信息安全管理体系(ISMS)

2009年12月28日

内容纲要

- 第一部分 ISMS体系概念综述
- 第二部分 ISMS国际标准介绍
- 第三部分 ISMS国家标准解读
  - GB/T 22080-2008《信息技术　安全技术　信息安全管理体系 要求》
  - GB/T 22081-2008《信息技术　安全技术　信息安全管理实用规则》
  - GB/T 20984-2007《信息安全技术　信息安全风险评估规范》
  - GB/T 20988-2007《信息安全技术　信息系统灾难恢复规范》
  - GB/Z 20985-2007《信息技术　安全技术　信息安全事件管理指南》

内容纲要

- **第一部分 ISMS体系概念综述**
- 第二部分 ISMS国际标准介绍
- 第三部分 ISMS国家标准解读
  - GB/T 22080-2008《信息技术　安全技术　信息安全管理体系 要求》
  - GB/T 22081-2008《信息技术　安全技术　信息安全管理实用规则》
  - GB/T 20984-2007《信息安全技术　信息安全风险评估规范》
  - GB/T 20988-2007《信息安全技术　信息系统灾难恢复规范》
  - GB/Z 20985-2007《信息技术　安全技术　信息安全事件管理指南》

第一部分 ISMS体系概念综述

- 1.1 ISMS概念
- 1.2 ISMS定位
- 1.3 ISMS方法
- 1.4 ISMS过程
- 1.5 ISMS内容
- 1.6 ISMS关键
- 1.7 ISMS全貌

第一部分 ISMS体系概念综述

- **1.1 ISMS概念**
- 1.2 ISMS定位
- 1.3 ISMS方法
- 1.4 ISMS过程
- 1.5 ISMS内容
- 1.6 ISMS关键
- 1.7 ISMS全貌

1.1 ISMS概念

- 概念要素
- 信息
- 安全
- 管理
- 体系
- 信息安全
- 信息安全管理
- 信息安全管理体系

1.1 ISMS概念

- 概念名称
  - 信息安全管理体系（Information Security Management System，ISMS）
- 概念要素
  - 信息（Information）
  - 安全（Security）
  - 管理（Management）
  - 体系（System）

1.1 ISMS概念

- 信息（Information）
  - 概念体系：数据、信息、知识、智慧

1.1 ISMS概念

- 信息（续）
  - 信息资产
    - 资产是具有价值的任何事物。
    - 信息也是一种资产。在当今的信息时代，继物质和能源之后，信息成为又一战略资源，起着至关重要的全局作用。
    - 信息具有广泛的内容，如国家政策、法律法规、公司战略、组织结构、规章制度、操作规程、日常记录、工作计划、技术资料、设计图纸、程序代码、产品手册、人员名簿、商业机密、公众形象等等。

1.1 ISMS概念

- 信息（续）
  - 信息系统
    - 信息本身是无形的，借助于载体而存在。
    - 信息载体类型：处理载体、存储载体、传输载体和接口载体。
    - 信息载体实例：人的大脑与五官；计算机与网络。
    - 信息系统范畴：计算机及其网络系统。
    - 信息系统技术：信息技术（IT）或信息与通信技术（ICT）。

1.1 ISMS概念

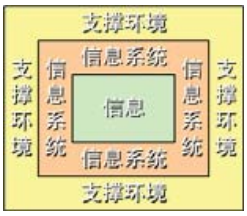
- 信息（续）
  - 信息系统（续）
    - 计算机信息系统定义：“由计算机及其相关的和配套的设备、设施（含网络）构成的，按照一定的应用目标和规则对信息进行采集、加工、存储、传输、检索等处理的人机系统。”（引自《中华人民共和国计算机信息系统安全保护条例》［国务院令第147号 1994年2月18日］第二条）

1.1 ISMS概念

- 信息（续）
  - 支撑环境
    - 信息系统建立并运行在一定的环境之中，包括硬环境和软环境。
    - 硬环境：机房、电力、照明、温控、湿控、防盗、防火、防震、防水、防雷、防电磁辐射、抗电磁干扰等设施；
    - 软环境：法律法规、规章制度、思想意识、政治经济、社会文化、组织机构、人员素质、教育培训、认证认可、监督管理等方面。

1.1 ISMS概念

- 信息（续）
  - 信息、信息系统和支撑环境之间的依赖关系

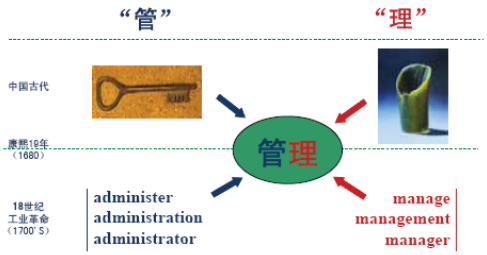


1.1 ISMS概念

- 安全（Security/Safety）
  - 任何有价值的事物（即资产）都存在安全问题。
  - 两个近似的安全概念："Security"和"Safety"。
  - Security：事物保持不受损害的一种能力属性。
  - Safety：事物处于不受损害的一种状态属性。
    - Safety定义："摆脱了不可接受风险。"（引自ISO/IEC指南51:1999《安全方面标准中安全引入指南》）
  - 为与Safety区别，Security也译为安全性。
  - "信息安全管理体系"中考虑的"安全"是指安全能力，即Security。

1.1 ISMS概念

- 管理（Management）
  - 文化背景

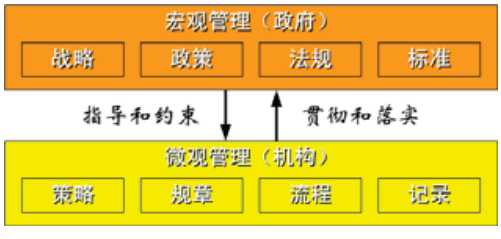


1.1 ISMS概念

- 管理（续）
  - 管理定义：通过规划、组织、领导、沟通和控制等环节来协调人力、物力、财力等资源，以期有效达成组织目标的过程。
  - 管理特征：在群体活动中，在特定环境下，针对给定对象，遵循确定原则，运用恰当方法，按照规定程序，利用可用资源，进行一组活动（包括规划、组织、指导、沟通和控制等），完成各项任务，评价执行成效，实现既定目标。

1.1 ISMS概念

- 管理（续）
  - 管理层面



1.1 ISMS概念

- 管理（续）
  - 管理方法：管理是一种过程，应采用过程方法。
  - 管理模型：PDCA模型是一种经实践证明的、被公认的有效管理模型。

1.1 ISMS概念

- 体系/系统（System）
  - 一般定义：由一定范围内具有内在联系的要素组成的科学有机整体，它反映出要素间的互依赖和互影响。
  - “System”中译文：“体系”或“系统”。
    - 当组成要素主要是人和文档这样的管理要素时，用“体系”来表述，例如，质量管理体系（QMS）；
    - 当组成要素以纯技术要素为主时，则用“系统”来表述，例如，入侵检测系统。
  - 体系更多地需要人的参与才能运行，而系统更多地依赖于技术手段来达到自动或半自动运行。
  - ISMS属于管理层面，因此用“体系”来表述。

1.1 ISMS概念

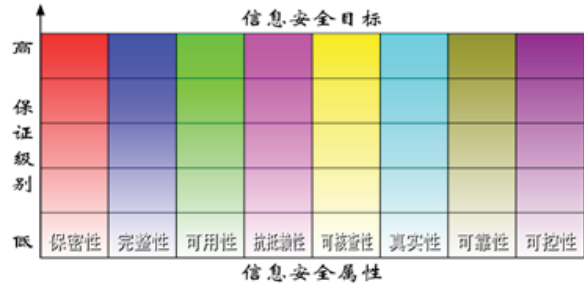
- 信息安全（Information Security）
  - 广义的信息安全
    - 泛指信息、信息系统及其支撑环境的安全性，将三者的安全性都包含在信息安全的概念范畴之内。
    - 信息是核心，信息系统和支撑环境是保障；信息本身的安全性是目的，信息系统和支撑环境的安全性是手段。
  - 狭义的信息安全
    - 仅指信息本身的安全性。

1.1 ISMS概念

- 信息安全（续）
  - 信息安全属性：信息、信息系统及其支撑环境的安全特性。
    - **保密性（confidentiality）**
    - **完整性（integrity）**
    - **可用性（availability）**
    - 抗抵赖性（non-repudiation）
    - 可核查性（accountability）
    - 真实性（authenticity）
    - 可靠性（reliability）
    - 可控性（controllability）

1.1 ISMS概念

- 信息安全（续）
  - 信息安全目标



1.1 ISMS概念

- 信息安全（续）
  - 信息安全属性关系
    - 信息安全基本属性之间不是相互孤立的，而是相互关联的。一种安全属性的损失会导致另一种或多种安全属性的损失。
    - 因此，更多关注某一方面的安全属性，不等于忽视其他方面的安全属性，而应依据安全目标的要求和安全属性的关联，在各安全属性之间进行权衡，以确保整体安全目标的达成。

1.1 ISMS概念

- 信息安全管理（Information Security Management）
  - 一般定义
    - 在信息安全方面，通过规划、组织、领导、沟通和控制等环节来协调人力、物力、财力等资源，以期有效达成组织信息安全目标的过程。
    - 对信息、信息系统及其支撑环境安全性的管理。

1.1 ISMS概念

- 信息安全管理（续）
  - 广义的信息安全管理
    - 包括宏观和微观两个层面。
    - 在宏观层面，通常被称为“信息安全保障”，例如，国家信息安全保障体系。
  - 狭义的信息安全管理
    - 仅指微观层面。
    - 通常所说的“信息安全管理”一般指微观层面，例如，信息安全管理体系（ISMS）。

1.1 ISMS概念

- 信息安全管理体系（Information Security Management Systems，ISMS）
  - 一般定义：对信息、信息系统及其支撑环境的安全性进行管理的体系。

1.1 ISMS概念

- 信息安全管理体系（续）
  - 考虑因素
    - 定位问题：在哪里管？
      答：针对微观层面实体（即一个组织或机构）而开展的信息安全管理。
    - 目的问题：为何而管？
      答：保护信息免受各种威胁的损害，以确保业务持续性，业务风险最小化，投资回报和商业机遇最大化。
    - 主体问题：由谁来管？
      答：信息和信息系统的拥有者和使用者。

1.1 ISMS概念

- 信息安全管理体系（续）
  - 考虑因素（续）
    - 客体问题：管控什么？
      答：信息、信息系统及其支撑环境的安全性。
    - 方法问题：怎么来管？
      答：系统的方法，包括过程方法、风险方法和测评方法等。
    - 资源问题：靠什么管？
      答：提供必要的人力、物力、财力、信息、知识和技术等。

1.1 ISMS概念

- 信息安全管理体系（续）
  - 考虑因素（续）
    - 测评问题：管得怎样？
      答：通过对管理效果和效率的测量、审核和评审。
    - 认证问题：如何相信？
      答：通过对管理能力和安全状况的权威证明。
    - 标准问题：遵循什么？
      答：通过标准化，规范信息安全管理的概念、要求、方法、技术、实践和准则，并提供相关指南。

1.1 ISMS概念

- 信息安全管理体系（续）
  - 层次架构（按信息系统的层次架构分）
    - 数据安全管理
    - 应用安全管理
    - 系统安全管理
    - 网络安全管理
    - 通信安全管理
    - 物理安全管理

第一部分 ISMS体系概念综述

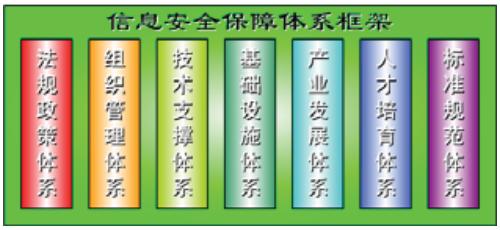
- 1.1 ISMS概念
- **1.2 ISMS定位**
- 1.3 ISMS方法
- 1.4 ISMS过程
- 1.5 ISMS内容
- 1.6 ISMS关键
- 1.7 ISMS全貌

1.2 ISMS定位

- 与信息安全保障体系的关系
- 与信息安全等级保护的关系
- 与信息安全风险评估/风险管理的关系
- 与其他管理体系的关系

1.2 ISMS定位

- 与信息安全保障体系的关系
  - 信息安全保障体系的框架



1.2 ISMS定位

- 与信息安全保障体系的关系（续）
  - ISMS与信息安全保障体系的关系
    - 信息安全保障体系面向整个社会和国家，属于宏观管理；ISMS面向各种机构、企业、部门等实体，属于微观管理。
    - ISMS是有效实现信息安全保障体系的重要管理手段。

1.2 ISMS定位

- 与信息安全等级保护的关系
  - 信息安全等级保护的地位
    - 国家信息安全保障工作的基本制度、基本策略、基本方法。
  - 信息安全等级保护的作用
    - 开展信息安全等级保护工作是保护信息化发展、维护国家信息安全的根本保障。
  - 信息安全等级保护的步骤
    - 系统定级、备案审查、安全建设、测评自查、监督检查。

1.2 ISMS定位

- 与信息安全等级保护的关系（续）
  - ISMS与信息安全等级保护的关系
    - 信息安全等级保护既是基本方法和策略，更是基本制度，具有强制性和监督性；ISMS是一种被公认为有效的信息安全管理方法和手段，具有推荐性和指导性。
    - 建立和维护ISMS，有助于有效实现信息安全等级保护。

1.2 ISMS定位

- 与信息安全风险评估/风险管理的关系
  - 信息安全风险评估的作用
    - 通过评估面临的信息安全风险，导出信息安全需求，为信息安全初期建设提供依据，以做到适度安全。
    - 通过持续的信息安全风险评估，把握信息安全状况，为信息安全持续改进提供建议，以做到恒久安全。
  - 信息安全风险管理的作用
    - 通过控制信息安全风险，实现信息安全目标。
  - 信息安全风险评估与风险管理的关系
    - 信息安全风险评估是信息安全风险管理的重要环节。

1.2 ISMS定位

- 与信息安全风险评估/风险管理的关系（续）
  - ISMS与信息安全风险评估/风险管理的关系
    - 信息安全风险管理是ISMS的基本方法。
    - 信息安全风险评估是为ISMS选择适当控制方式和措施的先决条件。

1.2 ISMS定位

- 与其他管理体系的关系
  - 其他管理体系
    - 战略与投资管理体系
    - 环境管理体系（ISO 14000）
    - 质量管理体系（ISO 9000）
    - 企业客户满意度管理体系
    - 投诉管理体系（ISO 10002/BS 8600）
    - 财务管理体系
    - 人力资源管理体系（ISO 10015）
    - 职业安全健康管理体系（OHSAS 18000）
    - 信息技术服务管理体系（ISO 20000/BS 15000）

1.2 ISMS定位

- 与其他管理体系的关系（续）
  - ISMS与其他管理体系的关系

第一部分 ISMS体系概念综述

- 1.1 ISMS概念
- 1.2 ISMS定位
- **1.3 ISMS方法**
- 1.4 ISMS过程
- 1.5 ISMS内容
- 1.6 ISMS关键
- 1.7 ISMS全貌

1.3 ISMS方法

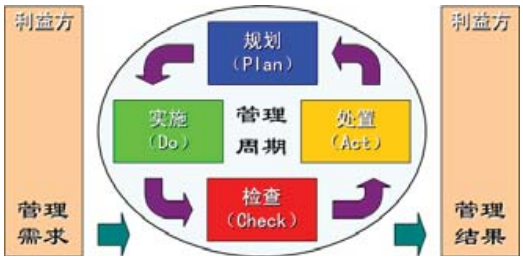
- 过程方法
- 风险方法
- 测量方法

1.3 ISMS方法

- 过程方法
  - 过程：一组将输入转化为输出的、相互关联或相互作用的活动。这种转化通常是在计划和受控的条件下，使用一定的资源来进行。
  - 过程关系
    - 过程串联：一个过程的输出直接形成下一个过程的输入。
    - 过程分解：过程中的活动也是一个过程，即一个过程可分解成多个子过程。
  - 过程方法：系统地识别、关联和控制组织中的各种过程。

1.3 ISMS方法

- 过程方法（续）
  - PDCA模型



1.3 ISMS方法

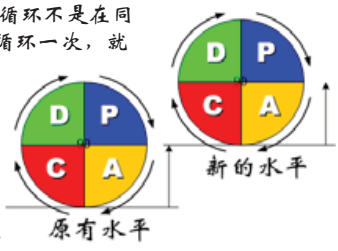
- 过程方法（续）
  - PDCA特点
    - 不间断循环：在组织的力量推动下，像车轮一样按P→D→C→A顺序滚动前进，周而复始，持续循环。

1.3 ISMS方法

- 过程方法（续）
  - PDCA特点（续）
    - 大环套小环：从整个组织、到各级部门、直至每个员工，均有各自PDCA循环，就像宇宙星系的运行一样，大环套小环，一级带一级，有机地构成一个运转体系。

1.3 ISMS方法

- 过程方法（续）
  - PDCA特点（续）
    - 阶梯式上升：PDCA循环不是在同一水平上循环，每循环一次，就解决一部分问题，取得一部分成果，工作就前进一步，水平就提高一步。到了下一次循环，又有了新的目标和内容，更上一层楼。



1.3 ISMS方法

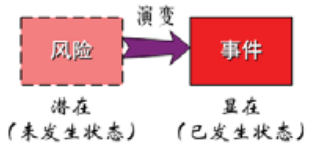
- 过程方法（续）
  - PDCA特点（续）
    - PDCA模型体现为嵌套式循环、阶梯式（或螺旋式）上升、可持续改进的管理模式。

1.3 ISMS方法

- 过程方法（续）
  - ISMS的PDCA模型

1.3 ISMS方法

- 风险方法
  - 风险与事件
    - 风险是事物可能面临特定情形发生的一种潜在状态。
    - 事件是事物已经面临特定情形发生的一种显在状态。



1.3 ISMS方法

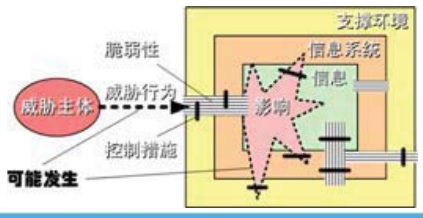
- 风险方法（续）
  - 风险：事件的可能性和其结果的结合。
  - 结果可以是正面的（利益），也可以是负面的（损失）。
  - 与之对应，风险可以是正面的（机遇），也可以是负面的（挑战）。
  - 风险管理：以合理的风险控制成本来最大化因冒风险而有机会带来的利益和最小化因冒风险而可能导致的损失。

1.3 ISMS方法

- 风险方法（续）
  - 合理并可行的安全管理应以风险为中心，从风险出发，最终再回到风险。
    - 首先，对所保护资产面临的安全风险进行识别和评估；
    - 然后，针对所识别的风险特点以及所评估的风险程度，选择和实施相应的、适度的安全控制措施；
    - 其后，检查所实施安全控制措施的效果，监视安全控制措施的运行状况和安全风险的变化情况，及时发现问题并寻求改进；
    - 从而，达到并保持将安全风险控制在可接受的程度。

1.3 ISMS方法

- 风险方法（续）
  - 信息安全风险的概念模型
    - 威胁主体**可能**利用信息、信息系统或支撑环境的脆弱性，对信息、信息系统和支撑环境实施威胁行为，**可能**造成负面影响。



1.3 ISMS方法

- 风险方法（续）
  - 信息安全风险的基本要素
    - 资产（asset）：对组织具有价值的任何东西。
    - 威胁（threat）：导致对系统或组织伤害事件的潜在原因。由威胁主体和威胁行为组成。
    - 脆弱性（vulnerability）：可能被一个或多个威胁利用的资产或资产组的弱点。
    - 影响（impact）：信息安全事件的结果。
    - 控制措施（control）：处理风险的实践、规程或机制。

1.3 ISMS方法

- 风险方法（续）
  - 信息安全风险管理的基本原理
    - 信息安全风险管理围绕着上述信息安全的基本属性（简称安全属性）和信息安全风险的基本要素（简称风险要素）展开。
    - 首先，从每个安全属性的角度对各个风险要素及其相互关系进行识别、分析和评价，得出反映风险重要程度的风险等级（即风险评估）。

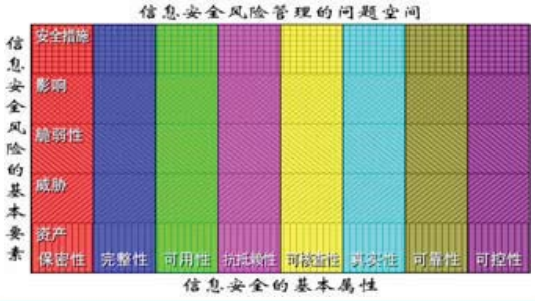
1.3 ISMS方法

- 风险方法（续）
  - 信息安全风险管理的基本原理（续）
    - 然后，对照事先确定的风险接受准则，判断风险是否可接受；对于不可接受的风险，针对各个风险要素分别采取相应的控制措施：
      - 针对资产的保护和备份措施
      - 针对威胁主体的威慑和打击措施
      - 针对威胁行为的防范和抵御措施
      - 针对脆弱性的加固和补丁措施
      - 针对影响的抑制和弥补措施

      从而改进和完善现有的控制措施（即风险处理）。

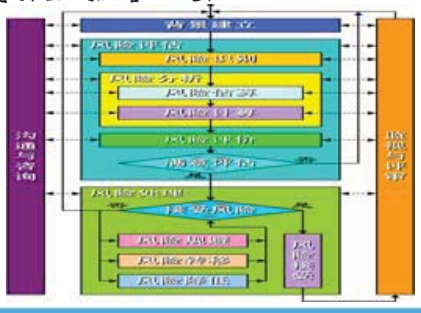
1.3 ISMS方法

- 风险方法（续）
  - 信息安全风险管理的问题空间



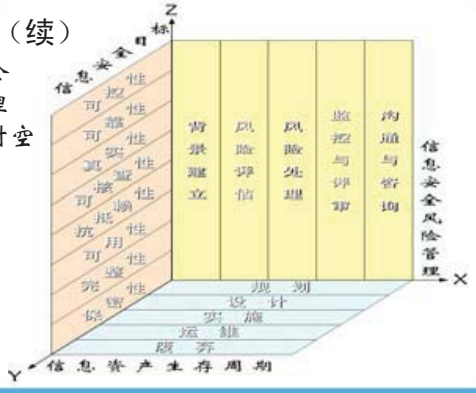
1.3 ISMS方法

- 风险方法（续）
  - 信息安全风险管理过程



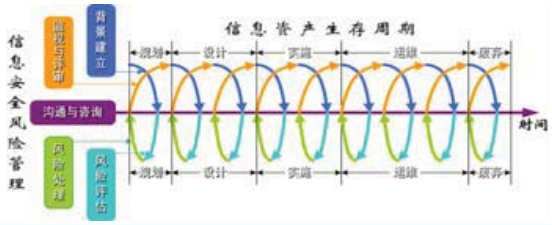
1.3 ISMS方法

- 风险方法（续）
  - 信息安全风险管理的运用时空
    - 从时间角度看



1.3 ISMS方法

- 风险方法（续）
  - 信息安全风险管理的运用时空（续）
    - 从时间角度看（续）
      - 信息安全风险管理与信息资产生命周期的过程嵌套关系



1.3 ISMS方法

- 风险方法（续）
  - 信息安全风险管理的运用时空（续）
    - 从空间纵向角度看
      - 可被运用在组织的许多层面上，包括战略层面、战术层面和运行层面。
      - 可被应用在从组织级的广泛问题到项目或系统级的特定问题中。
    - 从空间横向角度看
      - 可被运用于信息技术应用的所有领域中：政务、商务、财政、金融、保险、税务、海关、工商、质检、通信、交通、电力、制造、教育、医药、环保、传媒、娱乐、城管、公安、立法、司法、人事、外交、军事等。

1.3 ISMS方法

- 风险方法（续）
  - 背景建立
    - 建立组织的内外背景和风险管理背景的过程。
    - 风险管理的准备，为后续过程建立活动背景。
    - 信息安全风险管理过程总是发生在一定的背景之下，即组织背景和风险管理背景。
    - 组织背景
      - 组织的外部和内部背景及其相互关系.
    - 风险管理背景
      - 风险管理的目标、策略、范围、方法、依据、组织、对象、计划和文档以及风险测量的各项准则。

1.3 ISMS方法

- 风险方法（续）
  - 风险评估
    - 风险评估是风险识别、风险分析和风险评价的整个过程。
    - 风险管理的依据，为其他过程提供决策依据。

1.3 ISMS方法

- 风险方法（续）
  - 风险评估（续）
    - 风险评估原理
      - 风险识别解决风险是什么（What）、在哪里（Where）和何时（When）发生的问题；
      - 风险分析解决风险为什么（Why）发生和相对级别（Level）的问题；
      - 风险评价解决风险有多么（How）严重的问题。
      - 各项风险评估活动均围绕着风险要素（即资产、威胁、脆弱性、影响和控制措施）进行。

1.3 ISMS方法

- 风险方法（续）
  - 风险评估（续）
    - 风险要素评估
      - 资产价值的高低
        = 资产获取价值的贵廉 + 资产作用价值的高低
      - 威胁潜力的大小
        = 威胁主体动机的强弱 + 威胁行为能力的大小
      - 脆弱性被利用的难易
      - 影响程度的轻重
      - 控制措施效果的好坏

1.3 ISMS方法

- 风险方法（续）
  - 风险评估（续）
    - 风险评估方法
      - 基线评估法：仅评估资产和控制措施
      - 详细评估法：风险五要素均评估
      - 组合评估法：基线评估法＋详细评估法

1.3 ISMS方法

- 风险方法（续）
  - 风险评估（续）
    - 风险评估工具
      - 综合性评估工具。
      - 安全性检查工具，如安全测试与评价（ST&E）和安全审计系统等；
      - 脆弱性检测工具，如漏洞扫描等；
      - 渗透性测试工具，如黑客工具等；
      - 辅助性评估工具，如入侵检测系统、资产表、威胁库、漏洞库、安全知识库等。

1.3 ISMS方法

- 风险方法（续）
  - 风险评估（续）
    - 风险评估的工作形式
      - 自评估：由机构内部（包括决策层、管理层和操作层）发起，以对内改进机构安全状态和对外展示机构安全状态的符合性和有效性为目的。
      - 检查评估：由机构外部（包括上级主管、检查机关和合作伙伴等）发起，以监督机构安全状态的符合性和有效性为目的。

1.3 ISMS方法

- 风险方法（续）
  - 风险处理
    - 选择和实施控制措施来减轻风险的过程。
    - 风险管理的主体，为缓解风险做出直接贡献。
    - 安全需求
      - 当前风险等级超出可接受风险等级的差值就是安全需求，需要采取相应的处理方式和控制措施来解决。
    - 风险处理的目的
      - 将当前风险等级降低到可接受程度。

1.3 ISMS方法

- 风险方法（续）
  - 风险处理（续）
    - 风险处理方式
      - 风险规避
      - 风险转移
      - 风险降低
      - 风险接受

1.3 ISMS方法

- 风险方法（续）
  - 风险处理（续）
    - 风险处理计划
      - 遵循的原则和策略
      - 选定的控制措施
      - 实现的优先顺序
      - 所需的资源和成本
      - 分配的责任和权力
      - 人员的沟通和培训
      - 实施的时机和进度
      - 过程的报告和监视
      - 绩效的测量和评价等

1.3 ISMS方法

- 风险方法（续）
  - 风险处理（续）
    - 残余风险
      - 风险处理实施之后仍然存在的风险。
      - 可能是原有风险的残存，也可能是新的风险的引入，还包括未识别的风险。
    - 残余风险的保留
      - 出于残余风险已减少到可接受程度或者机构目前尚没有足够的资源或能力进一步处理残余风险等原因。
      - 当事方和决策者应意识到残余风险的性质和程度，特别是对于尚未达到可接受程度的残余风险应设定保留期限和适当约束，因此，残余风险应被记录在案并受到监视和评审。

1.3 ISMS方法

- 风险方法（续）
  - 风险处理（续）
    - 风险处理过程
      - 首先，对风险评估阶段输出的风险评价结果，对照背景建立阶段确立的风险接受准则，判定哪些风险是可接受的，哪些是不可接受。
      - 然后，对于那些可接受的风险，只需进行必要的风险接受处理后，便可进入监视与评审阶段，以保持对其变化的注视；对于那些不可接受的风险，需要在风险规避、风险转移和风险降低中选择合适的处理方式。在许多情况下，一种处理方式不太可能是一个完整的解决方案，需要多种处理方式的组合。

1.3 ISMS方法

- 风险方法（续）
  - 风险处理（续）
    - 风险处理过程（续）
      - 在实施了所选处理方式之后，再次进行风险接受判断，即判断残余风险（residual risk）是否可接受。如果仍然不可接受，或者继续挖掘风险处理的潜力，以期风险的进一步缓解；或者重新回到背景建立阶段，以期通过调整背景因素来改变风险，并经过风险评估后为风险处理提供新的可能。

1.3 ISMS方法

- 风险方法（续）
  - 监视与评审
    - 风险管理的监查，为有效地管理风险提供保障。
    - 监视与评审途径
      - 持续监视所有风险要素、风险管理过程要素和风险管理过程整体状态的变化，检查这些要素的符合性和有效性，进而把握风险管理过程的整体状态。

1.3 ISMS方法

- 风险方法（续）
  - 沟通与咨询
    - 风险管理的通道，为顺畅地管理风险提供保障。
    - 沟通与咨询做法
      - 在适当的时候就风险要素、风险管理过程要素和风险管理过程整体在组织内部和外部方中进行沟通和咨询。
    - 沟通与咨询途径和作用
      - 通过畅通的交流和充分的沟通，达成相关人员就风险管理在认知上的相互理解和在行动上的协调一致；
      - 通过有效的培训和便捷的咨询，保证相关人员为参与风险管理具备适当的知识和技能。

1.3 ISMS方法

- 风险方法（续）
  - 风险管理过程要点
    - 第一轮风险管理周期的工作是开创性的，应该本着可持续发展的原则全面考虑，为今后的工作打好基础。
    - 风险管理过程是持续的、循序渐进的过程，不是一两轮就能解决全部风险，况且新的风险会不断出现。
    - 任何新的一轮风险管理周期的工作都应建立的前面各轮工作结果的基础上，是对现有风险管理的改进和完善。
    - 监视与评审和沟通与咨询至始至终贯穿于整个风险管理周期，是风险管理得以有效发挥和顺畅进行的保障。

1.3 ISMS方法

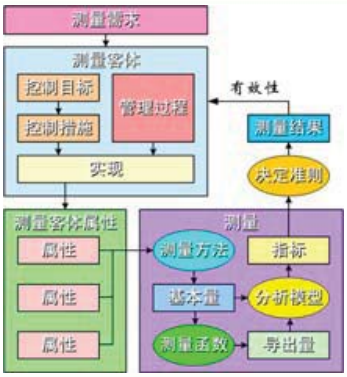
- 风险方法（续）
  - ISMS应采用风险方法，即信息安全风险管理。
  - 信息安全风险是ISMS的核心内容和基本途径。

1.3 ISMS方法

- 测量方法
  - 测量目的：为了比较或评价事物的某种属性（例如，信息系统的安全性、信息安全管理的有效性），需要对这种属性赋予量值。
  - 测量属于计量学的范畴，涉及到计量学中的一些基本概念和术语。
    - 量、值、量制、基本量、导出量、单位、单位制、测量、测量方法、测量程序、测量结果等。

1.3 ISMS方法

- 测量方法（续）
  - 信息安全测量是计量学在信息安全领域的应用。
  - 信息安全测量模型
    - 测量需求
    - 测量客体
    - 测量函数
    - 分析模型
    - 指标
    - 决定准则



第一部分 ISMS体系概念综述

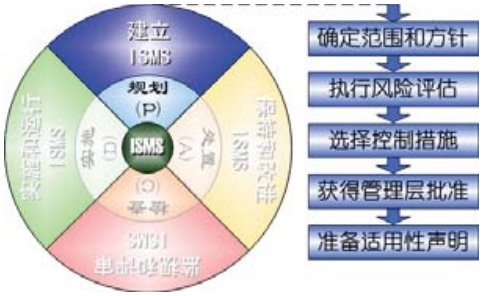
- 1.1 ISMS概念
- 1.2 ISMS定位
- 1.3 ISMS方法
- **1.4 ISMS过程**
- 1.5 ISMS内容
- 1.6 ISMS关键
- 1.7 ISMS全貌

1.4 ISMS过程

- ISMS的PDCA：建立、实施和运行、监视和评审、保持和改进。

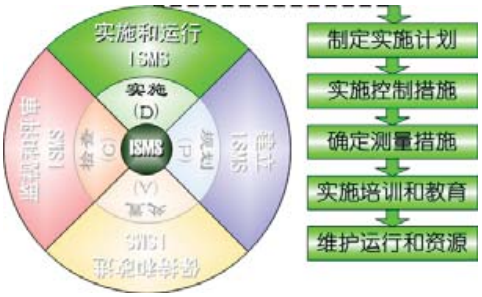
1.4 ISMS过程

- 建立阶段的活动



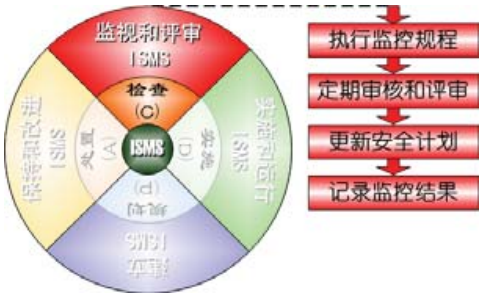
1.4 ISMS过程

- 实施和运行阶段的活动



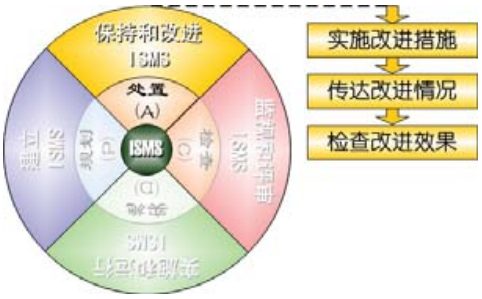
1.4 ISMS过程

- 监视和评审阶段的活动



1.4 ISMS过程

- 保持和改进阶段的活动



第一部分 ISMS体系概念综述

- 1.1 ISMS概念
- 1.2 ISMS定位
- 1.3 ISMS方法
- 1.4 ISMS过程
- **1.5 ISMS内容**
- 1.6 ISMS关键
- 1.7 ISMS全貌

1.5 ISMS内容

- ISMS控制域

1.5 ISMS内容

- 安全策略
  - 信息安全策略是ISMS的灵魂，它指导和规范信息安全管理的所有活动。
  - 信息安全策略具有层次结构，由高至低分为总体方针、管理制度、操作流程和执行记录四个层次，应按照适用对象（包括主体和客体）分别制定相应的安全策略。
  - 信息安全策略的管理包括策略文件的制定、审批、发布、宣贯和培训以及定期评审和变更记录。

1.5 ISMS内容

- 安全组织
  - 信息安全组织是ISMS的动力，它建立和执行信息安全策略。
  - 信息安全管理通常是跨部门的，涉及到一个组织的多个相关部门，因此需要建立能够统筹全局和协调关系的领导班子和工作班子，以及具有足够人力和技能的管理部门和执行部门。
  - 信息安全组织应与其他方面的组织管理协调和融合。

1.5 ISMS内容

- 资产管理
  - 信息资产包括类型
    - 有形资产：数据、软件、硬件、服务和人员等。
    - 无形资产：知识、信誉和品牌等。
  - 信息资产的价值
    - 获取价值：购置和维护资产时的成本。
    - 作用价值：资产对业务的重要程度，或者说，资产失效时对业务造成的损失。
  - 资产管理包括资产清单、资产使用和资产分级。

1.5 ISMS内容

- 人员安全
  - 人是信息安全管理中最活跃和最不确定的因素，既能够成为“最可靠防线”，也可能成为“最大威胁”。
  - 管理人力资源安全的目的就是通过一系列管理措施把人从潜在的“最大威胁”变为“最可靠防线”，形成“人力防火墙”。
  - 人力资源安全管理包括筛选、职责、素质、培训、奖罚和离岗等方面。

1.5 ISMS内容

- 物理安全
  - 信息、信息系统及其支撑环境的物理区域和设施设备应受到保护，包括区域安全和设备安全两方面。
  - 区域安全：防止对组织场所内信息资产的未授权物理访问、损坏和干扰。
  - 设备安全：保护设备（包括在组织之外使用的）免受物理的和环境的威胁。

1.5 ISMS内容

- 运行安全
  - 信息系统及其支撑环境的运行安全应得到保证和维持。
  - 运行安全涉及到操作规程、操作权限、变更管理、运行环境、外包服务、病毒防范、信息保护、移动代码、网络安全、运行监视等方面。

1.5 ISMS内容

- 访问控制
  - 对信息、信息系统及其支撑环境的访问应得到控制。
  - 访问控制涉及到控制策略、用户身份、用户口令、用户权限、用户职责、鉴别机制、访问机制、超时机制、在外办公等方面

1.5 ISMS内容

- 系统建设
  - 在信息系统的获取、开发和维护过程中，包括两个方面的安全建设：
    - 自身安全机制（内在安全性）：信息系统各子系统（包括网络系统、操作系统、数据库管理系统、中间件系统和应用系统等）自身具备的。
    - 专用安全系统（外加安全性）：物理隔离装置、防火墙、防病毒系统、入侵检测系统、漏洞扫描系统、补丁分发系统和终端管理系统等。
  - 两者相辅相成，共同形成纵深防御体系。

1.5 ISMS内容

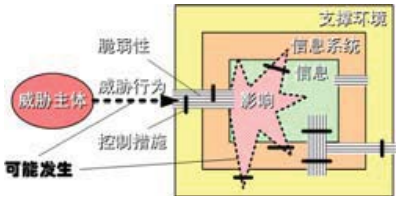
- 系统建设（续）
  - 建设过程包括需求分析、方案设计、实施计划、产品采购、功能开发、项目管理、工程监理、验收交付和后期维护等。

1.5 ISMS内容

- 事件管理
  - 三个基本概念
    - 信息安全风险（Information Security Risk）
    - 信息安全事态（Information Security Event）
    - 信息安全事件（Information Security Incident）

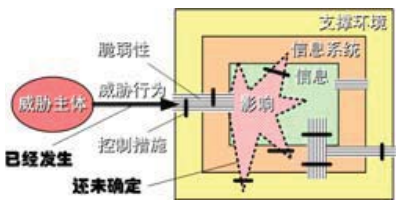
1.5 ISMS内容

- 事件管理（续）
  - 信息安全风险（Information Security Risk）
    - 威胁主体**可能**利用信息、信息系统或支撑环境的脆弱性，对信息、信息系统和支撑环境实施威胁行为，**可能**造成负面影响。



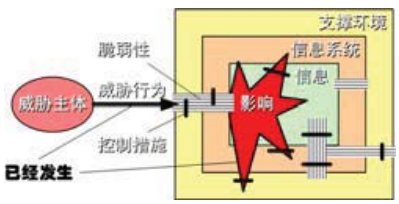
1.5 ISMS内容

- 事件管理（续）
  - 信息安全事态（Information Security Event）
    - 威胁主体**已经**利用信息、信息系统或支撑环境的脆弱性，对信息、信息系统和支撑环境实施威胁行为，**可能**造成负面影响。



1.5 ISMS内容

- 事件管理（续）
  - 信息安全事件（Information Security Incident）
    - 威胁主体**已经**利用信息、信息系统或支撑环境的脆弱性，对信息、信息系统和支撑环境实施威胁行为，**已经**造成负面影响。



1.5 ISMS内容

- 事件管理（续）
  - 信息安全风险、信息安全事态和信息安全事件的演变过程

1.5 ISMS内容

- 事件管理（续）
  - 安全不是绝对的
    - 任何安全防护措施都不能完全避免安全事件的发生。
    - 成本高于效益的安全措施也是没有意义的。
  - 安全总是动态的
    - 负面因素：安全风险层出不穷，安全事件各式各样。
    - 正面因素：安全技术日新月异，安全管理不断完善。
  - 管理是必然出路
    - 采用结构严谨、计划周全的管理方法，全程管理信息安全事件十分必要。
    - 信息安全事件管理是信息安全管理的重要组成部分。

1.5 ISMS内容

- 事件管理（续）
  - 总会有信息安全事件发生，往往是意料之外的，甚至是未知的。
  - 在发生信息安全事件时，有序、有力、有效地采取应对措施，稳定局面，降低负面影响并尽快恢复系统是至关重要的。

1.5 ISMS内容

- 事件管理（续）
  - 信息安全事件分类
    （Information Security Incident Categoriztion）
    - 起因角度：人为的（故意破坏、无意破坏）、客观的（自然灾害、技术故障）
    - 行为角度：恶意代码、网络攻击、信息破坏、有害内容、人身侵害、责任逃避、系统故障
    - 安全属性角度：保密性破坏、完整性破坏、可用性破坏、真实性破坏、抗抵赖性破坏、可核查性破坏、可靠性破坏、可控性破坏
    - 后果角度：财务损失、利益丧失、个人伤害、法规触犯、运行妨碍、声誉损害

1.5 ISMS内容

- 事件管理（续）
  - 信息安全事件分级
    （Information Security Incident Classification）
    - 依据
      - 信息系统的重要程度
      - 事件影响的严重程度
    - 目的：准确判断事件的严重性，从而做到适度响应，以避免
      - 响应不足：错过控制事态发展的最佳时机，使事件失控，导致本不该发生的更大损失；
      - 响应过度：不仅浪费资源，还会造成此事件本身更糟糕的影响。

1.5 ISMS内容

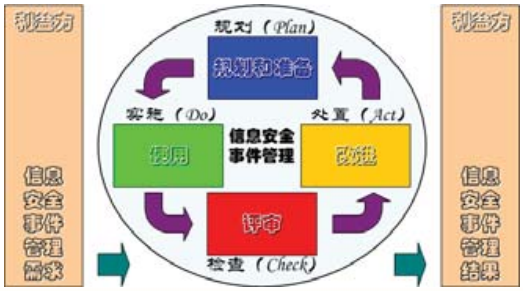
- 事件管理（续）
  - 信息安全事件分级（续）
    - GB/Z 20986-2007《信息安全技术 信息安全事件分类分级指南》
      - 综合信息系统的重要程度、系统损失和社会影响这三方面的因素
      - 从国家层面将信息安全事件划分为四级：
        - Ⅰ级：特别重大事件
        - Ⅱ级：重大事件
        - Ⅲ级：较大事件
        - Ⅳ级：一般事件

1.5 ISMS内容

- 事件管理（续）
  - 方法：采用一种结构严谨、计划周全的方法来全程管理信息安全事件。
  - 过程：事前做好规划和准备，事中及时发现、报告、评估和判别并有效抑制和取证，事后消除根源、恢复系统、总结经验和实施改进，以及不论事件是否发生均定期和/或应需评审和持续改进。
  - 活动：规划、准备、发现、报告、评估、判别、抑制、取证、根除、恢复、总结、评审和改进。

1.5 ISMS内容

- 事件管理（续）
  - 信息安全事件管理的PDCA



1.5 ISMS内容

- 事件管理（续）
  - 信息安全事件管理的PDCA
    - P阶段：规划和准备
      - 活动：规划、准备
    - D阶段：使用
      - 活动：发现、报告、评估、判别、抑制、取证、根除、恢复
    - C阶段：评审
      - 活动：总结、评审
    - A阶段：改进
      - 活动：改进

1.5 ISMS内容

- 业务持续
  - 随着信息系统在业务系统中发挥着越来越重要的作用，并已成为不可或缺的组成部分，信息系统的持续性直接关系着业务的持续性。
  - 保障信息系统持续性已成为保障业务持续性的必要条件，是业务持续性计划的重要内容之一。
  - 应急预案、应急培训、容灾备份、系统恢复是保证信息系统持续性的重要环节。

1.5 ISMS内容

- 合规管理
  - 合规性是信息安全管理的重要方面，体现在遵守法律法规、符合技术标准、信守合同规定和遵循安全策略等方面，应采取措施加以管理。

第一部分 ISMS体系概念综述

- 1.1 ISMS概念
- 1.2 ISMS定位
- 1.3 ISMS方法
- 1.4 ISMS过程
- 1.5 ISMS内容
- **1.6 ISMS关键**
- 1.7 ISMS全貌

1.6 ISMS关键

- ISMS的关键成功因素
  - 方向因素——对业务目标支持
  - 驱动因素——高管承诺和支持
  - 资源因素——资源提供和保障
  - 能力因素——专业队伍和技能
  - 意识因素——全员意识和参与
  - 环境因素——与组织环境融合
  - 风险因素——与安全风险相适
  - 测评因素——结果测量和评价

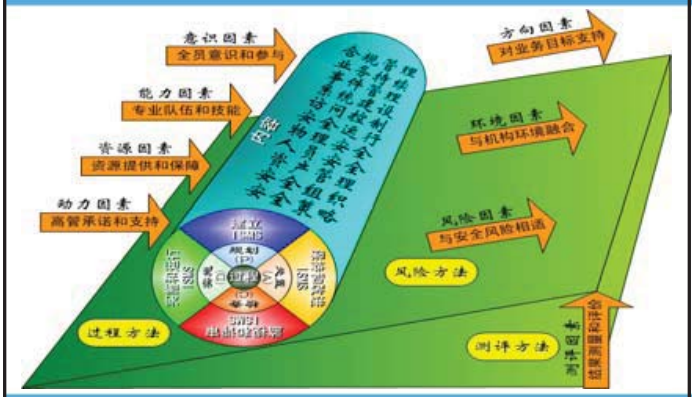
第一部分 ISMS体系概念综述

- 1.1 ISMS概念
- 1.2 ISMS定位
- 1.3 ISMS方法
- 1.4 ISMS过程
- 1.5 ISMS内容
- 1.6 ISMS关键
- **1.7 ISMS全貌**

1.7 ISMS全貌

- 方法
  - 过程方法、风险方法、测量方法
- 内容
  - 安全策略、安全组织、资产管理、人员安全、物理安全、运行安全、访问控制、系统建设、事件管理、业务持续、合规管理
- 关键
  - 对业务目标支持、高管承诺和支持、资源提供和保障、专业队伍和技能、全员意识和参与、与组织环境融合、与安全风险相适、结果测量和评价

1.7 ISMS全貌



内容纲要

- 第一部分 ISMS体系概念综述
- **第二部分 ISMS国际标准介绍**
- 第三部分 ISMS国家标准解读
  - GB/T 22080-2008《信息技术 安全技术 信息安全管理体系 要求》
  - GB/T 22081-2008《信息技术 安全技术 信息安全管理实用规则》
  - GB/T 20984-2007《信息安全技术 信息安全风险评估规范》
  - GB/T 20988-2007《信息安全技术 信息系统灾难恢复规范》
  - GB/Z 20985-2007《信息技术 安全技术 信息安全事件管理指南》

第二部分 ISMS国际标准介绍

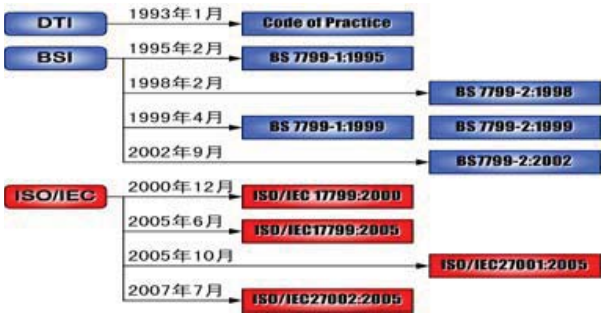
- 2.1 历史沿革
- 2.2 国际标准
- 2.3 他国标准

第二部分 ISMS国际标准介绍

- **2.1 历史沿革**
- 2.2 国际标准
- 2.3 他国标准

2.1 历史沿革

- ISMS标准的发展历程



第二部分 ISMS国际标准介绍

- 2.1 历史沿革
- **2.2 国际标准**
- 2.3 他国标准

2.2 国际标准

- ISO/IEC JTC1 SC27
  - 2005年4月正式启动了ISMS的标准化项目，即ISO/IEC 27000系列标准，或称ISMS标准族。
  - ISMS标准族包括体系、行业和领域三大类，标准编号分别从27000、27010和27030开始。

2.2 国际标准

- ISO/IEC JTC1 SC27（续）
  - 体系类

2.2 国际标准

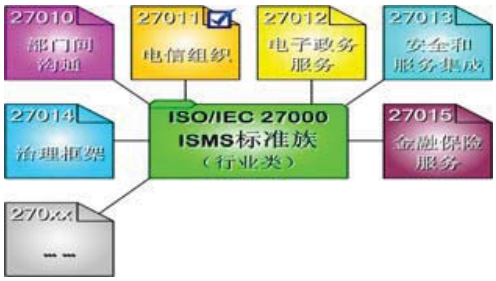
- ISO/IEC JTC1 SC27（续）
  - 体系类（续）
    - ISO/IEC 27000:2009《信息安全管理体系 — 概述和词汇》
    - ISO/IEC 27001:2005《信息安全管理体系 — 要求》
    - ISO/IEC 27002:2005《信息安全管理实用规则》
    - ISO/IEC FCD 27003《信息安全管理体系实施指南》
    - ISO/IEC FDIS 27004《信息安全管理 — 测量》
    - ISO/IEC 27005:2008《信息安全风险管理》

2.2 国际标准

- ISO/IEC JTC1 SC27（续）
  - 体系类（续）
    - ISO/IEC 27006:2007《信息安全管理体系审核认证机构的要求》
    - ISO/IEC 1st CD 27007《信息安全管理体系审核指南》
    - ISO/IEC 2nd WD 27008《信息安全管理体系控制措施审核员指南》

2.2 国际标准

- ISO/IEC JTC1 SC27（续）
  - 行业类



2.2 国际标准

- ISO/IEC JTC1 SC27（续）
  - 行业类（续）
    - ISO/IEC 1st WD 27010《部门间沟通的信息安全管理》
    - ISO/IEC 27011:2008 | ITU-T X.1051《基于ISO/IEC 27002的电信组织信息安全管理指南》
    - ISO/IEC Pre WD 27012《电子政务服务的ISM指南》
    - ISO/IEC Pre WD 27013《ISO/IEC 20000-1和ISO/IEC 27001 集成实施指南》
    - ISO/IEC 2nd WD 27014《信息安全治理框架》
    - ISO/IEC WD 27015《金融和保险服务的信息安全管理要求和指南》

2.2 国际标准

- ISO/IEC JTC1 SC27（续）
  - 领域类

2.2 国际标准

- ISO/IEC JTC1 SC27（续）
  - 领域类（续）
    - ISO/IEC 1st CD 27031《业务持续性的ICT就绪指南》
    - ISO/IEC 3nd WD 27032《网际安全指南》
    - ISO/IEC 27033《网络安全》
    - ISO/IEC 27034《应用安全》
    - ISO/IEC 2nd CD 27035《信息安全事件管理》
    - ISO/IEC 1st WD 27036《外包安全指南》
    - ISO/IEC 1st WD 27037《数字证据的标识、收集和/或保存》

第二部分 ISMS国际标准介绍

- 2.1 历史沿革
- 2.2 国际标准
- **2.3 他国标准**

2.3 他国标准

- 英国
- 美国
- 加拿大
- 澳大利亚和新西兰
- 德国

2.3 他国标准

- 英国
  - 英国标准协会（BSI）于1995年2月首先提出了ISMS的概念，并制定了世界上第一个ISMS标准，即BS 7799-1:1995《信息安全管理实用规则》（Code of Practice for Information Security Management）。
  - 为满足第三方认证的需求，BSI于1998年2月又制定了ISMS认证标准BS 7799-2:1998《信息安全管理体系规范》（Specification for Information Security Management System）。

2.3 他国标准

- 英国（续）
  - 鉴于信息技术在网络和通讯领域应用的迅速发展，BSI于1999年4月对上述两个标准进行了修订，推出了1999版，即BS 7799-1:1999和BS 7799-2:1999。
  - 2002年BSI对BS 7799-2:1999进行了重大改版，引入了国际上通行的管理方法和模式（即过程方法和PDCA模型），同时与ISO 9001:2000《质量管理体系 — 要求》（Quality management systems – Requirements）保持高度一致，并于同年9月5日正式发布了BS7799-2:2002。

2.3 他国标准

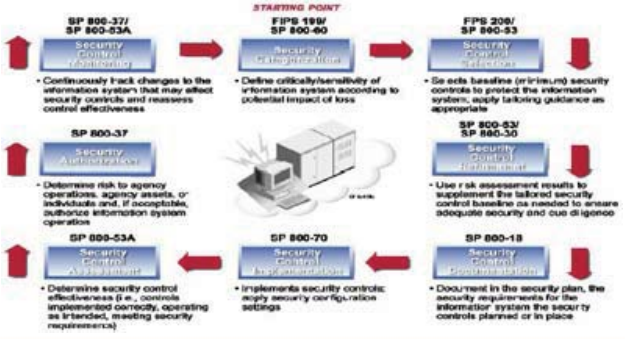
- 英国（续）
  - 国际标准ISO/IEC 17799（即现在的ISO/IEC 27002）和ISO/IEC 27001就是分别源自于BS 7799-1:1999和BS 7799-2:2002。

2.3 他国标准

- 美国
  - 美国政府于2002年12月通过了《联邦信息安全管理法案》（Federal Information Security Management Act，FISMA），随后为此启动了FISMA实施项目。
  - 该项目的第一阶段（2003年至2008年）就是为有效满足FISMA的规定开发所需的信息安全标准和指南，即美国联邦信息处理标准（FIPS）和美国国家标准与技术研究所（NIST）的计算机安全特别出版物SP 800系列。

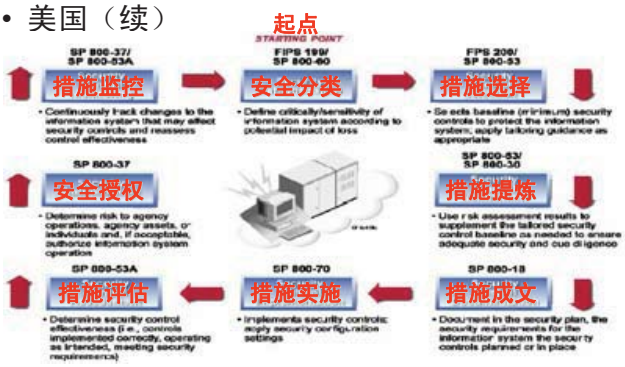
2.3 他国标准

- 美国（续）



2.3 他国标准

- 美国（续）



2.3 他国标准

- 美国（续）
  - 安全分类（Security Categorization）
    - 根据损失的潜在影响定义信息系统的关键性/敏感性。
    - FIPS 199《联邦信息和信息系统的安全类别标准》（Standards for Security Categorization of Federal Information and Information Systems）
    - SP 800-60《信息和信息系统类型到安全类别的映射指南》（Guide for Mapping Types of Information and Information Systems to Security Categories）

2.3 他国标准

- 美国（续）
  - 安全控制措施选择（Security Control Selection）
    - 选择基线（最小）安全控制措施保护信息系统；适当时使用剪裁指南。
    - FIPS 200《联邦信息和信息系统的最小安全要求》（Minimum Security Requirements for Federal Information and Information Systems）
    - SP 800-53《推荐给联邦信息系统的安全控制措施》（Recommended Security Controls for Federal Information Systems）

2.3 他国标准

- 美国（续）
  - 安全控制措施提炼（Security Control Refinement）
    - 需要时使用风险评估结果补充剪裁的安全控制基线，以确保足够的安全。
    - SP 800-53《推荐给联邦信息系统的安全控制措施》（Recommended Security Controls for Federal Information Systems）
    - SP 800-30《信息技术系统的风险管理指南》（Risk Management Guide for Information Technology Systems）

2.3 他国标准

- 美国（续）
  - 安全控制措施文件化（Security Control Documentation）
    - 文件化安全计划、信息系统的安全要求、计划的或现有的安全控制措施。
    - SP 800-18《联邦信息系统安全计划开发指南》（Guide for Developing Security Plans for Federal Information Systems）

2.3 他国标准

- 美国（续）
  - 安全控制措施实施（Security Control Implementation）
    - 实施安全控制措施；应用安全配置设置。
    - SP 800-70 《IT产品的安全配置检查表计划 — 检查表用户和开发者指南》（Security Configuration Checklists Program for IT Products – Guidance for Checklists Users and Developers）

2.3 他国标准

- 美国（续）
  - 安全控制措施评估（Security Control Assessment）
    - 确定安全控制有效性（即，正确地实施、按计划运行、满足安全要求的控制措施）。
    - SP 800-53A《联邦信息系统安全控制措施的评估指南》（Guide for Assessing the Security Controls in Federal Information Systems）

2.3 他国标准

- 美国（续）
  - 安全授权（Security Authorization）
    - 确定对机构运作、机构资产或个人的风险，如果可接收则授权信息系统运行。
    - SP 800-37《联邦信息系统安全认证认可指南》（Guide for the Security Certification and Accreditation of Federal Information Systems）

2.3 他国标准

- 美国（续）
  - 安全控制措施监控（Security Control Monitoring）
    - 持续跟踪可能影响安全控制措施的信息系统变化，并评估控制措施的有效性。
    - SP 800-37《联邦信息系统安全认证认可指南》（Guide for the Security Certification and Accreditation of Federal Information Systems）
    - SP 800-53A《联邦信息系统安全控制措施的评估指南》（Guide for Assessing the Security Controls in Federal Information Systems）

2.3 他国标准

- 加拿大
  - 加拿大通信安全机构（CSE）
    - MG-1:1996《网络安全、分析和实施》（Network Security, Analysis and Implementation）
    - MG-2:1996《信息技术系统安全风险管理指南》（A Guide to Security Risk Management for Information Technology Systems）
    - MG-3:1996《信息技术系统风险评估和安全措施选择指南》（A Guide to Risk Assessment and Safeguard Selection for Information Technology Systems）

2.3 他国标准

- 加拿大（续）
  - 加拿大通信安全机构（续）
    - MG-4:1996《信息技术系统认证认可指南》（A Guide to Certification and Accreditation for Information Technology Systems）
    - MG-9:1998《加拿大信息技术安全手册》（Canadian Handbook on Information Technology Security）
    - MG-11b《威胁与风险评估一般性工作声明》（Generic Statement Of Work For Threat and Risk Assessments）
    - CSE ITSG-04:1999《威胁与风险评估工作指南》（Threat and Risk Assessment Working Guide）

2.3 他国标准

- 澳大利亚和新西兰
  - AS/NZS 4360:1999《风险管理》（Risk Management）
- 德国
  - 德国联邦信息安全办公室（BSI）
    - 《IT基线保护手册》（IT Baseline Protection Manual），2004

内容纲要

- 第一部分 ISMS体系概念综述
- 第二部分 ISMS国际标准介绍
- **第三部分 ISMS国家标准解读**
  - GB/T 22080-2008《信息技术　安全技术　信息安全管理体系 要求》
  - GB/T 22081-2008《信息技术　安全技术　信息安全管理实用规则》
  - GB/T 20984-2007《信息安全技术　信息安全风险评估规范》
  - GB/T 20988-2007《信息安全技术　信息系统灾难恢复规范》
  - GB/Z 20985-2007《信息技术　安全技术　信息安全事件管理指南》

第三部分 ISMS国家标准解读

- 3.1 国家标准化组织
- 3.2 正式发布的国家标准
- 3.3 报批中的国家标准
- 3.4 标准解读
  - GB/T 22080-2008《信息技术　安全技术　信息安全管理体系 要求》
  - GB/T 22081-2008《信息技术　安全技术　信息安全管理实用规则》
  - GB/T 20984-2007《信息安全技术　信息安全风险评估规范》
  - GB/T 20988-2007《信息安全技术　信息系统灾难恢复规范》
  - GB/Z 20985-2007《信息技术　安全技术　信息安全事件管理指南》

第三部分 ISMS国家标准解读

- **3.1 国家标准化组织**
- 3.2 正式发布的国家标准
- 3.3 报批中的国家标准
- 3.4 标准解读
  - GB/T 22080-2008《信息技术　安全技术　信息安全管理体系 要求》
  - GB/T 22081-2008《信息技术　安全技术　信息安全管理实用规则》
  - GB/T 20984-2007《信息安全技术　信息安全风险评估规范》
  - GB/T 20988-2007《信息安全技术　信息系统灾难恢复规范》
  - GB/Z 20985-2007《信息技术　安全技术　信息安全事件管理指南》

3.1 国家标准化组织

- 全国信息安全标准化技术委员会（TC260）于2002年4月成立之初，便设立了信息安全管理标准工作组（WG7），专门负责信息安全管理领域的国家标准研究与制定工作。
- 多年来，WG7工作组陆续开展了多项信息安全管理基础标准和重要标准的研究和制定工作，同时也组织了对国际上重点的信息安全管理相关标准的跟踪研究和转标工作。

第三部分 ISMS国家标准解读

- 3.1 国家标准化组织
- **3.2 正式发布的国家标准**
- 3.3 报批中的国家标准
- 3.4 标准解读
  - GB/T 22080-2008《信息技术　安全技术　信息安全管理体系 要求》
  - GB/T 22081-2008《信息技术　安全技术　信息安全管理实用规则》
  - GB/T 20984-2007《信息安全技术　信息安全风险评估规范》
  - GB/T 20988-2007《信息安全技术　信息系统灾难恢复规范》
  - GB/Z 20985-2007《信息技术　安全技术　信息安全事件管理指南》

3.2 正式发布的国家标准

- GB/T 19716-2005《信息技术　信息安全管理实用规则》（修改采用国际标准ISO/IEC 17799:2000）
- GB/T 19715.1-2005《信息技术　信息技术安全管理指南　第1部分：信息技术安全概念和模型》（等同采用ISO/IEC TR 13335-1:1996）
- GB/T 19715.2-2005《信息技术　信息技术安全管理指南　第2部分：管理和规划信息技术安全》（等同采用ISO/IEC TR 13335-2:1997）

3.2 正式发布的国家标准

- GB/T 20282-2006《信息安全技术　信息系统安全工程管理要求》（自主研制）
- GB/T 20269-2006《信息安全技术　信息系统安全管理要求》（自主研制）
- GB/T 20984-2007《信息安全技术　信息安全风险评估规范》（自主研制）
- GB/Z 20985-2007《信息技术　安全技术　信息安全事件管理指南》（修改采用ISO/IEC TR 18044:2004）

3.2 正式发布的国家标准

- GB/Z 20986-2007《信息安全技术　信息安全事件分类分级指南》（自主研制）
- GB/T 20988-2007《信息安全技术　信息系统灾难恢复规范》（自主研制）
- GB/T 22080-2008《信息技术　安全技术　信息安全管理体系 要求》（等同采用ISO/IEC 27001:2005）
- GB/T 22081-2008《信息技术　安全技术　信息安全管理实用规则》（等同采用ISO/IEC 27002:2005）

第三部分 ISMS国家标准解读

- 3.1 国家标准化组织
- 3.2 正式发布的国家标准
- **3.3 报批中的国家标准**
- 3.4 标准解读
  - GB/T 22080-2008《信息技术　安全技术　信息安全管理体系 要求》
  - GB/T 22081-2008《信息技术　安全技术　信息安全管理实用规则》
  - GB/T 20984-2007《信息安全技术　信息安全风险评估规范》
  - GB/T 20988-2007《信息安全技术　信息系统灾难恢复规范》
  - GB/Z 20985-2007《信息技术　安全技术　信息安全事件管理指南》

3.3 报批中的国家标准

- GB/T xxxxx-xxxx《信息技术　安全技术　信息安全管理体系审核认证机构的要求》（等同采用ISO/IEC 27006:2007）（TC260与全国认证认可标准化技术委员会（TC261）联合编制）
- GB/Z xxxxx-xxxx《 信息安全技术　信息安全风险管理指南》（自主研制）
- GB/T xxxxx-xxxx《信息安全技术　信息安全应急响应计划规范》（自主研制）

第三部分 ISMS国家标准解读

- 3.1 国家标准化组织
- 3.2 正式发布的国家标准
- 3.3 报批中的国家标准
- **3.4 标准解读**
  - **GB/T 22080-2008《信息技术　安全技术　信息安全管理体系 要求》**
  - GB/T 22081-2008《信息技术　安全技术　信息安全管理实用规则》
  - GB/T 20984-2007《信息安全技术　信息安全风险评估规范》
  - GB/T 20988-2007《信息安全技术　信息系统灾难恢复规范》
  - GB/Z 20985-2007《信息技术　安全技术　信息安全事件管理指南》

GB/T 22080-2008

- 标准名称
  - 中文：信息技术　安全技术　信息安全管理体系 要求
  - 英文：Information technology – Security techniques – Information security management systems – Requirements
- 标准号：GB/T 22080-2008
- 中标分类：L80
- 采标情况：ISO/IEC 27001:2005，IDT

GB/T 22080-2008

- 发布日期：2008-6-19
- 实施日期：2008-11-1
- 发布单位
  - 中华人民共和国国家质量监督检验检疫总局
  - 中国国家标准化管理委员会

GB/T 22080-2008

- 标准简介
  - 该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信息安全管理体系（ISMS）规定了要求。它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。该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）。

GB/T 22080-2008

- 标准结构
  - 前言
  - 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

GB/T 22080-2008

- 标准结构（续）
  - 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） GB/T 9001-2000, GB/T 24001-2004 和本标准之间的对照
  - 参考文献

GB/T 22080-2008

- 前言
  - [给出该标准编制和管理相关的信息]
  - 该等同采用ISO/IEC 27001:2005《信息技术 — 安全技术 — 信息安全管理体系 — 要求》。

GB/T 22080-2008

- 引言
  - 0.1 总则
    - 标准用途：
      - 提供建立、实施、运行、监视、评审、保持和改进信息安全管理体系（ISMS）的模型。
      - 被组织的内部和外部相关方用于一致性评估。
    - 适用对象：组织。
    - ISMS定位：战略决策。
    - 影响因素：业务需求、安全要求、管理过程、规模和结构。
    - 实施策略：考虑影响因素的变化，按照实际需要实施ISMS

GB/T 22080-2008

- 引言（续）
  - 0.2 过程方法
    - 应用背景：为使组织有效运作，需要识别和管理众多相互关联的活动。
    - 过程定义：通过使用资源和管理，将输入转化为输出的活动。
    - 过程关系：通常，一个过程的输出直接形成下一个过程的输入。
    - 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。

GB/T 22080-2008

- 引言（续）
  - 0.2 过程方法（续）
    - 重要方面
      - 理解组织的信息安全要求和建立信息安全方针与目标的需要；
      - 从组织整体业务风险的角度，实施和运行控制措施，以管理组织的信息安全风险；
      - 监视和评审ISMS的执行情况和有效性；
      - 基于客观测量的持续改进。

GB/T 22080-2008

- 引言（续）
  - 0.2 过程方法（续）
    - 过程模型：采用PDCA模型。

GB/T 22080-2008

- 引言（续）
  - 0.2 过程方法（续）
    - 安全原则
      - 《OECD信息系统和网络安全指南：发展安全文化》（2002版）中所设置的原则：意识、责任、响应、道德规范、民主、风险评估、安全设计与实施、安全管理和再评估。
      - 采用PDCA模型反映了这些原则。
      - 为实施风险评估、安全设计与实施、安全管理和再评估的原则提供了一个强健的模型。

GB/T 22080-2008

- 引言（续）
  - 0.3 与其他管理体系的兼容性
    - 兼容标准：与GB/T 9001-2000和GB/T 24001-2004相结合。
    - 兼容目的：支持与相关管理标准一致的、整合的实施和运行。
    - 标准对照：参见附录C的表C.1。

GB/T 22080-2008

- 1 范围
  - 1.1 总则
    - 适用对象：所有类型的组织（例如，商业企业、政府机构、非赢利组织）。
    - 两类要求
      - 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信息安全管理体系（ISMS）规定了要求。
      - 为适应不同组织或其部门的需要而定制的安全控制措施规定了实施要求。

GB/T 22080-2008

- 1 范围（续）
  - 1.1 总则（续）
    - 设计原则：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。
    - 相关注释
      - 该标准中的“业务”一词应广义的解释为关系一个组织生存的核心活动。
      - GB/T 22081-2008提供了设计控制措施时可使用的实施指南。

GB/T 22080-2008

- 1 范围（续）
  - 1.2 应用
    - 应用范围：该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。
    - 符合性准则
      - 组织声称符合该标准时，对于第4章、第5章、第6章、第7章和第8章的要求不能删减。
      - 为了满足风险接受准则必要的进行的任何控制措施的删减，必须证明是合理的，且需要提供证据证明相关风险已被负责人员接受。
      - 除非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，否则不能声称符合该标准。

GB/T 22080-2008

- 1 范围（续）
  - 1.2 应用（续）
    - 相关注释：如果一个组织已经有一个运转着的业务过程管理体系（例如，与GB/T19001-2000或者GB/T 24001-2004相关的），那么在大多数情况下，更可取的是在这个现有的管理体系内满足该标准的要求。

GB/T 22080-2008

- 2 规范性引用文件
  - GB/T 22081-2008《信息技术 安全技术 信息安全管理实用规则》（ISO/IEC27002:2005，IDT）
    - 为在组织内启动、实施、维护和改进信息安全管理，以达到普遍接受的信息安全管理目标提供一般原则和通用指南。
    - 给出了为达到分布在11个控制域中的39项控制目标而建议的133项控制措施的实施指南和相关信息。
  - 该标准的规范性附录A中的控制目标和控制措施直接源自GB/T 22081-2008，并在编目上与其第5章至15章保持一致。

GB/T 22080-2008

- 3 术语和定义
  - 3.1 资产 asset
  - 3.2 可用性 availability
  - 3.3 保密性 confidentiality
  - 3.4 信息安全 information security
  - 3.5 信息安全事态 information security event
  - 3.6 信息安全事件 information security incident
  - 3.7 信息安全管理体系（ISMS） information security management system (ISMS)
  - 3.8 完整性 integrity

GB/T 22080-2008

- 3 术语和定义（续）
  - 3.9 残余风险 residual risk
  - 3.10 风险接受 risk acceptance
  - 3.11 风险分析 risk analysis
  - 3.12 风险评估 risk assessment
  - 3.13 风险评价 risk evaluation
  - 3.14 风险管理 risk management
  - 3.15 风险处置 risk treatment
  - 3.16 适用性声明 statement of applicability

GB/T 22080-2008

- 4 信息安全管理体系（ISMS）
  - 4.1 总要求
    - 在组织的整体业务活动中且在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；
    - 管理过程基于PDCA模型。

GB/T 22080-2008

- 4 信息安全管理体系（续）
  - 4.2 建立和管理ISMS
    - 4.2.1 建立ISMS
      - 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）

GB/T 22080-2008

- 4 信息安全管理体系（续）
  - 4.2 建立和管理ISMS / 4.2.2 实施和运行ISMS（续）
    - a) 制定风险处置计划
    - b) 实施风险处置计划
    - c) 实施选择的控制措施
    - d) 确定控制措施有效性的测量方法
    - e) 实施培训和意识教育计划
    - f) 管理ISMS的运行
    - g) 管理ISMS的资源
    - h) 实施检测和响应规程

GB/T 22080-2008

- 4 信息安全管理体系（续）
  - 4.2 建立和管理ISMS（续）
    - 4.2.3 监视和评审ISMS
      - a) 执行监视与评审规程
      - b) 进行ISMS有效性的定期评审
      - c) 测量控制措施的有效性
      - d) 定期进行风险评估的评审
      - e) 定期实施ISMS内部审核
      - f) 定期进行ISMS管理评审
      - g) 根据监视和评审结果更新安全计划
      - h) 记录可能影响ISMS有效性的措施和事态

GB/T 22080-2008

- 4 信息安全管理体系（ISMS）
  - 4.2 建立和管理ISMS
    - 4.2.4 保持和改进ISMS
      - a) 实施已识别的ISMS改进
      - b) 采取合适的纠正和预防措施
      - c) 沟通措施和改进情况
      - d) 确保改进达到了预期目标

GB/T 22080-2008

- 4 信息安全管理体系（ISMS）
  - 4.3 文件要求
    - 4.3.1 总则
      - 文件是指信息及其承载媒体。文件可以是程序文件、规范文件、记录、报告等，文件媒体包括纸张、磁盘、磁带或其他电子媒体等。
      - 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。

GB/T 22080-2008

- 4 信息安全管理体系（ISMS）
  - 4.3 文件要求
    - 4.3.1 总则（续）
      - ISMS文件内容
        - a) 形成文件的ISMS方针和目标
        - b) ISMS的范围
        - c) 支持ISMS的规程和控制措施
        - d) 风险评估方法的描述
        - e) 风险评估报告
        - f) 风险处置计划

GB/T 22080-2008

- 4 信息安全管理体系（ISMS）
  - 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，以便有效控制文件。
    - 文件控制措施
      - 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) 确保在使用处可获得适用文件的相关版本；
      - e) 确保文件保持清晰、易于识别；

GB/T 22080-2008

- 4 信息安全管理体系（ISMS）
  - 4.3.2 文件控制（续）
    - 文件控制措施（续）
      - f) 确保文件对需要的人员可用，并依照文件适用的类别规程进行传输、贮存和最终销毁；
      - g) 确保外来文件得到识别；
      - 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) 若因任何目的而保留作废文件时，对这些文件进行适当的标识。

GB/T 22080-2008

- 4 信息安全管理体系（ISMS）
  - 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。

GB/T 22080-2008

- 4 信息安全管理体系（ISMS）
  - 4.3.3 记录控制（续）
    - 记录类型
      - 4.2中列出的过程执行记录
      - 所有发生的与ISMS有关的重大安全事件的记录。
    - 记录示例
      - 访客登记薄
      - 审核报告
      - 访问授权单
      - 信息安全事态/事件报告单

GB/T 22080-2008

- 5 管理职责
  - 5.1 管理承诺
    - 管理者应通过相应活动，对建立、实施、运行、监视、评审、保持和改进ISMS的承诺提供证据。
    - 活动证据：方针、目标和计划、角色和职责、传达、资源、准则、内部审核、管理评审

GB/T 22080-2008

- 5 管理职责（续）
  - 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。
      - 资源用途：ISMS全过程、支持业务、合规、控制措施、评审、改进

GB/T 22080-2008

- 5 管理职责（续）
  - 5.2 资源管理
    - 5.2.2 培训、意识和能力
      - 组织应通过适当方式，确保所有被赋予ISMS职责的人员具有执行所要求任务的能力。
      - 组织还应确保所有相关人员意识到他们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。

GB/T 22080-2008

- 6 ISMS内部审核
  - 审核周期
    - 组织应按照计划的时间间隔进行ISMS内部审核。
    - 一般不超过一年。
  - 审核目的
    - 确定组织的ISMS控制目标、控制措施、过程和规程是否：
      - a) 符合该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。

GB/T 22080-2008

- 6 ISMS内部审核（续）
  - 审核方案
    - 制定时的考虑因素：
      - 拟审核的过程与区域的状况和重要性；
      - 以往审核的结果。
    - 涵盖内容：审核的准则、范围、频次和方法。
  - 审核员要求
    - 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。

GB/T 22080-2008

- 6 ISMS内部审核（续）
  - 审核职责
    - 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。
  - 审核响应
    - 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）。
  - 相关注释
    - GB/T 19011-2003也可为实施ISMS内部审核提供有用的指导。

GB/T 22080-2008

- 7 ISMS的管理评审
  - 7.1 总则
    - 评审周期：至少每年一次。
    - 评审目的：确保组织的ISMS持续的适宜性、充分性和有效性。
    - 评审内容：评估组织的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。
    - 评审结果：应清晰地形成文件，记录应加以保持（见4.3.3）。

GB/T 22080-2008

- 7 ISMS的管理评审（续）
  - 7.2 评审输入
    - a) ISMS审核和评审的结果；
    - b) 相关方的反馈；
    - c) 改进ISMS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。

GB/T 22080-2008

- 7 ISMS的管理评审（续）
  - 7.3 评审输出
    - a) ISMS有效性的改进。
    - b) 风险评估和风险处置计划的更新。
    - c) 必要时修改信息安全的规程和控制措施，以响应可能影响ISMS的内部或外部变更：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) 法律法规要求；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) 控制措施有效性测量方法的改进。

GB/T 22080-2008

- 8 ISMS改进
  - 8.1 持续改进
    - 持续改进ISMS有效性的途径
      - 信息安全方针
      - 信息安全目标
      - 审核结果
      - 对监视事态的分析
      - 纠正和预防措施
      - 管理评审（见第7章）

GB/T 22080-2008

- 8 ISMS改进（续）
  - 8.2 纠正措施
    - 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
      - 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。

GB/T 22080-2008

- 8 ISMS改进（续）
  - 8.3 预防措施
    - 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
      - 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。

GB/T 22080-2008

- 附录A（规范性附录） 控制目标和控制措施
  - 表A-1所列的控制目标和控制措施是直接源自并与GB/T 22081-2008（ISO/IEC 27002:2005, IDT）第5到15章一致。
  - 表A.1中的清单并不详尽，一个组织可能考虑另外必要的控制目标和控制措施。
  - 在这些表中选择控制目标和控制措施是条款4.2.1规定的ISMS过程的一部分。
  - GB/T 22081-2008（ISO/IEC 27002:2005, IDT）第5至15章提供了最佳实践的实施建议和指南，以支持A.5到A.15列出的控制措施。

GB/T 22080-2008

- 附录B （资料性附录） OECD原则和本标准
  - 在OECD信息系统和网络安全指南中给出的原则适用于治理信息系统和网络安全的所有方针和操作层。
    - 意识、责任、响应、道德规范、民主、风险评估、安全设计与实施、安全管理和再评估
  - 该标准提供信息安全管理体系框架，通过使用PDCA模型以及第4章、第5章、第6章和第8章所述的过程，来实现的某些OECD原则。
    - 意识、责任、响应、风险评估、安全设计与实施、安全管理、再评估

GB/T 22080-2008

- 附录C （资料性附录） GB/T 9001-2000, GB/T 24001-2004 和本标准之间的对照
  - GB/T 9001-2000《质量管理体系 — 要求》
  - GB/T 24001-2004《环境管理体系要求及使用指南》
  - 三个标准的内容架构基本一致。

第三部分 ISMS国家标准解读

- 3.1 国家标准化组织
- 3.2 正式发布的国家标准
- 3.3 报批中的国家标准
- **3.4 标准解读**
  - GB/T 22080-2008《信息技术 安全技术 信息安全管理体系 要求》
  - **GB/T 22081-2008《信息技术 安全技术 信息安全管理实用规则》**
  - GB/T 20984-2007《信息安全技术 信息安全风险评估规范》
  - GB/T 20988-2007《信息安全技术 信息系统灾难恢复规范》
  - GB/Z 20985-2007《信息技术 安全技术 信息安全事件管理指南》

GB/T 22081-2008

- 标准名称
  - 中文：信息技术 安全技术 信息安全管理实用规则
  - 英文： Information technology – Security techniques – Code of practice for information security management
- 标准号：GB/T 22081-2008
- 中标分类：L80
- 采标情况：ISO/IEC 27002:2005，IDT

GB/T 22081-2008

- 发布日期：2008-6-19
- 实施日期：2008-11-1
- 发布单位
  - 中华人民共和国国家质量监督检验检疫总局
  - 中国国家标准化管理委员会

GB/T 22081-2008

- 标准简介
  - 该标准给出了一个组织启动、实施、保持和改进信息安全管理的指南和一般原则。该标准列出的目标为通常所接受的信息安全管理的目的提供了一般性指导。

GB/T 22081-2008

- 标准结构
  - 前言
  - 引言
  - 1 范围
  - 2 术语和定义
  - 3 本标准的结构
  - 4 风险评估和处理
  - 5 安全方针
  - 6 信息安全组织
  - 7 资产管理

GB/T 22081-2008

- 标准结构（续）
  - 8 人力资源安全
  - 9 物理和环境安全
  - 10 通信和操作管理
  - 11 访问控制
  - 12 信息系统获取、开发和维护
  - 13 信息安全事件管理
  - 14 业务连续性管理
  - 15 符合性
  - 参考文献

GB/T 22081-2008

- 前言
  - [给出该标准编制和管理相关的信息]
  - 该等同采用ISO/IEC 27002:2005《信息技术 — 安全技术 — 信息安全管理实用规则》。
  - 代替并废止GB/T 19716-2005（修改采用国际标准ISO/IEC 17799:2000）

GB/T 22081-2008

- 引言
  - 0.1 什么是信息安全?
    - 信息安全是保护信息免受各种威胁的损害，以确保业务连续性，业务风险最小化，投资回报和商业机遇最大化。
    - 信息安全是通过实施一组合适的控制措施而达到的，包括策略、过程、规程、组织结构以及软件和硬件功能。
    - 在必要时需建立、实施、监视、评审和改进这些控制措施，以确保满足该组织的特定安全和业务目标。

GB/T 22081-2008

- 引言（续）
  - 0.2 为什么需要信息安全?
    - 信息及其支持过程、系统和网络都是重要的业务资产。
    - 定义、实现、保持和改进信息安全对保持竞争优势、现金周转、赢利、守法和商业形象可能是至关重要的。
    - 各组织及其信息系统和网络面临来自各个方面的安全威胁。
    - 信息安全对于政府和企业的业务以及保护关键基础设施是非常重要的。
    - 许多信息系统并没有被设计成是安全的。

GB/T 22081-2008

- 引言（续）
  - 0.3 如何建立安全要求
    - 通过对组织进行风险的评估获得，并考虑到组织的整体业务策略与目标。
    - 满足的法律、法规、规章和合同要求。
    - 组织开发的支持其运行的信息处理的原则、目标和业务要求的特定集合。
  - 0.4 评估安全风险
    - 通过对安全风险进行系统地评估，识别安全要求。
    - 风险评估宜定期进行，以应对可能影响风险评估结果的任何变化。

GB/T 22081-2008

- 引言（续）
  - 0.5 选择控制措施
    - 一旦安全要求和风险已被识别并已作出风险处理决定，则宜选择并实现合适的控制措施，以确保风险降低到可接受的级别。
    - 控制措施可以从该标准或其他控制措施集合中选择，或者当合适时设计新的控制措施以满足特定需求。
  - 0.6 信息安全起点
    - 许多控制措施被认为是实现信息安全的良好起点。
    - 它们或者是基于重要的法律要求，或者被认为是信息安全的常用惯例。
    - 但不能取代基于风险评估而选择的控制措施。

GB/T 22081-2008

- 引言（续）
  - 0.7 关键的成功因素
    - 反映业务目标
    - 与组织文化保持一致
    - 管理者可见的支持和承诺
    - 理解信息安全要求、风险评估和风险管理
    - 传达信息安全意识和知识
    - 分发信息安全指南
    - 资金支持
    - 意识、培训和教育
    - 信息安全事件管理
    - 信息安全管理绩效测量

GB/T 22081-2008

- 引言（续）
  - 0.8 编制组织的指南
    - 该标准可作为是组织开发其详细信息安全管理指南的起点。

GB/T 22081-2008

- 1 范围
  - 该标准给出了一个组织启动、实施、保持和改进信息安全管理的指南和一般原则。
  - 该标准列出的目标为通常所接受的信息安全管理的目的提供了一般性指导。
  - 该标准的控制目标和控制措施的实施旨在满足风险评估所识别的要求。
  - 该标准可作为建立组织的安全准则和有效安全管理实践的实用指南，并有助于在组织间的活动中构建互信。

GB/T 22081-2008

- 2 术语和定义
  - 资产 asset
  - 控制措施 control
  - 指南 guideline
  - 信息处理设施 information processing facilities
  - 信息安全 information security
  - 信息安全事态 information security event
  - 信息安全事件 information security incident
  - 方针 policy

GB/T 22081-2008

- 2 术语和定义（续）
  - 风险 risk
  - 风险分析 risk analysis
  - 风险评估 risk assessment
  - 风险评价 risk evaluation
  - 风险管理 risk management
  - 风险处理 risk treatment
  - 第三方 third party
  - 威胁 threat
  - 脆弱性 vulnerability

GB/T 22081-2008

- 3 本标准的结构
  - 11个安全控制措施的章节（共含有39个主要安全类别）
  - 1个介绍风险评估和处理的章节。
  - 每一个主要安全类别包含：
    - 一个控制目标，声明要实现什么；
    - 一个或多个控制措施，可被用于实现该控制目标。

GB/T 22081-2008

- 4 风险评估和处理
  - 4.1 评估安全风险
    - 风险评估宜对照风险接受准则和组织相关目标，识别、量化并区分风险的优先次序。
    - 风险评估宜周期性加以执行，以指出安全要求和风险情形的变化。
  - 4.2 处理安全风险
    - 确定风险是否能被接受的准则。
    - 作出风险处理决定。
      - 风险降低、风险接受、风险规避、风险转移
    - 降低风险：选择和实施适当的控制措施。

GB/T 22081-2008

- 5 安全方针
  - 5.1 信息安全方针
    - 控制目标：依据业务要求和相关法律法规提供管理指导并支持信息安全。
    - 控制措施
      - 5.1.1 信息安全方针文件
      - 5.1.2 信息安全方针的评审

GB/T 22081-2008

- 6 信息安全组织
  - 6.1 内部组织
    - 控制目标：管理组织范围内信息安全。
    - 控制措施
      - 6.1.1 信息安全的管理承诺
      - 6.1.2 信息安全协调
      - 6.1.3 信息安全职责的分配
      - 6.1.4 信息处理设施的授权过程
      - 6.1.5 保密性协议
      - 6.1.6 与政府部门的联系
      - 6.1.7 与特定利益集团的联系
      - 6.1.8 信息安全的独立评审

GB/T 22081-2008

- 6 信息安全组织（续）
  - 6.2 外部各方
    - 控制目标：保持组织的被外部各方访问、处理、管理或与外部进行通信的信息和信息处理设施的安全。
    - 控制措施
      - 6.2.1 与外部各方相关风险的识别
      - 6.2.2 处理与顾客有关的安全问题
      - 6.2.3 处理第三方协议中的安全问题

GB/T 22081-2008

- 7 资产管理
  - 7.1 对资产负责
    - 控制目标：实现和保持对组织资产的适当保护。
    - 控制措施
      - 7.1.1 资产清单
      - 7.1.2 资产责任人
      - 7.1.3 资产的可接受使用

GB/T 22081-2008

- 7 资产管理（续）
  - 7.2 信息分类
    - 控制目标：确保信息受到适当级别的保护。
    - 控制措施
      - 7.2.1 分类指南
      - 7.2.2 信息的标记和处理

GB/T 22081-2008

- 8 人力资源安全
  - 8.1 任用之前
    - 控制目标：确保雇员、承包方人员和第三方人员理解其职责、考虑对其承担的角色是适合的，以降低设施被窃、欺诈和误用的风险。
    - 控制措施
      - 8.1.1 角色和职责
      - 8.1.2 审查
      - 8.1.3 任用条款和条件

GB/T 22081-2008

- 8 人力资源安全（续）
  - 8.2 任用中
    - 控制目标：确保所有的雇员、承包方人员和第三方人员知悉信息安全威胁和利害关系、他们的职责和义务、并准备好在其正常工作过程中支持组织的安全方针，以减少人为出错的风险。
    - 控制措施
      - 8.2.1 管理职责
      - 8.2.2 信息安全意识、教育和培训
      - 8.2.3 纪律处理过程

GB/T 22081-2008

- 8 人力资源安全（续）
  - 8.3 任用的终止或变化
    - 控制目标：确保雇员、承包方人员和第三方人员以一个规范的方式退出一个组织或改变其任用关系。
    - 控制措施
      - 8.3.1 终止职责
      - 8.3.2 资产的归还
      - 8.3.3 撤销访问权

GB/T 22081-2008

- 9 物理和环境安全
  - 9.1 安全区域
    - 控制目标：防止对组织场所和信息的未授权物理访问、损坏和干扰。
    - 控制措施
      - 9.1.1 物理安全周边
      - 9.1.2 物理入口控制
      - 9.1.3 办公室、房间和设施的安全保护
      - 9.1.4 外部和环境威胁的安全防护
      - 9.1.5 在安全区域工作
      - 9.1.6 公共访问、交接区安全

GB/T 22081-2008

- 9 物理和环境安全（续）
  - 9.2 设备安全
    - 控制目标：防止资产的丢失、损坏、失窃或危及资产安全以及组织活动的中断。
    - 控制措施
      - 9.2.1 设备安置和保护
      - 9.2.2 支持性设施
      - 9.2.3 布缆安全
      - 9.2.4 设备维护
      - 9.2.5 组织场所外的设备安全
      - 9.2.6 设备的安全处置或再利用
      - 9.2.7 资产的移动

GB/T 22081-2008

- 10 通信和操作管理
  - 10.1 操作规程和职责
    - 控制目标：确保正确、安全的操作信息处理设施。
    - 控制措施
      - 10.1.1 文件化的操作规程
      - 10.1.2 变更管理
      - 10.1.3 责任分割
      - 10.1.4 开发、测试和运行设施分离

GB/T 22081-2008

- 10 通信和操作管理（续）
  - 10.2 第三方服务交付管理
    - 控制目标：实施和保持符合第三方服务交付协议的信息安全和服务交付的适当水准。
    - 控制措施
      - 10.2.1 服务交付
      - 10.2.2 第三方服务的监视和评审
      - 10.2.3 第三方服务的变更管理

GB/T 22081-2008

- 10 通信和操作管理（续）
  - 10.3 系统规划和验收
    - 控制目标：将系统失效的风险降至最小。
    - 控制措施
      - 10.3.1 容量管理
      - 10.3.2 系统验收

GB/T 22081-2008

- 10 通信和操作管理（续）
  - 10.4 防范恶意和移动代码
    - 控制目标：保护软件和信息的完整性。
    - 控制措施
      - 10.4.1 控制恶意代码
      - 10.4.2 控制移动代码

GB/T 22081-2008

- 10 通信和操作管理（续）
  - 10.5 备份
    - 控制目标：保持信息和信息处理设施的完整性及可用性。
    - 控制措施
      - 10.5.1 信息备份

GB/T 22081-2008

- 10 通信和操作管理（续）
  - 10.6 网络安全管理
    - 控制目标：确保网络中信息的安全性并保护支持性的基础设施。
    - 控制措施
      - 10.6.1 网络控制
      - 10.6.2 网络服务安全

GB/T 22081-2008

- 10 通信和操作管理（续）
  - 10.7 介质处置
    - 控制目标：防止资产遭受未授权泄露、修改、移动或销毁以及业务活动的中断。
    - 控制措施
      - 10.7.1 可移动介质的管理
      - 10.7.2 介质的处置
      - 10.7.3 信息处理规程
      - 10.7.4 系统文件安全

GB/T 22081-2008

- 10 通信和操作管理（续）
  - 10.8 信息的交换
    - 控制目标：保持组织内以及与组织外信息和软件交换的安全。
    - 控制措施
      - 10.8.1 信息交换策略和规程
      - 10.8.2 交换协议
      - 10.8.3 运输中的物理介质
      - 10.8.4 电子消息发送
      - 10.8.5 业务信息系统

GB/T 22081-2008

- 10 通信和操作管理（续）
  - 10.9 电子商务服务
    - 控制目标：确保电子商务服务的安全及其安全使用。
    - 控制措施
      - 10.9.1 电子商务
      - 10.9.2 在线交易
      - 10.9.3 公共可用信息

GB/T 22081-2008

- 10 通信和操作管理（续）
  - 10.10 监视
    - 控制目标：检测未经授权的信息处理活动。
    - 控制措施
      - 10.10.1 审计记录
      - 10.10.2 监视系统的使用
      - 10.10.3 日志信息的保护
      - 10.10.4 管理员和操作员日志
      - 10.10.5 故障日志
      - 10.10.6 时钟同步

GB/T 22081-2008

- 11 访问控制
  - 11.1 访问控制的业务要求
    - 控制目标：控制对信息的访问。
    - 控制措施
      - 11.1.1 访问控制策略

GB/T 22081-2008

- 11 访问控制（续）
  - 11.2 用户访问管理
    - 控制目标：确保授权用户访问信息系统，并防止未授权的访问。
    - 控制措施
      - 11.2.1 用户注册。
      - 11.2.2 特殊权限管理
      - 11.2.3 用户口令管理
      - 11.2.4 用户访问权的复查

GB/T 22081-2008

- 11 访问控制（续）
  - 11.3 用户职责
    - 控制目标：防止未授权用户对信息和信息处理设施的访问、损害或窃取。
    - 控制措施
      - 11.3.1 口令使用
      - 11.3.2 无人值守的用户设备
      - 11.3.3 清空桌面和屏幕策略

GB/T 22081-2008

- 11 访问控制（续）
  - 11.4 网络访问控制
    - 控制目标：防止对网络服务的未授权访问。
    - 控制措施
      - 11.4.1 使用网络服务的策略
      - 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
      - 11.4.5 网络隔离
      - 11.4.6 网络连接控制
      - 11.4.7 网络路由控制

GB/T 22081-2008

- 11 访问控制（续）
  - 11.5 操作系统访问控制
    - 控制目标：防止对操作系统的未授权访问。
    - 控制措施
      - 11.5.1 安全登录规程
      - 11.5.2 用户标识和鉴别
      - 11.5.3 口令管理系统
      - 11.5.4 系统实用工具的使用
      - 11.5.5 会话超时
      - 11.5.6 联机时间的限定

GB/T 22081-2008

- 11 访问控制（续）
  - 11.6 应用和信息访问控制
    - 控制目标：防止对应用系统中信息的未授权访问。
    - 控制措施
      - 11.6.1 信息访问限制
      - 11.6.2 敏感系统隔离

GB/T 22081-2008

- 11 访问控制（续）
  - 11.7 移动计算和远程工作
    - 控制目标：确保使用移动计算和远程工作设施时的信息安全。
    - 控制措施
      - 11.7.1 移动计算和通信
      - 11.7.2 远程工作

GB/T 22081-2008

- 12 信息系统获取、开发和维护
  - 12.1 信息系统的安全要求
    - 控制目标：确保安全是信息系统的一个有机组成部分。
    - 控制措施
      - 12.1.1 安全要求分析和说明

GB/T 22081-2008

- 12 信息系统获取、开发和维护（续）
  - 12.2 应用中的正确处理
    - 控制目标：防止应用系统中的信息的差错、遗失、未授权的修改或误用。
    - 控制措施
      - 12.2.1 输入数据确认
      - 12.2.2 内部处理的控制
      - 12.2.4 输出数据确认

GB/T 22081-2008

- 12 信息系统获取、开发和维护（续）
  - 12.3 密码控制
    - 控制目标：通过密码方法保护信息的保密性、真实性或完整性。
    - 控制措施
      - 12.3.1 使用密码控制的策略
      - 12.3.2 密钥管理

GB/T 22081-2008

- 12 信息系统获取、开发和维护（续）
  - 12.4 系统文件的安全
    - 控制目标：确保系统文件的安全。
    - 控制措施
      - 12.4.1 运行软件的控制
      - 12.4.2 系统测试数据的保护
      - 12.4.3 对程序源代码的访问控制

GB/T 22081-2008

- 12 信息系统获取、开发和维护（续）
  - 12.5 开发和支持过程中的安全
    - 控制目标：维护应用系统软件和信息的安全。
    - 控制措施
      - 12.5.1 变更控制规程
      - 12.5.2 操作系统变更后应用的技术评审
      - 12.5.3 软件包变更的限制
      - 12.5.4 信息泄露
      - 12.5.5 外包软件开发

GB/T 22081-2008

- 12 信息系统获取、开发和维护（续）
  - 12.6 技术脆弱性管理
    - 控制目标：降低利用公布的技术脆弱性导致的风险。
    - 控制措施
      - 12.6.1 技术脆弱性的控制

GB/T 22081-2008

- 13 信息安全事件管理
  - 13.1 报告信息安全事态和弱点
    - 控制目标：确保与信息系统有关的信息安全事态和弱点能够以某种方式传达，以便及时采取纠正措施。
    - 控制措施
      - 13.1.1 报告信息安全事态
      - 13.1.2 报告安全弱点

GB/T 22081-2008

- 13 信息安全事件管理（续）
  - 13.2 信息安全事件和改进的管理
    - 控制目标：确保采用一致和有效的方法对信息安全事件进行管理。
    - 控制措施
      - 13.2.1 职责和规程
      - 13.2.2 对信息安全事件的总结
      - 13.2.3 证据的收集

GB/T 22081-2008

- 14 业务连续性管理
  - 14.1 业务连续性管理的信息安全方面
    - 控制目标：防止业务活动中断，保护关键业务过程免受信息系统重大失误或灾难的影响，并确保它们的及时恢复。
    - 控制措施
      - 14.1.1 在业务连续性管理过程中包含信息安全
      - 14.1.2 业务连续性和风险评估
      - 14.1.3 制定和实施包含信息安全的连续性计划
      - 14.1.4 业务连续性计划框架
      - 14.1.5 测试、维护和再评估业务连续性计划

GB/T 22081-2008

- 15 符合性
  - 15.1 符合法律要求
    - 控制目标：避免违反任何法律、法令、法规或合同义务以及任何安全要求。
    - 控制措施
      - 15.1.1 可用法律的识别
      - 15.1.2 知识产权（IPR）
      - 15.1.3 保护组织的记录
      - 15.1.4 数据保护和个人信息的隐私
      - 15.1.5 防止滥用信息处理设施
      - 15.1.6 密码控制措施的规则

GB/T 22081-2008

- 15 符合性（续）
  - 15.2 符合安全策略和标准以及技术符合性
    - 控制目标：确保系统符合组织的安全策略及标准。
    - 控制措施
      - 15.2.1 符合安全策略和标准
      - 15.2.2 技术符合性核查

GB/T 22081-2008

- 15 符合性（续）
  - 15.3 信息系统审计考虑
    - 控制目标：将信息系统审计过程的有效性最大化，干扰最小化。
    - 控制措施
      - 15.3.1 信息系统审计控制措施
      - 15.3.2 信息系统审计工具的保护

第三部分 ISMS国家标准解读

- 3.1 国家标准化组织
- 3.2 正式发布的国家标准
- 3.3 报批中的国家标准
- **3.4 标准解读**
  - GB/T 22080-2008《信息技术　安全技术　信息安全管理体系 要求》
  - GB/T 22081-2008《信息技术　安全技术　信息安全管理实用规则》
  - **GB/T 20984-2007《信息安全技术 信息安全风险评估规范》**
  - GB/T 20988-2007《信息安全技术　信息系统灾难恢复规范》
  - GB/Z 20985-2007《信息技术　安全技术　信息安全事件管理指南》

GB/T 20984-2007

- 标准名称
  - 中文：信息安全技术　信息安全风险评估规范
  - 英文：Information security techniques – Risk assessment specification for information security
- 标准号：GB/T 20984-2007
- 中标分类：L80
- 采标情况：自主研制

GB/T 20984-2007

- 发布日期：2007-6-14
- 实施日期：2007-11-1
- 发布单位
  - 中华人民共和国国家质量监督检验检疫总局
  - 中国国家标准化管理委员会

GB/T 20984-2007

- 标准简介
  - 该标准提出了风险评估的基本概念、要素关系、分析原理、实施流程和评估方法，以及风险评估在信息系统生命周期不同阶段的实施要点和工作形式。该标准适用于规范组织开展的风险评估工作。

GB/T 20984-2007

- 标准结构
  - 前言
  - 引言
  - 1 范围
  - 2 规范性引用文件
  - 3 术语和定义
  - 4 风险评估框架及流程
  - 5 风险评估实施
  - 6 信息系统生命周期各阶段的风险评估
  - 7 风险评估的工作形式

GB/T 20984-2007

- 标准结构
  - 附录A （资料性附录） 风险的计算方法
  - 附录B （资料性附录） 风险评估的工具
  - 参考文献

GB/T 20984-2007

- 前言
  - [给出该标准编制和管理相关的信息]
- 引言
  - [简要阐述信息安全风险评估的含义，以及风险评估工作对于信息系统安全保障的重要作用]
  - 从**风险管理**角度，运用科学的方法和手段，系统地分析**信息系统**所面临的**威胁**及其存在的**脆弱性**，评估安全事件一旦发生可能造成的**危害程度**，提出有针对性的抵御威胁的**防护对策**和整改措施，为防范和化解信息安全风险，将风险控制在**可接受的水平**，最大限度地保障信息安全提供科学依据。

GB/T 20984-2007

- 引言（续）
  - 信息安全风险评估作为信息安全保障工作的基础性工作和重要环节，要**贯穿于信息系统的规划、设计、实施、运行维护以及废弃各个阶段**，是信息安全等级保护制度建设的重要科学方法之一。

GB/T 20984-2007

- 1 范围
  - [阐明该标准所涵盖的内容范围和适用范围]
  - 风险评估的基本概念、要素关系、分析原理、实施流程和评估方法；
  - 风险评估在信息系统生命周期不同阶段的实施要点和工作形式。
  - 适用于规范组织开展的风险评估工作。

GB/T 20984-2007

- 2 规范性引用文件
  - [提供该标准正文中所引用的相关标准或规范性文件的信息]
    - GB/T 9361《计算机场地安全要求》
    - GB 17859-1999《计算机信息系统安全保护等级划分准则》
    - GB/T 18336-2001《信息技术　安全技术　信息技术安全性评估准则》（ISO/IEC 15408:1999，IDT）
    - GB/T 19716-2005《信息技术　信息安全管理实用规则》（ISO/IEC 17799:2000，IDT）

GB/T 20984-2007

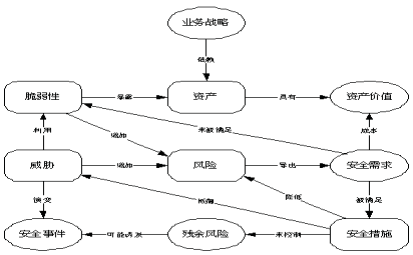
- 3 术语和定义
  - 3.1 资产 asset
  - 3.2 资产价值 asset value
  - 3.3 可用性 availability
  - 3.4 业务战略 business strategy
  - 3.5 保密性 confidentiality
  - 3.6 信息安全风险 information security risk
  - 3.7 （信息安全）风险评估 (information security) risk assessment
  - 3.8 信息系统 information system

GB/T 20984-2007

- 3 术语和定义（续）
  - 3.9 检查评估 inspection assessment
  - 3.10 完整性 integrity
  - 3.11 组织 organization
  - 3.12 残余风险 residual risk
  - 3.13 自评估 self-assessment
  - 3.14 安全事件 security incident
  - 3.15 安全措施 security measure
  - 3.16 安全需求 security requirement
  - 3.17 威胁 threat
  - 3.18 脆弱性 vulnerability

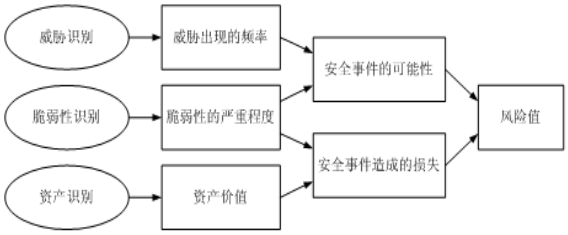
GB/T 20984-2007

- 4 风险评估框架及流程
  - 4.1 风险要素关系
    - [阐明风险评估的基本要素以及各要素之间的关系]



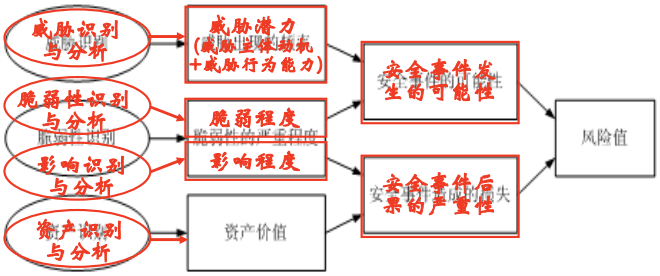
GB/T 20984-2007

- 4 风险评估框架及流程（续）
  - 4.2 风险分析原理
    - [阐明风险分析的原理和过程]



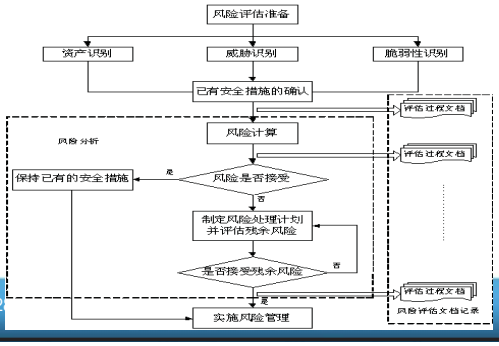
GB/T 20984-2007

- 4 风险评估框架及流程（续）
  - 4.2 风险分析原理（续）
    - 修正（个人观点）



GB/T 20984-2007

- 4 风险评估框架及流程（续）
  - 4.3 实施流程
    - [阐述风险评估实施流程]



GB/T 20984-2007

- 5 风险评估实施
  - 5.1 风险评估准备
    - [阐明风险评估实施之前的各项准备工作]
    - a) 确定风险评估的目标
    - b) 确定风险评估的范围
    - c) 组建适当的评估管理与实施团队
    - d) 进行系统调研
    - e) 确定评估依据和方法
    - f) 制定风险评估方案
    - g) 获得最高管理者对风险评估工作的支持

GB/T 20984-2007

- 5 风险评估实施（续）
  - 5.2 资产识别
    - 5.2.1 资产分类
      - [说明资产的价值判定原则以及资产的分类]
      - 资产的价值不是仅以资产的经济价值来衡量，而是由资产在保密性、完整性和可用性这三个安全属性上的达成程度或者其安全属性未达成时所造成的影响程度来决定的。
      - 数据、软件、硬件、服务、人员等类型
    - 5.2.2 资产赋值
      - [给出资产保密性、完整性和可用性的赋值参考，以及资产重要性等级评定方法]

GB/T 20984-2007

- 5 风险评估实施（续）
  - 5.3 威胁识别
    - 5.3.1 威胁分类
      - [给出威胁的分类方法]
      - 威胁来源的分类方法
      - 基于表现形式的威胁分类方法
    - 5.3.2 威胁赋值
      - [给出威胁的赋值方法]
      - 基于威胁出现频率的赋值方法

GB/T 20984-2007

- 5 风险评估实施（续）
  - 5.4 脆弱性识别
    - 5.4.1 脆弱性识别内容
      - [给出脆弱性识别的内容]
      - 技术脆弱性：物理环境、网络结构、系统软件、应用中间件、应用系统
      - 管理脆弱性：技术管理、组织管理
      - 识别方法：问卷调查、工具检测、人工核查、文档查阅、渗透性测试等

GB/T 20984-2007

- 5 风险评估实施（续）
  - 5.4 脆弱性识别
    - 5.4.2 脆弱性赋值
      - [脆弱性赋值方法]
      - “可以根据脆弱性对资产的暴露程度、技术实现的**难易程度**、流行程度等，采用等级方式对已识别的脆弱性的**严重程度**进行赋值。”
      - “表10 脆弱性严重程度赋值表”实际是对“影响”风险要素的赋值。
      - 准确来讲“脆弱性”风险要素的赋值应是对脆弱性被利用的难易程度进行赋值。

GB/T 20984-2007

- 5 风险评估实施（续）
  - 5.5 已有安全措施确认
    - [已有安全措施的确认方法]
    - 安全措施的确认应评估其有效性，即是否真正地降低了系统的脆弱性，抵御了威胁，**抑制了安全事件带来的影响**。
    - 对有效的安全措施继续保持，以避免不必要的工作和费用，防止安全措施的重复实施。
    - 对确认为不适当的安全措施应核实是否应被取消或对其进行修正，或用更合适的安全措施替代。
    - 安全措施：预防性安全措施、保护性安全措施

GB/T 20984-2007

- 5 风险评估实施（续）
  - 5.6 风险分析
    - 5.6.1 风险计算原理
      - 风险值 = R (A, T, V) = R (L (T, V), F (Ia, Va))
        - R：安全风险计算函数
        - A：资产
        - T：威胁潜力
        - V：脆弱程度（即脆弱性被利用的难易程度）
        - **Ia：对资产的影响程度**
        - **Va：资产所具有的价值**
        - L：威胁利用脆弱性导致安全事件的可能性
        - F：安全事件发生后造成的损失

GB/T 20984-2007

- 5 风险评估实施（续）
  - 5.6 风险分析（续）
    - 5.6.2 风险结果判定
      - [给出风险评估结果等级判定方法]
      - 五级划分
        - 5：很高
        - 4：高
        - 3：中等
        - 2：低
        - 1：很低

GB/T 20984-2007

- 5 风险评估实施（续）
  - 5.6 风险分析（续）
    - 5.6.3 风险处理计划
      - [给出风险处理计划的内容]
      - 明确采取的弥补脆弱性、**抵御威胁**、**抑制影响**的安全措施、预期效果、实施条件、进度安排、责任部门等。
      - 风险处理方式
        - 规避风险
        - 转移风险
        - 降低风险
        - 接受风险

GB/T 20984-2007

- 5 风险评估实施（续）
  - 5.6 风险分析（续）
    - 5.6.4 残余风险评估
      - [残余风险的评估方法]
      - 判断实施安全措施后的残余风险是否已经降低到可接受的水平。
      - 残余风险的评估可以依据本标准提出的风险评估流程实施，也可做适当裁减。
      - 若残余风险的结果仍处于不可接受的风险范围内，应考虑是否接受此风险或进一步增加相应的安全措施。

GB/T 20984-2007

- 5 风险评估实施（续）
  - 5.7 风险评估文档记录
    - 5.7.1 风险评估文档记录的要求
      - [给出风险评估文档记录的要求]
        - 得到批准、可识别更改、分发受控、防止作废文件被使用
        - 规定其标识、储存、保护、检索、保存期限以及处置所需的控制。

GB/T 20984-2007

- 5 风险评估实施（续）
  - 5.7 风险评估文档记录（续）
    - 5.7.2 风险评估文档
      - [风险评估文档的组成]
      - a) 风险评估方案
      - b) 风险评估程序
      - c) 资产识别清单
      - d) 重要资产清单
      - e) 威胁列表
      - f) 脆弱性列表

GB/T 20984-2007

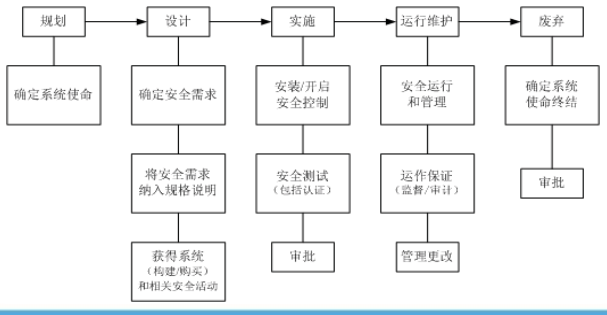
- 5 风险评估实施（续）
  - 5.7 风险评估文档记录（续）
    - 5.7.2 风险评估文档（续）
      - g) 已有安全措施确认表
      - h) 风险评估报告
      - i) 风险处理计划
      - j) 风险评估记录

GB/T 20984-2007

- 6 信息系统生命周期各阶段的风险评估
  - [阐明信息系统生命周期各阶段风险评估的含义，并分别说明规划阶段、设计阶段、实施阶段以及运行维护阶段的风险评估工作重点]
  - 6.1 信息系统生命周期概述
  - 6.2 规划阶段的风险评估
  - 6.3 设计阶段的风险评估
  - 6.4 实施阶段的风险评估
  - 6.5 运行维护阶段的风险评估
  - 6.6 废弃阶段的风险评估

GB/T 20984-2007

- 6 信息系统生命周期各阶段的风险评估（续）
  - 信息系统生命周期各阶段安全活动



GB/T 20984-2007

- 7 风险评估的工作形式
  - 7.1 概述
    - [概述风险评估的工作形式]
    - 两种形式：自评估、检查评估
    - 以自评估为主，自评估和检查评估相互结合、互为补充。
  - 7.2 自评估
    - [给出自评估的工作要求]
    - 信息系统拥有、运营或使用单位发起的对本单位信息系统进行的风险评估。
    - 由发起方实施或委托风险评估服务技术支持方实施。

GB/T 20984-2007

- 7 风险评估的工作形式
  - 7.3 检查评估
    - [给出检查评估的工作要求]
    - 信息系统上级管理部门组织的或国家有关职能部门依法开展的风险评估。
    - 可在自评估实施的基础上，对关键环节或重点内容实施抽样评估
    - 可委托风险评估服务技术支持方实施，但评估结果仅对检查评估的发起单位负责。

GB/T 20984-2007

- 附录A （资料性附录） 风险的计算方法
  - [介绍目前通用的风险计算方法]
  - A.1 使用矩阵法计算风险
  - A.2 使用相乘法计算风险

GB/T 20984-2007

- 附录B （资料性附录） 风险评估的工具
  - [介绍风险评估与管理工具]
  - B.1 风险评估与管理工具
    - 基于信息安全标准的风险评估与管理工具
    - 基于知识的风险评估与管理工具
    - 基于模型的风险评估与管理工具

GB/T 20984-2007

- 附录B （资料性附录） 风险评估的工具（续）
  - B.2 系统基础平台风险评估工具
    - 脆弱性扫描工具
      - 基于网络的扫描器
      - 基于主机的扫描器
      - 分布式网络扫描器
      - 数据库脆弱性扫描器
    - 渗透性测试工具

GB/T 20984-2007

- 附录B （资料性附录） 风险评估的工具（续）
  - B.3 风险评估辅助工具
    - 检查列表
    - 入侵检测系统
    - 安全审计工具
    - 拓扑发现工具
    - 资产信息收集系统
    - 其他：如评估指标库、知识库、漏洞库、算法库、模型库等。

第三部分 ISMS国家标准解读

- 3.1 国家标准化组织
- 3.2 正式发布的国家标准
- 3.3 报批中的国家标准
- **3.4 标准解读**
  - GB/T 22080-2008《信息技术　安全技术　信息安全管理体系 要求》
  - GB/T 22081-2008《信息技术　安全技术　信息安全管理实用规则》
  - GB/T 20984-2007《信息安全技术　信息安全风险评估规范》
  - **GB/T 20988-2007《信息安全技术 信息系统灾难恢复规范》**
  - GB/Z 20985-2007《信息技术　安全技术　信息安全事件管理指南》

GB/T 20988-2007

- 标准名称
  - 中文：信息安全技术　信息系统灾难恢复规范
  - 英文：Information security techniques – Disaster recovery specifications for information systems
- 标准号：GB/T 20988-2007
- 中标分类：L80
- 采标情况：自主研制

GB/T 20988-2007

- 发布日期：2007-6-14
- 实施日期：2007-11-1
- 发布单位
  - 中华人民共和国国家质量监督检验检疫总局
  - 中国国家标准化管理委员会

GB/T 20988-2007

- 标准简介
  - 该标准规定了信息系统灾难恢复应遵循的基本要求。该标准适用于信息系统灾难恢复的规划、、审批、实施和管理。

GB/T 20988-2007

- 标准结构
  - 前言
  - 引言
  - 1 范围
  - 2 规范性引用文件
  - 3 术语和定义
  - 4 灾难恢复概述
  - 5 灾难恢复需求的确定
  - 6 灾难恢复策略的制定
  - 7 灾难恢复策略的实现

GB/T 20988-2007

- 标准结构（续）
  - 附录A（规范性附录） 灾难恢复能力等级划分
  - 附录B（资料性附录） 灾难恢复预案框架
  - 附录C（资料性附录） 某行业RTO/RPO与灾难恢复能力等级的关系示例

GB/T 20988-2007

- 前言
  - [给出该标准编制和管理相关的信息]
- 引言
  - 该标准参照和借鉴国内外相关标准，结合国家重要信息系统行业技术发展和实践经验制定而成。
  - 各行业可根据行业特点和信息技术的应用情况制定相应的信息系统灾难恢复能力等级要求和指标体系。

GB/T 20988-2007

- 1 范围
  - 该标准规定了信息系统灾难恢复应遵循的基本要求。
  - 该标准适用于信息系统灾难恢复的规划、审批、实施和管理。
- 2 规范性引用文件
  - GB/T 5271.8-2001《信息技术 词汇 第8部分：安全》

GB/T 20988-2007

- 3 术语和定义
  - 3.1 灾难备份中心 backup center for disaster recovery
  - 3.2 灾难备份 backup for disaster recovery
  - 3.3 灾难备份系统 backup system for disaster recovery
  - 3.4 业务连续管理 business continuity management (BCM)
  - 3.5 业务影响分析 business impact analysis (BIA)
  - 3.6 关键业务功能 critical business functions
  - 3.7 数据备份策略 data backup strategy

GB/T 20988-2007

- 3 术语和定义（续）
  - 3.8 灾难 disaster
  - 3.9 灾难恢复 disaster recovery
  - 3.10 灾难恢复预案 disaster recovery plan
  - 3.11 灾难恢复规划 disaster recovery planning (DRP)
  - 3.12 灾难恢复能力 disaster recovery capability
  - 3.13 演练 exercise
  - 3.14 场外存放 offsite storage
  - 3.15 主中心 primary center / 主站点 primary site / 生产中心 production center

GB/T 20988-2007

- 3 术语和定义（续）
  - 3.16 主系统 primary system / 生产系统 production system
  - 3.17 区域性灾难 regional disaster
  - 3.18 恢复时间目标 recovery time objective
  - 3.19 恢复点目标 recovery point objective

GB/T 20988-2007

- 3 术语和定义（续）
  - 3.20 重续 resumption
  - 3.21 回退 return / 复原 restoration

GB/T 20988-2007

- 4 灾难恢复概述
  - 4.1 灾难恢复的工作范围
    - 灾难恢复规划
      - 灾难恢复需求的确定
      - 灾难恢复策略的制定
      - 灾难恢复策略的实现
      - 灾难恢复预案的制定、落实和管理
    - 灾难备份中心的日常运行
    - 关键业务功能在灾难备份中心的恢复和重续运行
    - 主系统的灾后重建和回退工作
    - 突发事件发生后的应急响应

GB/T 20988-2007

- 4 灾难恢复概述（续）
  - 4.2 灾难恢复的组织机构
    - 4.2.1 组织机构的设立
      - 由管理、业务、技术和行政后勤等人员组成
        - ➢灾难恢复领导小组
        - ➢灾难恢复规划实施组
        - ➢灾难恢复日常运行组。
      - 可聘请具有相应资质的外部专家，也可委托具有相应资质的外部机构。

GB/T 20988-2007

- 4 灾难恢复概述（续）
  - 4.2 灾难恢复的组织机构（续）
    - 4.2.2 组织机构的职责
      - 灾难恢复领导小组：审核并批准经费预算、灾难恢复策略、预案、预案的执行。
      - 灾难恢复规划实施组：需求分析、策略和等级提出、策略实现、预案制定、预案测试和演练。
      - 灾难恢复日常运行组：灾难恢复系统实施、日常管理、系统运维、专业技术支持、教育/培训/演练、预案维护和管理、损失控制和损害评估、信息系统和业务功能恢复、外部协作。

GB/T 20988-2007

- 4 灾难恢复概述（续）
  - 4.3 灾难恢复规划的管理
    - 评估分析、筹备资源、制定计划、监管活动、跟踪进展、问题管理、变更管理。
  - 4.4 灾难恢复的外部协作
    - 与相关管理部门、设备及服务提供商、电信、电力、新闻媒体等保持联络和协作；
    - 确保在灾难发生时能及时通报准确情况和获得适当支持。
  - 4.5 灾难恢复的审计和备案
    - 审计和备案灾难恢复的等级评定、预案制定。

GB/T 20988-2007

- 5 灾难恢复需求的确定
  - 5.1 风险分析
    - 标识信息系统的**资产**价值，识别信息系统面临的自然的和人为的**威胁**，识别信息系统的**脆弱性**，分析各种威胁发生的可能性并定量或定性描述可能造成的**损失**，识别现有的风险防范和**控制措施**。
    - 通过**技术和管理手段**，防范或控制信息系统的风险。
    - 依据防范或控制风险的可行性和**残余风险**的可接受程度，确定对风险的防范和控制措施。
    - 参考GB/T 20984-2007《信息安全技术 信息安全风险评估规范》

GB/T 20988-2007

- 5 灾难恢复需求的确定（续）
  - 5.2 业务影响分析
    - 5.2.1 分析业务功能和相关资源配置
      - 明确相关信息的保密性、完整性和可用性要求。
    - 5.2.2 评估中断影响
      - 采用定量和/或定性的方法。
  - 5.3 确定灾难恢复目标
    - 关键业务功能及恢复的优先顺序；
    - 灾难恢复时间范围，即RTO和RPO的范围。

GB/T 20988-2007

- 6 灾难恢复策略的制定
  - 6.1 灾难恢复策略制定的要素
    - 6.1.1 灾难恢复资源要素
      - 数据备份系统
      - 备用数据处理系统
      - 备用网络系统
      - 备用基础设施
      - 专业技术支持能力
      - 运行维护管理能力
      - 灾难恢复预案

GB/T 20988-2007

- 6 灾难恢复策略的制定（续）
  - 6.1 灾难恢复策略制定的要素
    - 6.1.2 成本效益分析原则
      - 根据灾难恢复目标，按照成本风险平衡原则，确定每项关键业务功能的灾难恢复策略。
    - 6.1.3 灾难恢复策略的组成
      - 灾难恢复资源的获取方式；
      - 灾难恢复能力等级，或灾难恢复资源各要素的具体要求。

GB/T 20988-2007

- 6 灾难恢复策略的制定（续）
  - 6.2 灾难恢复资源的获取方式
    - 数据备份系统：自建、租用
    - 备用数据处理系统：预定、购买、租用
    - 备用网络系统：预定、购买、租用
    - 备用基础设施：自建、共建、租用
    - 专业技术支持能力：专职、外援、兼职
    - 运行维护管理能力：自行、委托
    - 灾难恢复预案：自制、咨询、委托

GB/T 20988-2007

- 6 灾难恢复策略的制定（续）
  - 6.3 灾难恢复资源的要求
    - 数据备份系统：数据备份的范围、时间间隔、技术及介质、线路速率和设备规格
    - 备用数据处理系统：数据处理能力、与主系统的兼容性、平时状态（就绪或运行）
    - 备用网络系统：通信技术和线路带宽、通信设备功能和容量
    - 备用基础设施：与主中心的距离、场地和环境、运行维护和管理

GB/T 20988-2007

- 6 灾难恢复策略的制定（续）
  - 6.3 灾难恢复资源的要求（续）
    - 专业技术支持能力：软件/硬件/网络的技术支持、技术支持的组织架构、技术支持人员的数量和素质
    - 运行维护管理能力：组织架构、人员的数量和素质、管理制度
    - 灾难恢复预案：整体、制定过程、教育/培训/演练、管理

GB/T 20988-2007

- 7 灾难恢复策略的实现
  - 7.1 灾难备份系统技术方案的实现
    - 7.1.1 技术方案的设计
      - 数据备份系统、备用数据处理系统、备用网络系统的技术方案
    - 7.1.2 技术方案的验证、确认和系统开发
      - 确保技术方案满足灾难恢复策略的要求
    - 7.1.3 系统安装和测试
      - 确认各项功能可正确实现

GB/T 20988-2007

- 7 灾难恢复策略的实现（续）
  - 7.2 灾难备份中心的选择和建设
    - 7.2.1 选址原则
      - 避免与主中心遭受同类风险
      - 两种类型：同城、异地
      - 完备的通信、电力、交通等基础设施
      - 统筹规划、资源共享、平战结合
    - 7.2.2 基础设施的要求
      - 计算机机房符合国家标准
      - 工作辅助设施和生活设施符合灾难恢复目标

GB/T 20988-2007

- 7 灾难恢复策略的实现（续）
  - 7.3 专业技术支持能力的实现
    - 建立相应的技术支持组织
    - 定期对技术支持人员进行技能培训
  - 7.4 运行维护管理能力的实现
    - 建立各种操作规程和管理制度

GB/T 20988-2007

- 7 灾难恢复策略的实现（续）
  - 7.5 灾难恢复预案的实现
    - 7.5.1 灾难恢复预案的制定
      - 原则：完整性、易用性、明确性、有效性、兼容性
      - 过程：起草、评审、测试、完善、审核和批准
    - 7.5.2 灾难恢复预案的教育、培训和演练
      - 初期宣传教育
      - 培训需求评估、培训课程开发、培训记录
      - 演练计划
      - 演练记录和报告
      - 定期完整演练（至少每年一次）

GB/T 20988-2007

- 7 灾难恢复策略的实现（续）
  - 7.5 灾难恢复预案的实现（续）
    - 7.5.3 灾难恢复预案的管理
      - 保存和分发原则：专人负责、多份拷贝、分散保存、人手一份、统一更新、旧版销毁
      - 维护和变更管理：业务流程/信息系统/人员的变更、测试/演练/实战的详细记录和效果评估以及预案相应修订、预案定期评审和修订（至少每年一次）

GB/T 20988-2007

- 附录A （规范性附录） 灾难恢复能力等级划分
  - A.1 第1级 基本支持
  - A.2 第2级 备用场地支持
  - A.3 第3级 电子传输和部分设备支持
  - A.4 第4级 电子传输及完整设备支持
  - A.5 第5级 实时数据传输及完整设备支持
  - A.6 第6级 数据零丢失和远程集群支持

GB/T 20988-2007

- 附录A （规范性附录） 灾难恢复能力等级划分（续）
  - A.7 灾难恢复能力等级评定原则
    - 同时满足7个要素的相应要求
  - A.8 灾难备份中心的等级
    - 等级等于其可支持的灾难恢复最高等级

GB/T 20988-2007

- 附录B （资料性附录） 灾难恢复预案框架
  - B.1 目标和范围
  - B.2 组织和职责
  - B.3 联络与通讯
  - B.4 突发事件响应流程
    - B.4.1 事件通告
    - B.4.2 人员疏散
    - B.4.3 损害评估
    - B.4.4 灾难宣告

GB/T 20988-2007

- 附录B （资料性附录） 灾难恢复预案框架（续）
  - B.5 恢复及重续运行流程
    - B.5.1 恢复
    - B.5.2 重续运行
  - B.6 灾后重建和回退
  - B.7 预案的保障条件
  - B.8 预案附录

GB/T 20988-2007

- 附录C （资料性附录） 某行业RTO/RPO与灾难恢复能力等级的关系示例
  - C.1 RTO/RPO与灾难恢复能力等级的关系
    - 信息系统灾难恢复能力等级与恢复时间目标（RTO）和恢复点目标（RPO）具有一定的对应关系；
    - 各行业可根据行业特点和信息技术的应用情况制定相应的灾难恢复能力等级要求和指标体系。

第三部分 ISMS国家标准解读

- 3.1 国家标准化组织
- 3.2 正式发布的国家标准
- 3.3 报批中的国家标准
- **3.4 标准解读**
  - GB/T 22080-2008《信息技术 安全技术 信息安全管理体系 要求》
  - GB/T 22081-2008《信息技术 安全技术 信息安全管理实用规则》
  - GB/T 20984-2007《信息安全技术 信息安全风险评估规范》
  - GB/T 20988-2007《信息安全技术 信息系统灾难恢复规范》
  - **GB/Z 20985-2007《信息技术 安全技术 信息安全事件管理指南》**

GB/Z 20985-2007

- 标准名称
  - 中文：信息技术 安全技术 信息安全事件管理指南
  - 英文：Information technology – Security techniques – Information security incident management guide
- 标准号：GB/Z 20985-2007
- 中标分类：L80
- 采标情况：ISO/IEC TR 18044:2004,MOD

GB/Z 20985-2007

- 发布日期：2007-6-14
- 实施日期：2007-11-1
- 发布单位
  - 中华人民共和国国家质量监督检验检疫总局
  - 中国国家标准化管理委员会

GB/Z 20985-2007

- 标准简介
  - 该指导性技术文件描述了信息安全事件的管理过程，提供了规划和制定信息安全事件管理策略和方案的指南，给出了管理信息安全事件和开展后续工作的相关过程和规范。

GB/Z 20985-2007

- 标准结构
  - 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

GB/Z 20985-2007

- 标准结构（续）
  - 5 背景
  - 6 信息安全事件管理方案的益处及需要应对的关键问题
  - 7 规划和准备
  - 8 使用
  - 9 评审
  - 10 改进

GB/Z 20985-2007

- 标准结构（续）
  - 附录A（资料性附录）信息安全事态和事件报告单示例
  - 附录B（资料性附录）信息安全事件评估要点指南示例
  - 附录C（资料性附录）本指导性技术文件与ISO/IEC TR 18044:2004技术性差异及其原因
  - 参考文献

GB/Z 20985-2007

- 前言
  - [给出该指导性技术文件编制和管理相关的信息]
  - GB/Z 20985-2007修改采用ISO/IEC TR 18044:2004。
  - 鉴于ISO/IEC TR 18044:2004是技术报告，GB/Z 20985-2007作为指导性技术文件发布。
  - GB/Z 20985-2007对ISO/IEC TR 18044:2004最主要的修改是增加引用我国自主编制的GB/Z 20986-2007《信息安全技术 信息安全事件分类分级指南》，并对文本中的相关章节和附录进行了相应补充和修改。相关详情，参见附录C。

GB/Z 20985-2007

- 引言
  - [作为GB/Z 20985-2007的编制背景，简要阐述信息安全事件管理的必要性和工作内容]
  - 总会有信息安全事件发生，往往是意料之外的，甚至是未知的。
  - 在发生信息安全事件时，有序、有力、有效地采取应对措施，稳定局面，降低负面影响并尽快恢复系统是至关重要的。
  - 采用一种结构严谨、计划周全的方法来全程管理信息安全事件是十分必要的。

GB/Z 20985-2007

- 引言（续）
  - 全程管理：事前要做好规划和准备，事中要及时发现、报告、评估和判断并有效抑制和取证，事后要消除根源、恢复系统、总结经验和寻求改进，以及不论事件是否发生都要定期/应需评审和持续改进。
  - 全程活动：规划、准备、发现、报告、评估、判断、抑制、取证、根除、恢复、评审和改进的整个过程。
  - 持续改进：信息安全事件管理过程应是循环迭代的持续改进过程。

GB/Z 20985-2007

- 1 范围
  - [界定GB/Z 20985-2007的适用范围]
  - 内容范围
    - 信息安全事件管理的过程模型和过程中各阶段的步骤及其指南。
  - 对象范围
    - 信息安全管理者以及信息系统、服务和网络管理者。
    - 任何与信息安全事件相关或对信息安全事件管理感兴趣的人员。

GB/Z 20985-2007

- 2 规范性引用文件
  - [提供正文中所引用的相关标准或规范性文件的信息]
  - GB/T 19716-2005《信息技术　信息安全管理实用规则》（修改采用ISO/IEC 17799:2000）
  - GB/Z 20986-2007《信息安全技术　信息安全事件分类分级指南》
  - ISO/IEC 13335-1:2004《信息技术　安全技术　信息和通信技术安全管理　第1部分：信息和通信技术安全管理的概念和模型》

GB/Z 20985-2007

- 3 术语和定义
  - 业务持续性规划 business continuity planning
    - 业务持续性是组织业务层面的安全目标，其实现需要人财物等各方面的安全保障，其中信息安全保障是不可或缺的。
    - 在进行业务持续性规划时需要全面考虑包括信息安全要素在内的多方面要素以及要素之间的关系，以便形成一个全面、互补、协同的业务连续性的保障体系。
  - 信息安全事态 information security event
  - 信息安全事件 information security incident

GB/Z 20985-2007

- 3 术语和定义（续）
  - 信息安全事件响应组（ISIRT）Information Security Incident Response Team
    - ISIRT在信息安全事件响应中扮演着重要角色，但不是全部角色，需要各种相关人员的配合和支持。
    - ISIRT可以由一个或多个人组成。
    - ISIRT的组建方式可以是自建也可以是外包，这取决于组织的业务性质和安全策略。

GB/Z 20985-2007

- 4 缩略语
  - CERT 计算机应急响应组（Computer Emergency Response Team）
  - ISIRT 信息安全事件响应组（Information Security Incident Response Team）
  - CERT与ISIRT属于同类机构，只是名称不同而已。

GB/Z 20985-2007

- 5 背景
  - 5.1 目标
    - [明确信息安全事件管理的地位、方法和目标]
    - 信息安全事态的及时发现、有效处理（主要是报告）和准确判断（即确定是否属于信息安全事件）；
    - 信息安全事件的正确评估和恰当、有效的响应（包括最小化负面影响的安全措施）；
    - 事后的经验总结和改进（既有信息安全措施的改进，也有信息安全事件管理方案的改进）。

GB/Z 20985-2007

- 5 背景
  - 5.2 过程
    - [概述信息安全事件管理的过程]
    - 5.2.1 规划和准备（Plan and Prepare）
      - [概述第一阶段“规划和准备”的主要活动]
    - 5.2.2 使用（Use）
      - [概述第二阶段“使用”的主要活动]
    - 5.2.3 评审（Review）
      - [概述第三阶段“评审”的主要活动]
    - 5.2.4 改进（Improve）
      - [概述第四阶段“改进”的主要活动]

GB/Z 20985-2007

- 6 信息安全事件管理方案的益处及需要应对的关键问题
  - 6.1 信息安全事件管理方案的益处
    - [列举有效的信息安全事件管理方案所带来的益处]
    - 一、提高安全保障水平
    - 二、降低对业务的负面影响
    - 三、强化着重预防信息安全事件
    - 四、强化调查的优先顺序和证据
    - 五、有利于预算和资源合理利用
    - 六、改进风险分析和管理评审结果
    - 七、增强信息安全意识和提供培训计划材料
    - 八、为信息安全策略及相关文件的评审提供信息

GB/Z 20985-2007

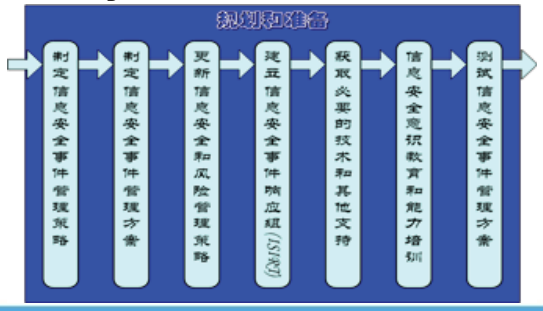
- 6 信息安全事件管理方案的益处及需要应对的关键问题
  - 6.2 关键问题
    - [阐述实现良好信息安全事件管理方案的关键问题]
    - 一、管理层的承诺
    - 二、安全意识
    - 三、法律法规
    - 四、运行效率和质量
    - 五、匿名性
    - 六、保密性
    - 七、可信运行
    - 八、系统化分类

GB/Z 20985-2007

- 7 规划和准备
  - [列出信息安全事件管理在规划和准备阶段的工作要点]
  - 信息安全事件管理策略和方案（包括相关规程）以及信息安全事态/事件报告单是开展信息安全事件管理工作的依据。
  - 信息安全事件管理的组织结构和人员是执行信息安全事件管理策略和方案的主体。
  - 信息安全意识、知识和技能的教育与培训是有效执行信息安全事件管理策略和方案的保障。

GB/Z 20985-2007

- 7 规划和准备（续）
  - 7.1 概述



GB/Z 20985-2007

- 7 规划和准备（续）
  - 7.2 信息安全事件管理策略
    - [阐明信息安全事件管理策略的目的、相关者、内容]
    - 目的
      - 信息安全事件管理的灵魂，为每一位合法访问组织的信息、信息系统及其支撑环境的人员提供应对信息安全事态/事件的指导原则和行为规范。

GB/Z 20985-2007

- 7 规划和准备（续）
  - 7.2 信息安全事件管理策略（续）
    - 要点
      - 形成文件，由组织的最高管理层来正式批准和发布，使其对组织的所有成员和合作伙伴可用；
      - 制定并实施相关的意识教育和技能培训计划；
      - 编制并下发相应的工作文件和模板。
    - 内容
      - a) 事前指导；b) 事发指导；c) 评估指导；d) 处理指导；e) 取证指导；f) 事后指导；g) 文件指导；h) 执行指导；i) 宣贯指导；j) 合规指导。

GB/Z 20985-2007

- 7 规划和准备（续）
  - 7.3 信息安全事件管理方案
    - [阐明信息安全事件管理方案的目的、相关者、内容、规程、测试]
    - 目的
      - 为参与信息安全事件管理的所有人员提供针对信息安全事态/事件所进行的发现、报告、评估、判断、抑制、取证、根除、恢复、总结、评审和改进等活动的指南文件，为这些活动给出有关责任分配、操作规程、工作表单、评估准则和支持工具等方面的详细说明。

GB/Z 20985-2007

- 7 规划和准备（续）
  - 7.3 信息安全事件管理方案（续）
    - 要点
      - 符合信息安全事件管理策略；
      - 根据事件或产品类型制定可操作的规程；
      - 形成经过检查的正式规程文件并便于使用；
      - 为每个规程文件指明其使用和管理的负责人员；
      - 对那些敏感的规程不对外公开。

GB/Z 20985-2007

- 7 规划和准备（续）
  - 7.4 信息安全和风险管理策略
    - [在信息安全和风险管理策略中包含信息安全事件管理的目的、内容]
    - 目的
      - 将信息安全事件管理策略融入信息安全和风险管理策略中，不论是在组织的总体层面，还是在具体的系统、网络和服务层面。

GB/Z 20985-2007

- 7 规划和准备（续）
  - 7.4 信息安全和风险管理策略（续）
    - 要点
      - 更新总体信息安全和风险管理策略以及具体系统、服务和网络的信息安全策略，使之体现信息安全事件管理方面的内容，以确保各项信息安全相关策略的一致性。

GB/Z 20985-2007

- 7 规划和准备（续）
  - 7.5 ISIRT的建立
    - [阐明ISIRT的目的、规模、结构、成员、权限、与组织其他部门的关系、与外部方的关系]
    - 目的
      - 为信息安全事件处理（包括评估、判断、抑制、取证、根除、恢复、总结、评审和改进）信息安全事件提供合格的人员和有效的组织。

GB/Z 20985-2007

- 7 规划和准备（续）
  - 7.5 ISIRT的建立（续）
    - 要点
      - 与组织的规模和结构相适应；
      - 选用合格的专业人员和业务人员；
      - 明确ISIRT管理者和成员的权利和职责；
      - 明确与组织其他部门的关系；
      - 与外部方建立适当关系；
      - 确保可以随时与ISIRT成员联系；
      - 具备协调、专业、应对、预防和外联能力。

GB/Z 20985-2007

- 7 规划和准备（续）
  - 7.6 技术和其他支持
    - [阐述信息安全事件管理的技术手段和其他支持]
    - 目的
      - 及时、有效地应对信息安全事件。
    - 要点
      - 认真挑选、正确实施和定期测试所有技术手段；
      - 保持响应信息安全事件的任何技术手段具有一定独立性，避免在主体信息系统、服务或网络上运行，可能时做到完全独立。

GB/Z 20985-2007

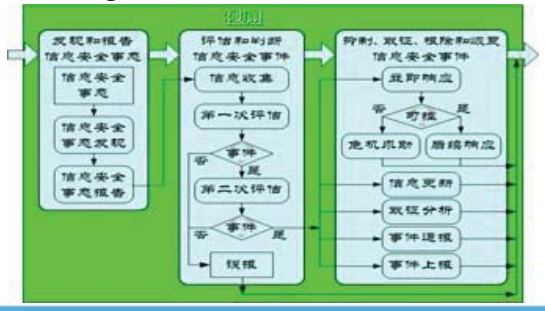
- 7 规划和准备（续）
  - 7.7 意识和培训
    - [阐述信息安全事件管理的意识教育和技能培训]
    - 目的
      - 得到组织内有适当信息安全意识并经过培训的人员支持。

GB/Z 20985-2007

- 7 规划和准备（续）
  - 7.7 意识和培训（续）
    - 要点
      - 作为总体信息安全意识教育和能力培训计划的必要组成部分，将信息安全事件管理灌输给所有相关人员；
      - 根据参与信息安全事件管理方案的方式、频度和重要程度的不同，进行不同级别的培训；
      - 培训内容得到运行支持组、ISIRT成员以及信息安全相关人员的具体演练和测试；
      - 信息安全事件管理方案开始运行之前，所有相关人员熟悉自己的角色和职责，并有能力完成被赋予的任务。

GB/Z 20985-2007

- 8 使用
  - 8.1 概述



GB/Z 20985-2007

- 8 使用（续）
  - 8.2 关键过程的概述
    - 发现和报告信息安全事态。
    - 收集信息，评估和判断（包括运行支持组的第一次和ISIRT的第二次）是否属于信息安全事件。
    - 判断信息安全事件是否处于ISIRT的可控范围：
      - 如果可控，则ISIRT继续实施后续响应措施；
      - 否则，启动“危机求助”行动（例如，机房发生重大火灾时，求助消防部门）。
    - 上报高层管理。
    - 记录所有活动。
    - 获取和保管法律有效证据。
    - 更新信息安全事态/事件数据库。

GB/Z 20985-2007

- 8 使用（续）
  - 8.3 发现和报告
    - [阐述信息安全事态/事件的发现和报告]
    - 手段
      - 通过人工或自动方式发现信息安全事态。
      - 填写和提交信息安全事态报告单。

GB/Z 20985-2007

- 8 使用（续）
  - 8.3 发现和报告（续）
    - 要点
      - 在第一时间按照事先规定的报告规程（包括职责、内容、流程和途径等）进行报告；
      - 尽量使用叙述性文字和当时可用的其他信息完成信息安全事态报告单，必要时与其所在部门管理者取得联系；
      - 报告单最好采用电子格式，并且以安全的方式发送；
      - 填写信息安全事态报告单时，不仅力求准确性而且及时性；
      - 报告途径有备用方式，以备在默认电子报告机制出现安全问题或安全隐患时使用。

GB/Z 20985-2007

- 8 使用（续）
  - 8.4 事态/事件评估和决策
    - [阐述信息安全事态/事件的第一次和第二次评估与判断]
    - 步骤
      - 运行支持组进行第一次评估并作出初始判定。
      - ISIRT进行第二次评估并作出最终判定。

GB/Z 20985-2007

- 8 使用（续）
  - 8.4 事态/事件评估和决策（续）
    - 要点
      - 将信息安全事态报告单填写完毕；
      - 尽可能地将信息安全事件报告单填写完整；
      - 当被确定为重大信息安全事件时，直接通知ISIRT管理者；
      - 如果事件的严重性到达危机程度，通知业务连续性管理者和高层管理。

GB/Z 20985-2007

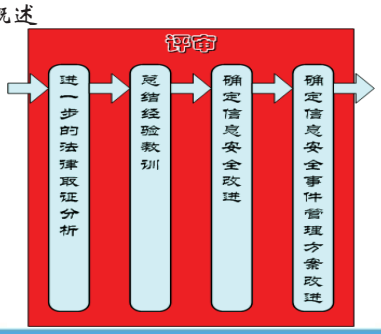
- 8 使用（续）
  - 8.5 响应
    - [阐述立即响应及其措施、事件信息的更新、进一步的响应活动、如何判断和处理事件是否可控、后续响应措施、“危机求助”行动、法律取证分析、事件通报、事件上报、事件响应的活动日志和变更控制]

GB/Z 20985-2007

- 8 使用（续）
  - 8.5 响应（续）
    - 步骤
      - 一旦判定所报确属信息安全事件，ISIRT作出立即响应，包括采取抑制事件发展、根除事件原因、更新事件信息、法律取证分析、通报相关人员和上报高层管理。
      - 判断信息安全事件是否处于控制之下。如果已经处于控制之下，则可以采取后续响应，包括将受影响的信息系统、服务和网络恢复到正常运行，将响应结果的细节记录到信息安全事件报告单中并存入信息安全事态/事件数据库等；否则就应启动“危机救助”行动，包括业务连续性计划，以及防火、防洪和防爆等应急预案的启用。

GB/Z 20985-2007

- 9 评审
  - 9.1 概述



GB/Z 20985-2007

- 9 评审
  - 9.2 进一步的法律取证分析
    - [阐述进一步的法律取证分析]
    - 要点
      - 信息安全事件被解决后，可能依然需要进行法律取证分析以进一步确定证据。

GB/Z 20985-2007

- 9 评审
  - 9.3 经验教训
    - [阐述如何总结经验教训]
    - 要点
      - 一旦信息安全事件的处理工作结束，迅速从信息安全事件中总结经验教训，提出改进建议并立即付诸实施。
    - 方面
      - 信息安全策略、规程和控制措施。
      - 信息安全事件管理方案及其过程、信息安全事态/事件报告单及其数据库。
    - 方法
      - 分析事件的发展趋势和发生模式；
      - 对信息系统、服务和网络进行全面的脆弱性评估和安全测试。

GB/Z 20985-2007

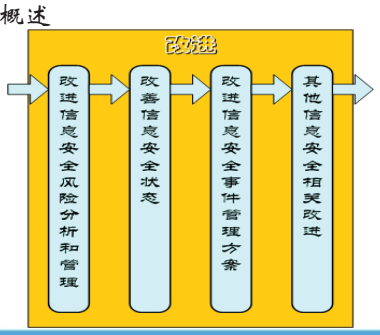
- 9 评审
  - 9.4 确定安全改进
    - [阐述如何确定信息安全的改进]
    - 要点
      - 根据经验教训的总结结果，确定全新或更改的信息安全策略、规程和控制措施（技术的或非技术的）。
      - 尽可能立即实施改进建议和相关措施；但因财务或运作等方面原因不能马上做到时，作为组织的长期目标逐步实行。

GB/Z 20985-2007

- 9 评审
  - 9.5 确定方案改进
    - [阐述如何确定信息安全事件管理方案的改进]
    - 要点
      - 尽快就本次应对信息安全事件的全部过程和整体效果进行评审和评估，并将所得到的经验教训和改进建议反馈到信息安全事件管理方案中。
      - 将评审和评估结果形成正式文件存档。

GB/Z 20985-2007

- 10 改进
  - 10.1 概述



GB/Z 20985-2007

- 10 改进
  - 10.2 安全风险分析和管理改进
    - [阐述信息安全风险分析和管理的改进]
    - 要点
      - 根据信息安全事件的严重程度和影响，考虑新的威胁和脆弱性来评估信息安全风险分析和管理评审的结果。
      - 作为完成信息安全风险分析和管理评审更新的后续工作，引入更新的或全新的防护措施（必要时）。

GB/Z 20985-2007

- 10 改进
  - 10.3 改善安全状况
    - [阐述信息安全状态的改善]
    - 要点
      - 执行评审阶段提出的有关信息安全的改进建议，包括修订信息安全策略和规程，实施新的信息安全控制措施或更改现有信息安全控制措施等。
      - 通过各种沟通渠道迅速将因改进引起的变更通知到所有相关人员。

GB/Z 20985-2007

- 10 改进
  - 10.4 改进方案
    - [阐述信息安全事件管理方案的改进]
    - 要点
      - 在认真评审和判断评审阶段提出的有关信息安全事件管理方案的改进建议之后，修订信息安全事件管理方案，包括更改信息安全事件管理过程、规程和信息安全事态/事件报告单等。
      - 上述任何更改都应经过全面检查和测试后方可投入使用。

GB/Z 20985-2007

- 10 改进
  - 10.5 其他改进
    - [阐述其他信息安全的相关改进]
    - 要求
      - 执行评审阶段确定其他信息安全相关的改进建议，如信息安全标准和技术的变更，IT硬件和软件配置的变更等。

GB/Z 20985-2007

- 附录A（资料性附录）信息安全事态和事件报告单示例
  - [给出信息安全事态和事件报告单模版及其填写说明]
  - 信息安全事态报告单内容
    - 信息安全事态的基本信息；
    - 报告人的详细情况；
    - 信息安全事态的描述；
    - 信息安全事态的细节。

GB/Z 20985-2007

- 附录A （资料性附录） 信息安全事态和事件报告单示例（续）
  - 信息安全事件报告单内容
    - 信息安全事件的基本信息
    - 运行支持组成员的详细情况
    - ISIRT成员的详细情况
    - 信息安全事件的描述
    - 信息安全事件的细节
    - 信息安全事件的类型（参照GB/Z 20986-2007《信息安全技术　信息安全事件分类分级指南》）
    - 受影响的资产
    - 信息安全事件对业务的负面影响
    - 信息安全事件的全部恢复成本

GB/Z 20985-2007

- 附录A （资料性附录） 信息安全事态和事件报告单示例（续）
  - 信息安全事件报告单内容（续）
    - 信息安全事件的解决情况
    - 涉及的人员/作恶者
    - 作恶者的描述
    - 实际的或察觉的动机
    - 已采取的解决事件措施
    - 计划采取的解决事件措施
    - 未完成的措施
    - 事件后果的结论
    - 被通知的个人/实体
    - 涉及的个人（签字）

GB/Z 20985-2007

- 附录B （资料性附录） 信息安全事件评估要点指南示例
  - [给出对信息安全事件所导致的后果进行分类和评估的要点指南]
  - 信息安全事件的后果类别
    - 财务损失
    - 利益丧失
    - 个人伤害
    - 法规触犯
    - 运行妨碍
    - 声誉损害

GB/Z 20985-2007

- 附录B （资料性附录） 信息安全事件评估要点指南示例（续）
  - 将后果的影响程度由低到高分为1-10十个级别，且从信息安全事件的以下方面考虑：
    - 未授权泄露信息——保密性受损；
    - 未授权修改信息——完整性受损；
    - 抵赖信息——抗抵赖性受损；
    - 信息和/或服务不可用——可用性受损；
    - 信息和/或服务遭受破坏——完整性和可用性受损。

GB/Z 20985-2007

- 附录C （资料性附录） 本指导性技术文件与ISO/IEC TR 18044:2004技术性差异及其原因
  - [列出GB/Z 20985-2007与ISO/IEC TR 18044:2004的技术性差异及其原因]
  - 最主要的技术性差异
    - 增加引用我国自主编制的GB/Z 20986-2007《信息安全技术　信息安全事件分类分级指南》，并对文本中的相关章节和附录进行了相应补充和修改。

谢谢！