

ISO/IEC 27002:2005

信息安全管理实用规则

4 信息安全管理体系(ISMS)

4.1 总要求

4.2 建立和管理ISMS

4.2.1建立ISMS

4.2.2 实施和运行ISMS

4.2.3 监视和评审ISMS

4.2.4 保持和改进ISMS

4.3 文件要求

4.3.1 总则

4.3.2 文件控制

4.3.3 记录控制

4.1 总要求

组织应在其整体业务活动和所面临风险的环境下建立、实施、运行、监视、评审、保持和改进文件化的**ISMS**。

标准所使用的过程基于**PDCA**模型。

管理体系

- 信息安全管理体系（ISMS）

  基于业务风险方法，建立、实施、运行、监视、评审、保持和改进信息安全的体系，是一个组织整个管理体系的一部分。

  注：管理体系包括组织结构、方针策略、规划活动、职责、实践、规程、过程和资源。[ISO/IEC 27001:2005]

- 管理体系

  为实现组织目标而确立的方针、规程、指南和相关资源的框架。[ISO/IEC 27000:2009]

- 质量管理体系

  在质量方面指导和控制组织的管理体系。[ISO 9000:2005]

4.2 建立和管理ISMS

4.2.1 建立ISMS

组织要做以下方面的工作：

a)确定ISMS的范围和边界；
b)确定ISMS方针；
c)确定组织的风险评估方法
d)识别风险
e)分析和评价风险
f)识别和评价风险处置的可选措施
g)为处理风险选择控制目标和控制措施
h)获得管理者对建议的残余风险的批准
i)获得管理者对实施和运行ISMS的授权
j)准备适用性声明（SoA）

其中d—i属于风险管理阶段

4.2.1建ISMS

a)确定ISMS的范围和边界

- 根据业务、组织、位置、资产和技术等 方面的特性，确定ISMS的 范围和边界，包括对范围任何删减的详细说明和正当性理由。

ISMS的范围说明

ISMS的范围通常包括

- 覆盖的组织机构、职能(部门)和涉及的人员
- 需要保护的信息资产和系统(ICT基础架构)
- 物理位置及分支机构
- 使用的流程和服务

确定ISMS的范围还应考虑

- 与相关方（范围外）的接口和依赖关系

范围说明示例

某国际银行实施信息安全管理，先期所确定的范围为：因特网银行服务

具体识别为：

- ■提供网上银行服务的人员
- ■人员使用的流程
  - ●系统操作手册
  - ●安全手册
  - ●网银规程
- ■使用的信息
  - ●顾客的详细信息
  - ●内部的银行数据
  - ●来自其它银行的外部数据

- 用以提供在线交易的网络服务
  - □顾客接入
  - □与其它银行的连接和接口（内部和外部）
- 便利在线服务的技术
  - □桌面计算机和其它ICT设备
  - □电话

4.2.1建立ISMS

b)确定ISMS方针

根据业务、组织、位置、资产和技术等方面的特性，确定ISMS方针。

ISMS方针应：

1）包括设定目标的框架和建立信息安全工作的总方向和原则；

2）考虑业务和法律法规的要求，及合同中的安全义务；

3）在组织的战略性风险管理环境下，建立和保持ISMS；

4）建立风险评价的准则（见4.2.1c）；

5）获得管理者批准。

信息安全风险管理

标准引用的有关风险管理的术语和定义

- 风险管理(risk management)
  指导和控制一个组织相关风险的协调活动。
- 风险评估(risk assessment)
  风险分析和风险评价的整个过程。
- 风险分析(risk analysis)
  系统地使用信息来识别风险来源和估计风险。
- 风险评价(risk evaluation)
  将估计的风险与给定的风险准则加以比较以确定风险严重性的过程。

风险管理的术语和定义

●风险处置(risk treatment)

选择并且执行措施来更改风险的过程。

●风险接受(risk acceptance)

接受风险的决定。

●残余风险(residual risk)

经过风险处置后遗留的风险。

注：以上术语的定义均来自[ISO/IEC Guide 73:2002] 为ISO/IEC 27001所引用。

●识别风险(risk identification)

发现、列出并描述风险要素的过程活动。

[ISO/IEC Guide 73:2002]

4.2.1建立ISMS

c)确定组织的风险评估方法

1）识别适合ISMS、已识别的业务信息安全和法律法规要求的风险评估方法。

2）制定接受风险的准则，识别可接受的风险级别。选择的风险评估方法应确保风险评估产生可比较的和可再现的结果。

注：风险评估具有不同的方法。在ISO/IEC TR 13335-3中描述了风险评估方法的例子。

风险评估方法

ISO/IEC TR 13335-3给出的风险评估方法：

- ■基准法(Baseline Approach)
  - ●组织通过选择标准的防护为系统各部分的安全保护设立统一的基准
- ■详细的风险分析(Detailed Risk Analysis)
  - ●包括资产的深度鉴定和估价，对这些资产的威胁评估和脆弱性评估。结果用于评估风险及选择合理的安全控制措施。
- ■非正式的方法(Informal Approach)
  - ●依据个人知识和经验的简化风险分析
- ■综合的方法(Combined Approach)
  - ●先对系统进行宏观风险分析，确定出高风险或重要的业务领域，再按优先顺序分别进行详细的风险分析。

接受风险

- 接受风险的准则
  - 判别风险造成的损失或后果为可容忍程度或量级的尺度
  - 描述了组织愿意接受风险的情形
  - 可以针对某类风险而具体规定，或制定为通用的判定依据

4.2.1 建立ISMS

d) 识别风险

1）识别ISMS范围内的资产及其责任人；

2）识别资产所面临的威胁；

3）识别可能被威胁利用的脆弱性；

4）识别丧失保密性、完整性和可用性可能对资产造成的影响。

识别风险的主要活动

■识别资产

- ●资产(asset)
  对组织有价值的任何东西。[ISO/IEC 13335-1:2004]
- ●确定资产类别
  资产应按组织的需要划分类别。例如，可分类如下：
  信息、业务和管理过程、人员、方针和规程、服务、
  ICT系统、场所、以及公司的品牌和声誉等。
- ●列出资产清单

识别风险的主要活动

■识别资产的脆弱性、威胁和风险

- 威胁
  可能对系统或组织产生损害的不期望事件的潜在原因。
- 脆弱性
  可能被某个威胁所利用的资产或控制措施的弱点。
  [ISO/IEC27000:2009]
- 风险
  意味着可能发生安全事件
  威胁+ 脆弱性⇒安全事件

4.2.1 建立ISMS

e）分析和评价风险

1）在考虑丧失资产的保密性、完整性和可用性所造成的后果的情况下，评估安全失效可能造成的对组织的影响。

2）根据主要的威胁和脆弱性、对资产的影响以及当前所实施的控制措施，评估安全失效发生的现实可能性。

3）估计风险的级别。

4）确定风险是否可接受，或者是否需要使用在4.2.1 c)2)中所建立的接受风险的准则进行处理。

风险估计与评价

■风险估计

●对业务的影响

- 信息安全突破的后果
- 资产的价值

●可能性

- 脆弱性被利用的难易程度
- 威胁源的动机和能力

●风险级别

可能性	影响		
	低	中	高
低	低	低	低
中	低	中	中
高	低	中	高

■风险评价

●排列风险的优先级，关注重大风险

●剔除低风险项或可接受的风险项

4.2.1 建立ISMS

f）识别和评价风险处理的可选措施

可能的措施包括：

1）采用适当的控制措施；

2）在明显满足组织方针策略和接受风险的准则的条件下，有意识地、客观地接受风险[见4.2.1 c)2)]；

3）避免风险；

4）将相关业务风险转移到其他方，如：保险，供应商等。

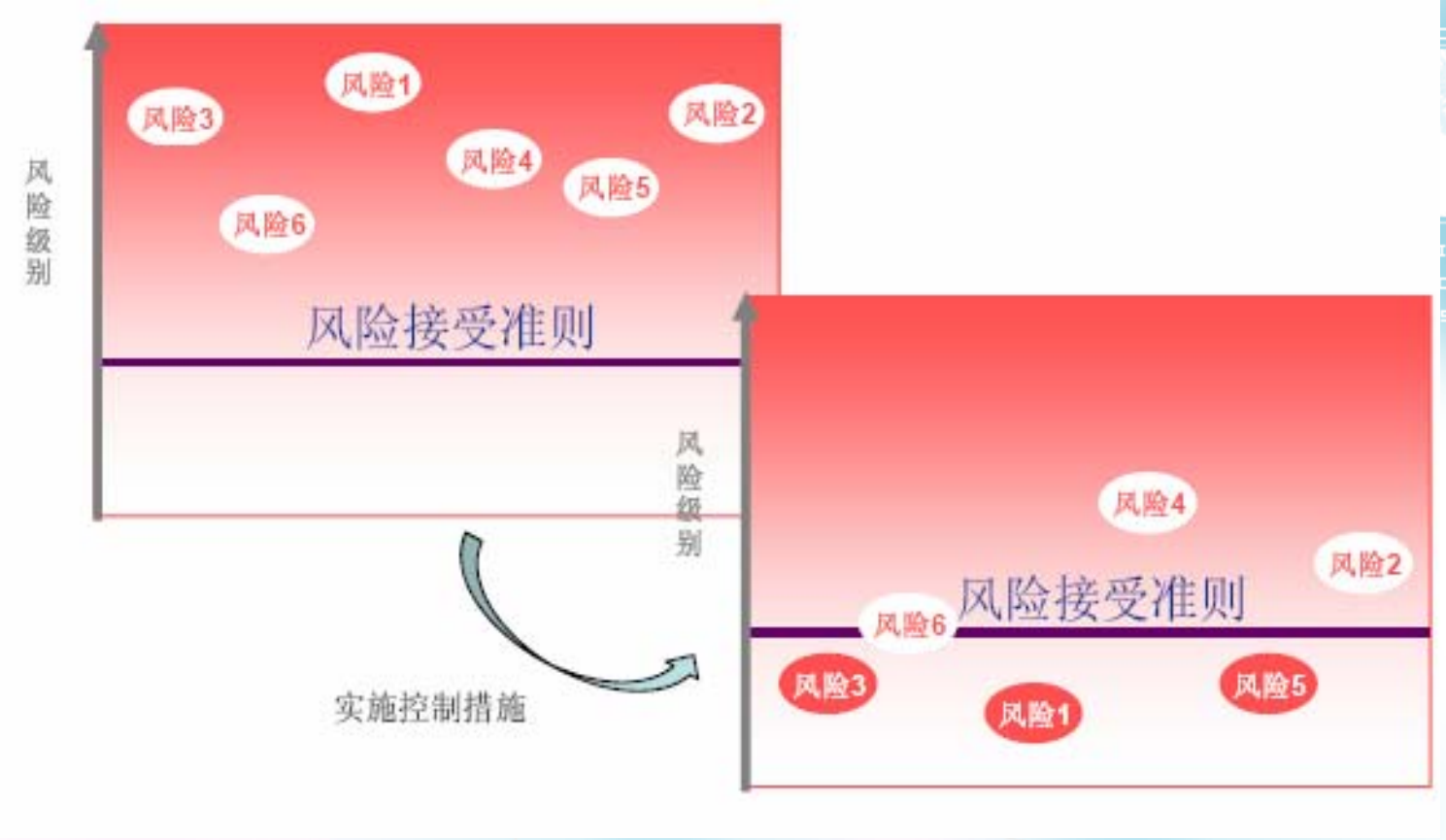
风险的应对策略

- 风险降低(risk reduction)
  采取行动降低风险发生的可能性或减轻负面后果，或同时降低风险发生的可能性和减轻负面后果
- 风险避免(risk avoidance)
  决定不卷入风险处境或从风险处境中撤出
- 风险保持(risk retention)
  接受特定风险带来的损失或收益
- 风险转移(risk transfer)
  与其它组织分担风险的损失或收益

注：在安全风险范畴内，转移风险只考虑负面后果（损失）。

注：以上术语的定义均来自[ISO/IEC Guide 73:2002]

风险降低


风险级别
风险1
风险2
风险3
风险4
风险5
风险6
风险接受准则
风险级别
实施控制措施
风险4
风险2
风险6
风险接受准则
风险3
风险1
风险5

风险保持

- 管理者在某种情形下可有意、客观地接受风险，例如：
  - 控制措施不能使风险降低到可接受的水平
  - 受资金或技术的限制
  - 风险无法避免或转移
- 风险保持并非放弃管理，风险仍需进行跟踪监督：
  - 定期评估风险状况的改变和趋势
  - 如风险状况持续恶化，必要时应启动应急措施

4.2.1 建立ISMS

g) 为处理风险选择控制目标和控制措施

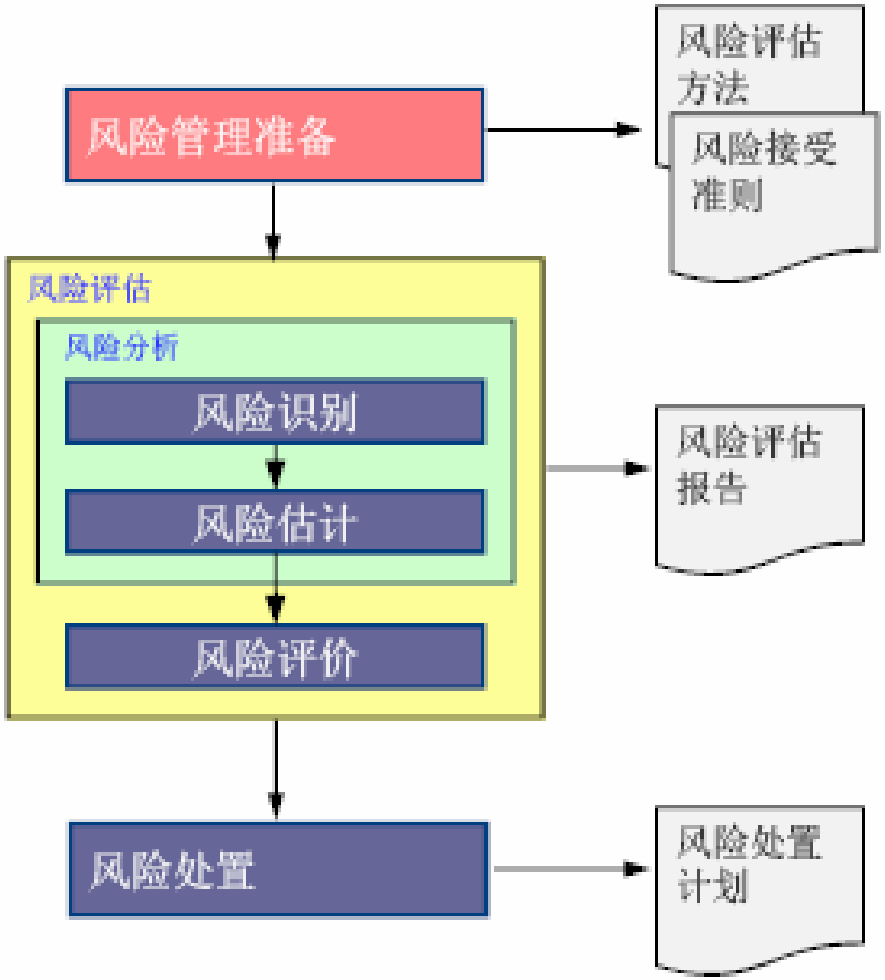
- 控制目标和控制措施应加以选择和实施，以满足风险评估和风险处置过程中所识别的要求。这种选择应考虑接受风险的准则（见**4.2.1c）2）**）以及法律法规和合同要求。
- 从附录**A**中选择控制目标和控制措施应成为此过程的一部分，该过程适合于满足这些已识别的要求。
- 附录**A**所列的控制目标和控制措施并不是所有的控制目标和控制措施，组织也可能需要选择另外的控制目标和控制措施。

4.2.1 建立ISMS

h) 获得管理者对建议的残余风险的批准

- 建议的残余风险：
- 是对选择的风险控制措施实施后的效果所作出的预测；
- 对控制措施的预期结果由管理层作出决策.

风险管理活动及输出


风险管理准备
风险评估方法
风险接受准则
风险评估
风险分析
风险识别
风险估计
风险评价
风险评估报告
风险处置
风险处置计划

4.2.1 建立ISMS

i) 获得管理者对实施和运行ISMS的授权

j) 准备适用性声明（SoA）

应从以下几方面准备适用性声明：

1）4.2.1 g）所选择的控制目标和控制措施，以及选择的理由；

2）当前实施的控制目标和控制措施（见4.2.1e）2））；

3）对附录A中任何控制目标和控制措施的删减，以及删减的合理性说明。

注：适用性声明提供了一份关于风险处理决定的综述。删减的合理性说明提供交叉检查，以证明不会因疏忽而遗漏控制措施。

适用性声明

控制措施参引号	控制措施	适用性(是/否)	合理性说明
A.9.2.2	支持性设施	是	已配置了UPS电源，可保证主机1小时供电； 经风险评估，供电保障不充分，计划购买应急发电机。
A.10.4.1	恶意代码	是	一安装了覆盖全公司的防病毒服务器； 后续措施包括： 1. 制定防病毒策略文件

4.2 建立和管理ISMS

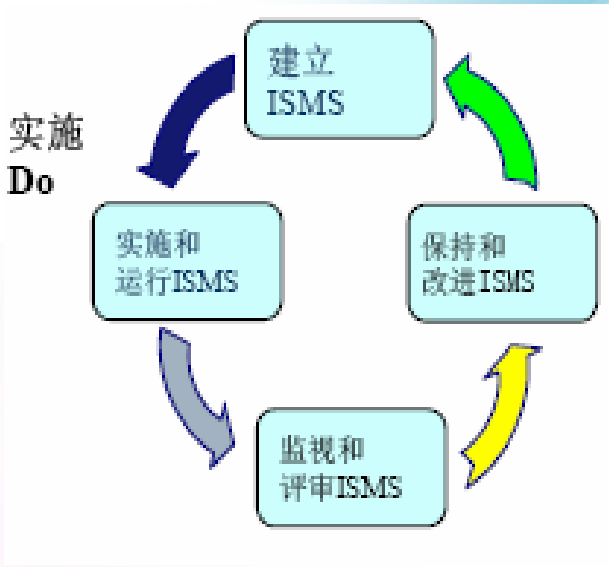
4.2.2 实施和运行ISMS

组织应：

a）为管理信息安全风险识别适当的管理措施、资源、职责和优先顺序，即：制定风险处置计划（见第5章）。

b）实施风险处置计划以达到已识别的控制目标，包括资金安排、角色和职责的分配。

c）实施4.2.1 g）中所选择的控制措施，以满足控制目标。



4.2 建立和管理ISMS

4.2.2 实施和运行ISMS（续）

d）确定有效性，并指明如何用来评估控制措施的有效性，以产生可比较的和可再现的结果（见4.2.3 c））如何测量所选择的控制措施或控制措施集的。

注：测量控制措施的有效性可使管理者和员工确定控制措施达到既定的控制目标的程度。

e）实施培训和意识教育计划（见5.2.2）。

f）管理ISMS的运行。

g）管理ISMS的资源（见5.2）。

h）实施能够迅速检测安全事态和响应安全事件的规程和其他控制措施（见4.2.3a））

信息安全事件管理

术语和定义

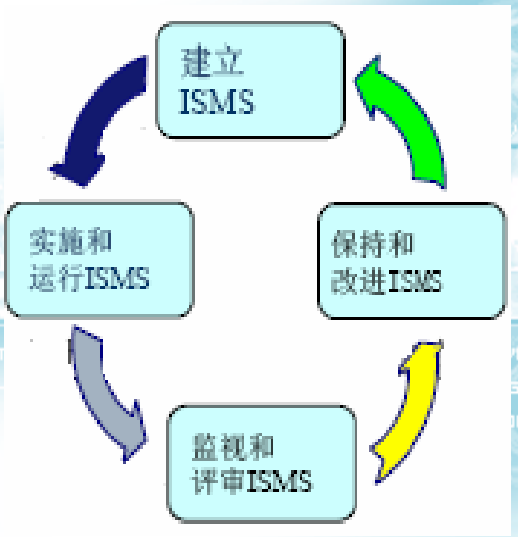
- 信息安全事态(information security event)
  信息安全事态是指系统、服务或网络的一种可识别的状态的发生，它可能是对信息安全策略的违反或防护措施的失效，或是和安全关联的一个先前未知的状态。
- 信息安全事件(information security incident)
  一个信息安全事件由单个的或一系列的有害或意外信息安全事态组成，它们具有损害业务运作和威胁信息安全的极大的可能性。

响应安全事件

- 预先制定信息安全事件处理流程
- 当发生安全事件时，启动处理流程

4.2 建立和管理ISMS

4.2.3 监视和评审ISMS



组织应：

a) 执行监视与评审规程和其它控制措施，以：

1）迅速检测过程运行结果中的错误；

2）迅速识别试图的和得逞的安全违规和事件；

3）使管理者能够确定分配给人员的安全活动或通过信息技术实施的安全活动是否被如期执行；

4）通过使用指示器，帮助检测安全事态并预防安全事件；

5）确定解决安全违规的措施是否有效。

4.2 建立和管理ISMS

4.2.3 监视和评审ISMS（续）

b) 在考虑安全审核结果、事件、有效性测量结果、所有相关方的建议和反 馈的基础上，进行ISMS有效性的定期评审（包括满足ISMS方针和目标，以及安全控制措施的评审）。

c) 测量控制措施的有效性以验证安全要求是否被满足。

4.2 建立和管理ISMS

4.2.3 监视和评审ISMS （续）

d) 按照计划的时间间隔进行风险评估的评审，以及对残余风险和已确定的可接受的风险级别进行评审，应考虑以下方面的变化：

- 组织；
- 技术；
- 业务目标和过程；
- 已识别的威胁；
- 已实施的控制措施的有效性；
- 外部事态，如法律法规环境的变更、合同义务的变更和社会环境的变更。

4.2 建立和管理ISMS

4.2.3 监视和评审ISMS

e) 按计划的时间间隔，实施ISMS内部审核（见第6章）。

f) 定期进行ISMS管理评审，以确保ISMS范围保持充分，ISMS过程的改进得到识别（见7.1）。

g) 考虑监视和评审活动的结果，以更新安全计划。

h) 记录可能影响ISMS的有效性或执行情况的措施和事态（见4.3.3）。

测量

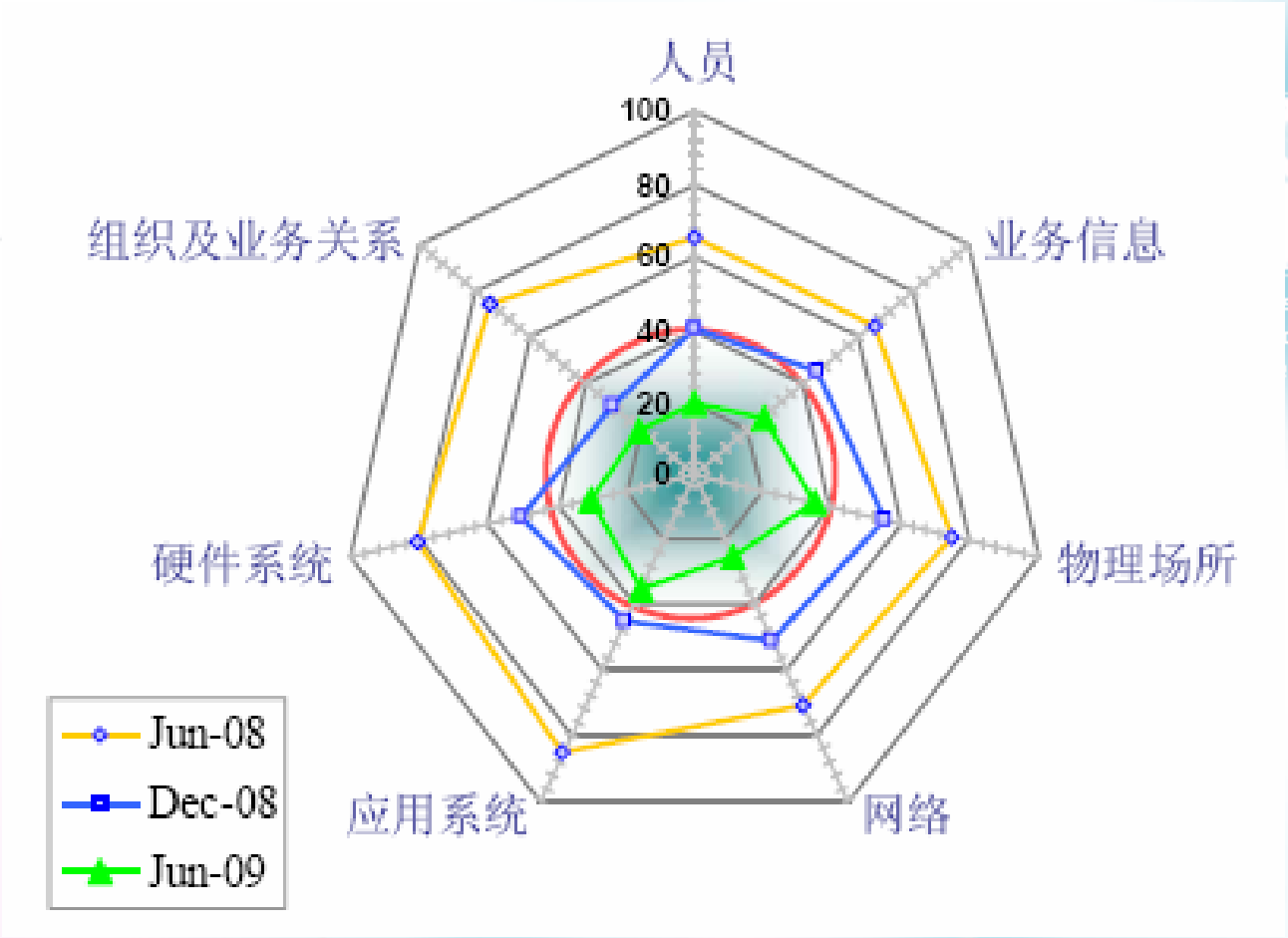
■测量的目的

- ●证实ISMS和已实施的风险控制措施的有效性
- ●向管理层提供信息资产安全及管理状况的客观信息，以便决策
- ●为ISMS改进提供输入
- ●建立基准

■可测量的领域

- ●风险（再）评估和处置的结果
- ●信息安全事件处理过程的性能
- ●信息安全审核结果
- ●人员信息安全意识和知识能力的提升
- ●信息安全管理的成本和效益

示例：信息资产安全指示器



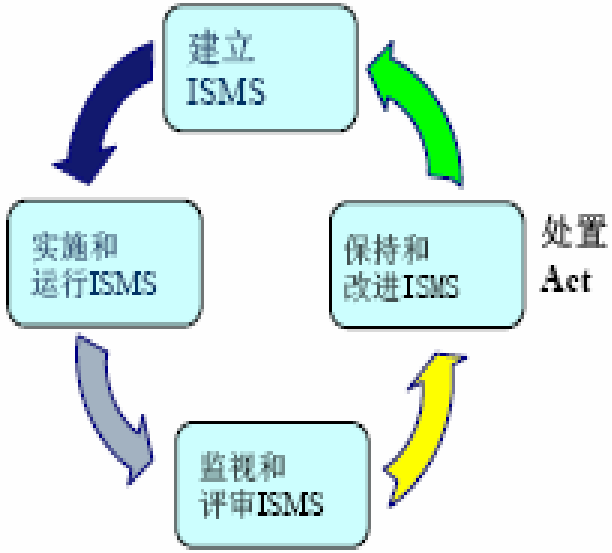
评审

两类评审

- 管理评审
  - 评审ISMS，确保其适用性、充分性和有效性
  - 高层管理者和各业务单位主管
  - 频度： 按管理体系要求，但每年至少一次。
- 体系运行监督评审
  - 安全管理细节和技术相关内容的研讨
  - 参与者为与评审主题相关联的人员
  - 定期（如，季/月度），或事件驱动

4.2 建立和管理ISMS

4.2.4 保持和改进ISMS



组织应经常：

a) 实施已识别的ISMS改进措施。

b) 依照8.2和8.3采取合适的纠正和预防措施。从其它组织和组织自身的安全经验中吸取教训。

c) 向所有相关方沟通措施和改进情况保持，其详细程度应与环境相适应，需要时，商定如何进行。

d) 确保改进达到了预期目标。

改进ISMS

■包括：

- ●ISMS相关的方针、过程、规程
- ●管理能力
  - 测量分析
  - 方法和工具

4.3 文件要求

●4.3.1 总则

- 文件应包括管理决定的记录，以确保所采取的措施符合管理决定和方针策略，还应确保所记录的结果是可重复产生的。
- 重要的是，能够显示出所选择的控制措施回溯到风险评估和风险处置过程的结果、并进而回溯到ISMS方针和目标之间的关系。

文件和记录

■文件

信息及其承载媒介

示例：记录、规范、程序文件、图样、报告、标准。

注1：媒介可以是纸张，磁性的、电子的光学的计算机盘片，照片或标准样品，或它们的组合。

■记录

阐明所取得的结果或提供所完成活动的证据的文件。

[ISO 9000:2005]

4.3 文件要求

4.3.1 总则

ISMS文件应包括：

a) 形成文件的ISMS方针[见4.2.1b）]和目标；
b) ISMS的范围[见4.2.la）]；
c) 支持ISMS的规程和控制措施；
d) 风险评估方法的描述[见4.2.1c）]；
e) 风险评估报告[见4.2.1c）到4.2.1g）]；
f) 风险处置计划[见4.2.2b）]；
g) 组织为确保其信息安全过程的有效规划、运行和控制以及描述如何测量控制措施的有效性所需的形成文件的规程（见.2.3c））；
h) 本标准所要求的记录（见4.3.3）；
I) 适用性声明。

4.3 文件要求

4.3.1 总则

注1：本标准出现“形成文件的规程”之处，即要求建立该规程，形成文件，并加以实施和保持。

注2：不同组织的ISMS文件的详略程度取决于：组织的规模和活动的类型；安全要求和被管理系统的范围及复杂程度；

注3：文件和记录可以采用任何形式或类型的介质。

4.3 文件要求

4.3.2 文件控制

ISMS所要求的文件应予以保护和控制。应编制形成文件的规程，以规定以下方面所需的管理措施：

a) 文件发布前得到批准，以确保文件是适当的；
b) 必要时对文件进行评审、更新并再次批准；
c) 确保文件的更改和现行修订状态得到标识；
d) 确保在使用处的获得适用文件的相关版本；
e) 确保文件保持清晰、易于识别；
f) 确保文件对需要的人员可用，并依照文件适用的类别程序进行传输、贮存和最终销毁；
g) 确保外来文件得到标识；
h) 确保文件的分发得到控制；
i) 防止作废文件的非预期使用；
j) 若因任何的目的而保留作废文件时，对这些文件进行适当的标识。

4.3 文件要求

4.3.3 记录控制

- 应建立记录并加以保持，以提供符合ISMS要求和有效运行的证据。应对记录加以保护和控制。ISMS的记录应考虑相关法律法规要求和合同义务。记录应保持清晰、易于识别和检索。记录的标识、贮存、保护、检索、保存期限和处置所需的控制措施应形成文件并实施。
- 应保留4.2中列出的过程执行记录和所有发生的与ISMS有关的重大安全事件的记录。
- 例如：记录包括访客登记薄、审核报告和已完成的访问授权单

5 管理职责

■5.1 管理承诺

管理者应通过以下活动，对建立、实施、运行、监视、评审、保持和改进ISMS的承诺提供证据：

a) 制定ISMS方针；
b) 确保ISMS目标和计划得以制定；
c) 建立信息安全的角色和职责；
d) 向组织传达满足信息安全目标、符合信息安全方针、履行法律责任和持续改进的重要性；
e) 提供足够资源，以建立、实施、运行、监视、评审、保持和改进ISMS（见5.2.1）；
f) 决定接受风险的准则和风险的可接受级别；
g) 确保ISMS内部审核的执行（见第6章）；
h) 实施ISMS的管理评审（见第7章）。

5 管理职责

■5.2 资源管理

●5.2.1 资源提供

组织应确定并提供所需的资源，以：

a) 建立、实施、运行、监视、评审、保持和改进ISMS；

b) 确保信息安全规程支持业务要求；

c) 识别和满足法律法规要求、以及合同中的安全义务；

d) 通过正确实施所有的控制措施保持适当的安全；

e) 必要时，进行评审，并适当响应评审的结果；

f) 在需要时，改进ISMS的有效性。

5 管理职责

■5.2 资源管理

●5.2.2 培训、意识和能力

组织应通过以下方式，确保所有分配有ISMS职责的人员具有执行所要求任务的能力：

a) 确定从事影响ISMS工作的人员所必要的能力；

b) 提供培训或采取其他措施（如聘用有能力的人员）以满足这些需求；

c) 评价所采取的措施的有效性；

d) 保持教育、培训、技能、经历和资格的记录（见4.3.3）。

e) 组织也应确保所有相关人员意识到其信息安全活动的相关性和重要性，以及如何为达到ISMS目标做出贡献。

6 ISMS内部审核

组织应按照计划的时间间隔进行内部ISMS审核，以确定其ISMS的控制目标、控制措施、过程和规程是否：

a) 符合本标准和相关法律法规的要求；

b) 符合已确定的信息安全要求；

c) 得到有效地实施和保持；

d) 按预期执行。

6 ISMS内部审核

●应在考虑拟审核的过程与区域的状况和重要性以及以往审核的结果的情况下，制定审核方案。应确定审核的准则、范围、频次和方法。审核员的选择和审核的实施应确保审核过程的客观性和公正性。审核员不应审核自己的工作。

●策划和实施审核、报告结果和保持记录（见**4.3.3**）的职责和要求应在形成文件的规程中做出规定。

●负责受审区域的管理者应确保及时采取措施，以消除已发现的不符合及其产生的原因。跟踪活动应包括对所采取措施的验证和验证结果的报告（见第**8**章）。

• 注：**GB/T 19011-2003(**《质量和(或)环境管理体系审核指南》 **)**也可为实施内部**ISMS**审核提供有用的指导。

7 ISMS的管理评审

■7.1 总则

管理者应按计划的时间间隔（至少每年1次）评审组织的ISMS，以确保其持续的适宜性、充分性和有效性。评审应包括评估ISMS改进的机会和变更的需要，包括信息安全方针和信息安全目标。评审的结果应清晰地形成文件，记录应加以保持（见4.3.3）。

7 ISMS的管理评审

■7.2 评审输入

管理评审的输入应包括：

a) ISMS审核和评审的结果；

b) 相关方的反馈；

c) 组织用于改进ISMS执行情况和有效性的技术、产品或规程；

d) 预防和纠正措施的状况；

e) 以往风险评估没有充分强调的脆弱点或威胁；

f) 有效性测量的结果；

g) 以往管理评审的跟踪措施；

h) 可能影响ISMS的任何变更；

I) 改进的建议。

7 ISMS的管理评审

■7.3 评审输出

管理评审的输出应包括与以下方面有关的任何决定和措施：

a) ISMS有效性的改进；

b) 风险评估和风险处理计划的更新；

c) 必要时修改影响信息安全的规程和控制措施，以响应内部或外部可能影响ISMS的事态，包括以下的变更：

1. 业务要求；
2. 安全要求；
3. 影响现有业务要求的业务过程；
4. 法律法规环境；
5. 合同义务；
6. 风险级别和/或接受风险的准则。

d) 资源需求；

e) 如何测量控制措施有效性的改进。

8 ISMS改进

8.1 持续改进

组织应通过使用信息安全方针、安全目标、审核结果、监视事态的分析、纠正和预防措施以及管理评审（见第7章），持续改进ISMS的有效性。

8 ISMS改进

8.2 纠正措施

组织应采取措施，以消除与ISMS要求不符合的原因，以防止再发生。形成文件的纠正措施规程，应规定以下方面的要求：

a)识别不符合；

b)确定不符合的原因；

c) 评价确保不符合不再发生的措施需求；

d)确定和实施所需要的纠正措施；

e)记录所采取措施的结果（见4.3.3）；

f) 评审所采取的纠正措施。

8 ISMS改进

■8.3 预防措施

组织应确定措施，以消除潜在不符合的原因，防止其发生。预防措施应与潜在问题的影响程度相适应。形成文件的预防措施规程，应规定以下方面的要求：

a) 识别潜在的不符合及其原因；

b) 评价防止不符合发生的措施需求；

c) 确定和实施所需要的预防措施；

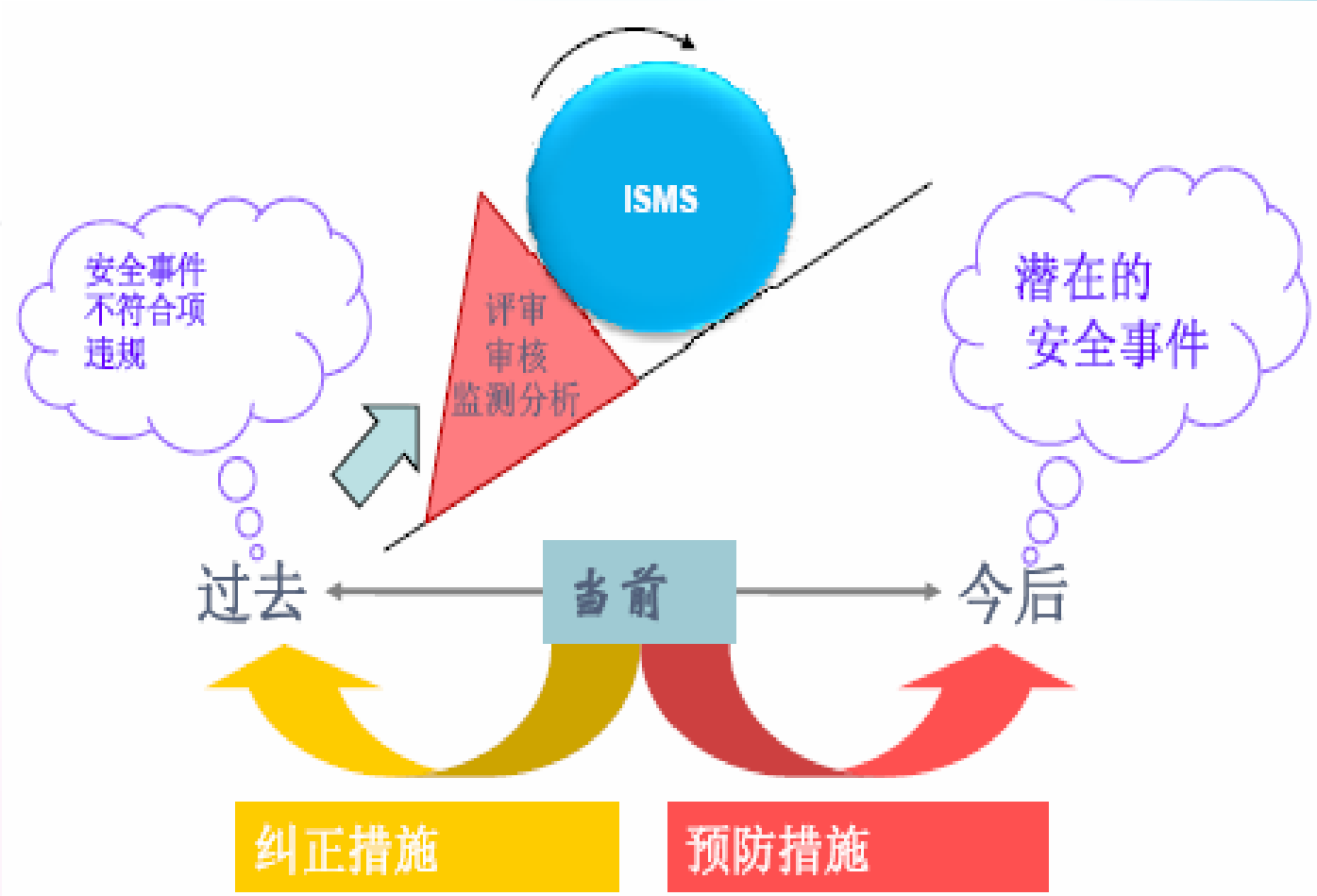
d) 记录所采取措施的结果（见**4.3.3**）；

e) 评审所采取的预防措施。

组织应识别变化的风险，并识别针对重大变化的风险的预防措施的要求。预防措施的优先级要根据风险评估的结果确定。

注：预防不符合的措施通常比纠正措施更节约成本。

ISMS改进



国佳基业
GORGEOUS

谢谢！