《信息技术 安全技术 信息安全管理实用规则》解读

电子四所 上官晓丽

2008年12月1日

对应标准编号及其与国际标准的关系

- 国标编号：GB/T 22081:2008

- 与国际标准的关系：

  等同采用ISO/IEC 27002:2005，“Information technology-Security techniques-Code of practice for information security management”

本标准与GB/T 22080:2008的关系

- GB/T 22080:2008《信息技术 安全技术 信息安全管理体系 要求》
- GB/T 22080:2008：阐述组织建立、实施、运行、监视、评审、保持与改进其ISMS应满足的要求；
- GB/T 22080:2008的规范性附录A：直接引用本标准，即与本标准第5到15章中关于控制目标和控制措施的描述保持一致；
- 本标准：提供了控制目标和控制措施集合，是信息安全管理最佳实践的实施建议和指南。

内容大纲

- 国际标准ISO/IEC 27002:2005背景简介
- 国家标准GB/T 22081:2008研究及编制背景介绍
- GB/T 22081:2008内容解读

一、国际标准ISO/IEC 27002:2005背景简介

国际ISO/IEC 27000系列标准的现状

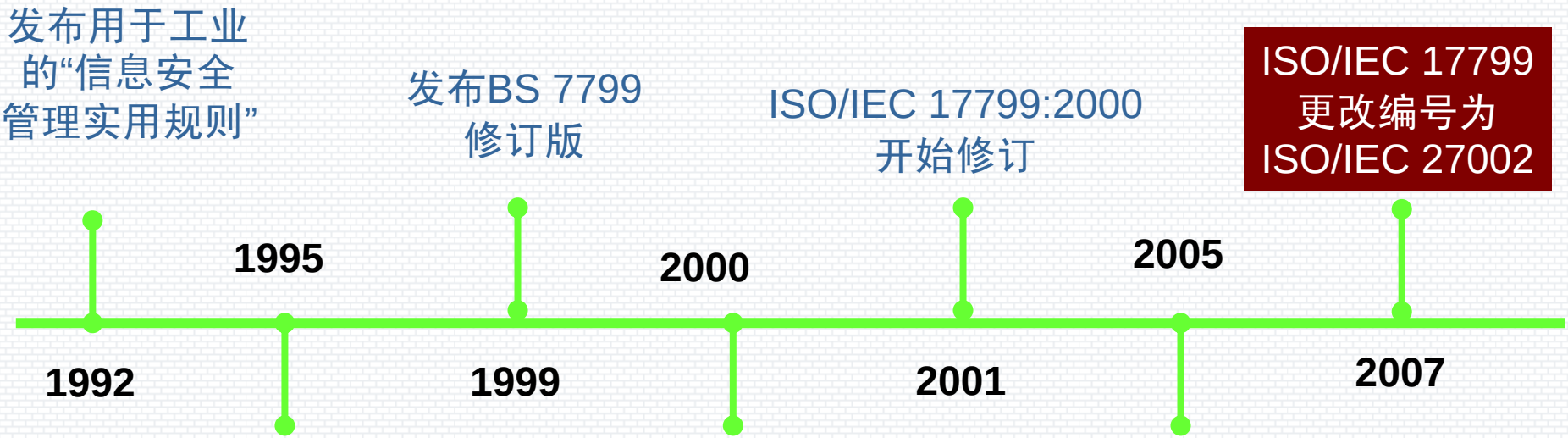
标准编号	名称	状态
ISO/IEC 27000	信息技术 安全技术 信息安全管理体系 基础和词汇	制定中
ISO/IEC 27001:2005	信息技术 安全技术 信息安全管理体系 要求	已发布
ISO/IEC 27002:2005	信息技术 安全技术 信息安全管理实用规则	已发布
ISO/IEC 27003	信息技术 安全技术 信息安全管理体系实施指南	制定中
ISO/IEC 27004	信息技术 安全技术 信息安全管理 测量	制定中
ISO/IEC 27005:2008	信息技术 安全技术 信息安全风险管理	已发布
ISO/IEC 27006:2007	信息技术 安全技术 信息安全管理体系审核认证机构的要求	已发布
ISO/IEC 27007	信息技术 安全技术 信息安全管理体系 审核指南	制定中
……		

国际ISO/IEC 27000系列标准的现状

- 此外，ISMS监视和评审、ISMS持续改进等标准的制定也被纳入了国际ISMS标准族研究的考虑范围之内。

- 在与其它技术委员会沟通、协调的基础上，国际ISMS路线图逐渐将其它行业的ISMS标准或指南纳入了ISO/IEC 27000标准系列，像电信、金融、健康等方面的信息安全管理标准和指南。

ISO/IEC 27002:2005的发展历程



二、国家标准GB/T 22081:2008研究及编制背景简介

研究背景信息

- 2002年，在全国信安标委WG7工作组的组织下，启动了ISO/IEC 17799:2000的转标工作。2005年，作为国家标准发布，即GB/T 19716:2005《信息技术 信息安全管理实用规则》。
- 随着国际ISO/IEC 27000标准族研究的全面推进，以及它所带来的对国内外企业市场竞争的影响，为了能与国际信息安全管理体系认证形势相衔接，并给国内企业和机构的信息安全管理工作提供参考，在长期跟踪研究国际信息安全管理体系标准族发展动态的同时，2006年，正式启动对GB/T 19716:2005的修订工作。2008年，GB/T 22081:2008《信息技术 安全技术 信息安全管理实用规则》发布。

GB/T 22081:2008的编制原则

- 在参考国际标准ISO/IEC 17799：2000 《信息技术 信息安全管理实用规则》制定GB/T19716：2005时，。在其中12.1.6中增加了“a)使用国家主管部门审批的密码算法和密码产品”内容。修改采用了ISO/IEC 17799：2000。
- 而ISO/IEC 27002：2005（原标准号为ISO/IEC 17799：2005）相比ISO/IEC 17799：2000而言，其内容和结构均发生了较大变化，因此在本次修订工作中，考虑到信息安全管理体系标准的完整性、科学性和严谨性，经与国家密码管理局、国家保密局等相关职能部门及工作组成员单位的积极沟通，达成一致，等同采用了ISO/IEC 27002：2005。

GB/T 22081:2008的编制过程

- 2005年，跟踪国际标准17799的发展动态，组织专家等同转化，多次研讨；
- 2006年，作为原国信办组织的“信息安全管理标准应用试点”的基础标准之一，在税务、证券等重要信息系统和北京市、上海市、武汉钢铁集团公司等单位进行试用；
- 2007年2月-3月，就标准的编制原则、标准的编制进度安排以及标准编写组成员单位组成等问题组织专家进行讨论和研究，修改完善文本，形成标准征求意见稿；
- 2007年3月30日，邀请重要应用信息系统部门相关领导以及全国信安标委的部分专家在北京召开征求意见会；
- 2007年3月至8月，对反馈意见进行汇总和处理，进一步修改完善标准文本，形成标准送审稿；
- 2007年9月6日，信安标委秘书处在北京召开送审稿专家审定会，与会专家就送审稿提出了修改意见和建议，希望编制组根据专家意见进行修改后尽快形成报批稿。

三、 GB/T 22081:2008内容解读

GB/T 22081:2008的内容

引言
第一章 范围
第二章 术语和定义
第三章 本标准的结构
第四章 风险评估和处理
第五章 安全方针
第六章 信息安全组织
第七章 资产管理
第八章 人力资源安全
第九章 物理和环境安全
第十章 通信和操作管理
第十一章 访问控制
第十二章 信息系统获取、开发和维护
第十三章 信息安全事件管理
第十四章 业务连续性管理
第十五章 符合性

引言

0.1什么是信息安全？
0.2为什么需要信息安全？
0.3如何建立安全要求？
0.4评估安全风险
0.5选择控制措施
0.6信息安全起点
0.7关键的成功因素
0.8开发组织自己的指南

引言：0.1什么是信息安全？

- 信息是一种资产，对组织的业务运行至关重要；
- 组织业务环境互连的日益增加，使得信息面临的威胁和风险越来越多、越来越复杂；
- 信息的存在形式多样化；

- 信息安全是保护信息免受各种威胁的损害，确保业务连续性，使业务风险最小化，投资回报和商业机遇最大化；【本标准的目的】

引言：0.2为什么需要信息安全？

- 定义、实现、保持和改进信息安全，对于组织保持业务竞争优势、现金周转、赢利、守法和商业形象至关重要；
- 来自各方面的安全威胁 ：计算机辅助欺诈、间谍活动、恶意破坏、毁坏行为、火灾或洪水。诸如恶意代码、计算机黑客捣乱和拒绝服务攻击等已经十分普遍；
- 信息安全对于公共和专用两部分的业务以及保护关键基础设施非常重要；
- 通过技术手段可获得的安全是有限的，组织应通过适当的管理和规程提高安全。

引言：0.3如何建立安全要求？

- 在考虑组织整体业务战略和目标的情况下，通过风险评估所确定的安全要求；
- 组织、贸易伙伴、合同方和服务提供者必须满足的法律、法规、规章和合同要求，以及他们的社会文化环境；
- 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。

引言：0.4评估安全风险

- 安全要求是通过对安全风险的系统评估来确定的；
- 风险评估的结果有助于指导和决定适当的管理行为、确定风险的优先级，以及实现所选的用以防范风险的控制措施；
- 风险评估应定期进行，以应对可能影响风险评估结果的任何变化。

引言：0.5选择控制措施

- 确定安全要求和风险，并作出风险处理决定之后，应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；
- 安全控制措施的选择应考虑组织的风险接受准则、风险处理决定和风险管理方法，并且要遵守所有相关的国家和国际法律法规；
- 控制措施可以从本标准中或其他控制措施集合中选择。需要时，可以设计新的控制措施以满足特定需求；

引言：0.6信息安全起点

组织应根据适用的法律要求，考虑下列适当的控制措施：

- 数据保护和个人信息的隐私（见15.1.4）；
- 保护组织的记录（见15.1.3）；
- 知识产权（见15.1.2）。

作为信息安全的常用惯例，组织应考虑的控制措施包括：

- 信息安全方针文件（见5.1.1）；
- 信息安全职责的分配（见6.1.3）；
- 信息安全意识、教育和培训（见8.2.2）；
- 应用中的正确处理（见12.2）；
- 技术脆弱性管理（见12.6）；
- 业务连续性管理（见14）；
- 信息安全事件和改进管理（见13.2）。

引言：0.7关键的成功因素

- 反映业务目标的信息安全方针、目标以及活动；
- 和组织文化保持一致的实现、保持、监视和改进信息安全的方法和框架；
- 来自所有级别管理者的可视化的支持和承诺；
- 正确理解信息安全要求、风险评估和风险管理；
- 向所有管理人员、员工和其它方传达有效的信息安全知识以使他们具备安全意识；
- 向所有管理人员、员工和其它方分发关于信息安全方针和标准的指导意见；
- 提供资金以支持信息安全管理活动；
- 提供适当的意识、培训和教育；
- 建立一个有效的信息安全事件管理过程；
- 实现一个测量系统，它可用来评价信息安全管理的执行情况和反馈的改进建议。

引言：0.8开发组织自己的指南

- 本实用规则是一个组织开发其详细指南的基础；
- 对一个组织来说，本实用规则中的控制措施和指南并非全部适用；
- 组织需要根据自身的实际需求，选择其他的、本标准中未包括的控制措施和指南。

1、范围

- 本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。本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指导。
- 本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。
- 本标准可作为建立组织的安全准则和有效安全管理惯例的实用指南，并有利于在组织间的活动中建立信心。

2、术语和定义

2.1 资产 asset
2.2 控制措施 control
2.3 指南 guideline
2.4 信息处理设施 information processing facilities
2.5 信息安全 information security
2.6 信息安全事态 information security event
2.7 信息安全事件 information security incident
2.8 方针 policy
2.9 风险 risk
2.10 风险分析 risk analysis
2.11 风险评估 risk assessment
2.12 风险评价 risk evaluation
2.13 风险管理 risk management
2.14 风险处理 risk treatment
2.15 第三方 third party
2.16 威胁 threat
2.17 脆弱性 vulnerability

2.1 资产 asset

- 对组织有价值的任何东西[ISO/IEC 13335-1:2004]。

2.2 控制措施 control

管理风险的方法，包括策略、规程、指南、惯例或组织结构。它们可以是行政、技术、管理、法律等方面的。

术语和定义

2.3 指南 guideline： 阐明应做什么和怎么做以达到方针策略中制定的目标的描述。[ISO/IEC TR 13335-1：2004]

2.4 信息处理设施 information processing facilities：任何信息处理系统、服务或基础设施，或放置它们的场所 。

2.5 信息安全 information security:保持信息的保密性、完整性、可用性；另外也可包括例如真实性、可核查性、不可否认性和可靠性等。

2.6 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[GB/Z 20985-2007]。

2.7 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[GB/Z 20985-2007]。

2.8 方针 policy

管理者正式发布的总的宗旨和方向 。

风险管理相关术语和定义：引自ISO/IEC Guide 73：2002

2.9 风险 risk：事态的概率及其结果的组合。

2.10 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。

2.11 风险评估 risk assessment：风险分析和风险评价的整个过程。

2.12 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。

2.13 风险管理 risk management：指导和控制一个组织相关风险的协调活动。

注：风险管理一般包括风险评估、风险处置、风险接受和风险沟通。

2.14 风险处置 risk treatment：选择并且执行措施来更改风险的过程。

2.15 第三方 third party

就所涉及的问题被公认为是独立于有关各方的个人或机构[ISO Guide 2：1996]。

2.16 威胁 threat

可能导致对系统或组织的损害的不期望事件发生的潜在原因[ISO/IEC TR 13335-1：2004]。

2.17 脆弱性 vulnerability

可能会被一个或多个威胁所利用的资产或一组资产的弱点[ISO/IEC TR 13335-1：2004]。

3、本标准的结构之3.1 章节

引言

- 范围
- 术语和定义
- 本标准的结构
- 风险评估和处理
- 安全方针
- 信息安全组织
- 资产管理
- 人力资源安全
- 物理和环境安全
- 通信和操作管理
- 访问控制
- 信息系统获取、开发和维护
- 信息安全事件管理
- 业务连续性管理
- 符合性

11个安全控制措施的章节（共含有39个主要安全类别）

3、本标准的结构之3.2 主要安全类别

每个主要安全类别（main security category）包括：

- 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。

主要安全类别的描述示例

例如：

7.2 信息分类

目标：确保信息受到适当级别的保护。

……

7.2.1 分类指南

控制措施

……

实施指南

……

其他信息

……

7.2.2 信息的标记和处理

……

控制措施的描述结构

控制措施

定义满足控制目标的特定的控制措施的陈述。

实施指南

为支持控制措施的实施和满足控制目标，提供更详细的信息。本指南的某些内容可能不适用于所有情况，所以其他实现控制措施的方法可能更为合适。

其它信息

提供需要考虑的进一步的信息，例如考虑法律相关注意事项和引用其他标准。

控制措施的描述示例:7.2.2 信息的标记和处理

控制措施

应按照组织所采纳的分类机制建立和实施一组合适的信息标记和处理程序。

实施指南

信息标记的程序需要涵盖物理和电子格式的信息资产。

包含分类为敏感或关键信息的系统输出应在该输出中携带合适的分类标记。该标记要根据7.2.1中所建立的规则反映出分类。待考虑的项目包括打印报告、屏幕显示、记录介质（例如磁带、磁盘、CD）、电子消息和文件传送。

对每种分类级别，要定义包括安全处理、储存、传输、删除、销毁的处理程序。还要包括一系列任何安全相关事件的监督和记录程序。

涉及信息共享的与其他组织的协议应包括识别信息分类和解释其他组织分类标记的程序。

其它信息

分类信息的标记和安全处理是信息共享的一个关键要求。物理标记是常用的标记形式。然而，某些信息资产（诸如电子形式的文件等）不能做物理标记，而需要使用电子标记手段。例如，通知标记可在屏幕上显示出来。当标记不适用时，可能需要应用信息分类指定的其他方式，例如通过程序或元数据。

4、风险评估和处理

- 评估安全风险
  风险评估包括：风险分析和风险评价；
  应定期进行风险评估；
  应有一个清晰定义的信息安全风险评估的范围；
- 处理安全风险
  首先要确定组织的风险接受准则；
  对风险评估识别出的每个风险，必须作出风险处理的决定：降低风险、接受风险、规避风险、转移风险；

注：关于风险评估和管理的详细信息，可参见ISO/IEC 27005：2008《信息技术 安全技术 信息安全风险管理》

5、安全方针

5.1信息安全方针

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。

管理者应根据业务目标制定清晰的方针指导，并通过在整个组织中颁布和维护信息安全方针来表明对信息安全的支持和承诺。

- 5.1.1信息安全方针文件

  信息安全方针文件应由管理者批准、发布并传达给所有员工和外部相关方。

- 5.1.2信息安全方针的评审

  应按计划的时间间隔或当重大变化发生时进行信息安全方针评审，以确保它持续的适宜性、充分性和有效性。

6、信息安全组织

- 6.1 内部组织
  目标：在组织内管理信息安全。

- 8个控制措施：
  信息安全的管理承诺
  信息安全协调
  信息安全职责的分配
  信息处理设施的授权过程
  保密性协议
  与政府部门的联系
  与特定利益集团的联系
  信息安全的独立评审

- 6.2 外部各方
  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。

- 3个控制措施：
  与外部各方相关风险的识别
  处理与顾客有关的安全问题
  处理第三方协议中的安全问题

7、资产管理

- 7.1 对资产负责
  目标：实现和保持对组织资产的适当保护。

- 3个控制措施：
  7.1.1资产清单
  7.1.2资产责任人
  7.1.3资产的合格使用

- 7.2 信息分类
  目标：确保信息受到适当级别的保护。

- 2个控制措施：
  7.2.1分类指南
  7.2.2信息的标记和处理

8、人力资源安全之8.1 任用之前

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。

- 8.1.1角色和职责
  雇员、承包方人员和第三方人员的安全角色和职责应按照组织的信息安全方针定义并形成文件。
- 8.1.2审查
  关于所有任用的候选者、承包方人员和第三方人员的背景验证检查应按照相关法律法规、道德规范和对应的业务要求、被访问信息的类别和察觉的风险来执行。
- 8.1.3任用条款和条件
  作为他们合同义务的一部分，雇员、承包方人员和第三方人员应同意并签署他们的任用合同的条款和条件，这些条款和条件要声明他们和组织的信息安全职责。

8、人力资源安全之8.2任用中

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，以减少人为过失的风险。

- 8.2.1管理职责
  管理者应要求雇员、承包方人员和第三方人员按照组织已建立的方针策略和程序对安全尽心尽力。
- 8.2.2信息安全意识、教育和培训
  组织的所有雇员，适当时，包括承包方人员和第三方人员，应受到与其工作职能相关的适当的意识培训和组织方针策略及程序的定期更新培训。
- 8.2.3纪律处理过程
  对于安全违规的雇员，应有一个正式的纪律处理过程。

8、人力资源安全之8.3任用的终止或变化

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。

- 8.3.1终止职责
  任用终止或任用变化的职责应清晰的定义和分配。
- 8.3.2资产的归还
  所有的雇员、承包方人员和第三方人员在终止任用、合同或协议时，应归还他们使用的所有组织资产。
- 8.3.3撤销访问权
  所有雇员、承包方人员和第三方人员对信息和信息处理设施的访问权应在任用、合同或协议终止时删除，或在变化时调整。

9、物理和环境安全

- 9.1 安全区域
  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。

- 6个控制措施：
  物理安全边界
  物理入口控制
  办公室、房间和设施的安全保护
  外部和环境威胁的安全防护
  在安全区域工作
  公共访问、交接区安全

- 9.2 设备安全
  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。

- 7个控制措施：
  设备安置和保护
  支持性设施
  布缆安全
  设备维护
  组织场所外的设备安全
  设备的安全处置和再利用
  资产的移动

10、通信和操作管理

- 10.1操作程序和职责
- 10.2第三方服务交付管理
- 10.3系统规划和验收
- 10.4防范恶意和移动代码
- 10.5备份
- 10.6网络安全管理
- 10.7介质处置
- 10.8信息的交换
- 10.9电子商务服务
- 10.10监视

10.1 操作程序和职责

目标：确保正确、安全的操作信息处理设施。

- 文件化的操作程序
  操作程序应形成文件、保持并对所有需要的用户可用。
- 变更管理
  对信息处理设施和系统的变更应加以控制。
- 责任分割
  各类责任及职责范围应加以分割，以降低未授权或无意识的修改或者不当使用组织资产的机会。
- 开发、测试和运行设施分离
  开发、测试和运行设施应分离，以减少未授权访问或改变运行系统的风险。

10.2 第三方服务交付管理

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。

- 服务交付
  应确保第三方实施、运行和保持包含在第三方服务交付协议中的安全控制措施、服务定义和交付水准。
- 第三方服务的监视和评审
  应定期监视和评审由第三方提供的服务、报告和记录，审核也应定期执行。
- 第三方服务的变更管理
  应管理服务提供的变更，包括保持和改进现有的信息安全方针策略、程序和控制措施，要考虑业务系统和涉及过程的关键程度及风险的再评估。

10.3系统规划和验收

目标：将系统失效的风险降至最小。

- 容量管理
  资源的使用应加以监视、调整，并应作出对于未来容量要求的预测，以确保拥有所需的系统性能。
- 系统验收
  应建立对新信息系统、升级及新版本的验收准则，并且在开发中和验收前对系统进行适当的测试。

10.4 防范恶意和移动代码

目标：保护软件和信息的完整性。

- 控制恶意代码
  应实施恶意代码的监测、预防和恢复的控制措施，以及适当的提高用户安全意识的程序。
- 控制移动代码
  当授权使用移动代码时，其配置应确保授权的移动代码按照清晰定义的安全策略运行，应阻止执行未授权的移动代码。

10.5 备份

目标：保持信息和信息处理设施的完整性及可用性。

- 信息备份
  应按照已设的备份策略，定期备份和测试信息和软件。

10.6 网络安全管理

目标：确保网络中信息的安全性并保护支持性的基础设施。

- 网络控制
  应充分管理和控制网络，以防止威胁的发生，维护系统和使用网络的应用程序的安全，包括传输中的信息。
- 网络服务安全
  安全特性、服务级别以及所有网络服务的管理要求应予以确定并包括在所有网络服务协议中，无论这些服务是由内部提供的还是外包的。

10.7介质处置

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。

- 可移动介质的管理
  应有适当的可移动介质的管理程序。
- 介质的处置
  不再需要的介质，应使用正式的程序可靠并安全地处置。
- 信息处理程序
  应建立信息的处理及存储程序，以防止信息的未授权的泄漏或不当使用。
- 系统文件安全
  应保护系统文件以防止未授权的访问。

10.8 信息的交换

目标：保持组织内信息和软件交换及与外部组织信息和软件交换的安全。

- 信息交换策略和程序
  应有正式的交换策略、程序和控制措施，以保护通过使用各种类型通信设施的信息交换。
- 交换协议
  应建立组织与外部团体交换信息和软件的协议。
- 运输中的物理介质
  包含信息的介质在组织的物理边界以外运送时，应防止未授权的访问、不当使用或毁坏。
- 电子消息发送
  包含在电子消息发送中的信息应给予适当的保护。
- 业务信息系统
  应建立和实施策略和程序以保护与业务信息系统互联的信息。

10.9 电子商务服务

目标：确保电子商务服务的安全及其安全使用。

- 电子商务
  包含在使用公共网络的电子商务中的信息应受保护，以防止欺诈活动、合同争议和未授权的泄露和修改。
- 在线交易
  包含在在线交易中的信息应受保护，以防止不完全传输、错误路由、未授权的消息篡改、未授权的泄露、未授权的消息复制或重放。
- 公共可用信息
  在公共可用系统中可用信息的完整性应受保护，以防止未授权的修改。

10.10 监视

目标：检测未经授权的信息处理活动。

- 审计日志
  应产生记录用户活动、异常和信息安全事件的审计日志，并要保持一个已设的周期以支持将来的调查和访问控制监视。
- 监视系统的使用
  应建立信息处理设施的监视使用程序，监视活动的结果要经常评审。
- 日志信息的保护
  记录日志的设施和日志信息应加以保护，以防止篡改和未授权的访问。
- 管理员和操作员日志
  系统管理员和系统操作员的活动应记入日志。
- 故障日志
  故障应被记录、分析，并采取适当的措施。
- 时钟同步
  一个组织或安全域内的所有相关信息处理设施的时钟应使用已设的精确时间源进行同步。

11、访问控制

- 11.1访问控制的业务要求
- 11.2用户访问管理
- 11.3用户职责
- 11.4网络访问控制
- 11.5操作系统访问控制
- 11.6应用和信息访问控制
- 11.7移动计算和远程工作

11.1访问控制的业务要求

目标：控制对信息的访问。

- 访问控制策略
  访问控制策略应建立、形成文件，并基于业务和访问的安全要求进行评审。

11.2 用户访问管理

- 目标：确保授权用户访问信息系统，并防止未授权的访问。

- 用户注册
  应有正式的用户注册及注销程序，来授权和撤销对所有信息系统及服务的访问。
- 特殊权限管理
  应限制和控制特殊权限的分配及使用。
- 用户口令管理
  应通过正式的管理过程控制口令的分配。
- 用户访问权的复查
  管理者应定期使用正式过程对用户的访问权进行复查。

11.3 用户职责

- 目标：防止未授权用户对信息和信息处理设施的访问、危害或窃取。

- 口令使用
  应要求用户在选择及使用口令时，遵循良好的安全习惯。

- 无人值守的用户设备
  用户应确保无人值守的用户设备有适当的保护。

- 清空桌面和屏幕策略
  应采取清空桌面上文件、可移动存储介质的策略和清空信息处理设施屏幕的策略。

11.4网络访问控制

- 目标：防止对网络服务的未授权访问。

- 使用网络服务的策略
  用户应仅能访问已获专门授权使用的服务。
- 外部连接的用户鉴别
  应使用适当的鉴别方法以控制远程用户的访问。
- 网络上的设备标识
  应考虑自动设备标识，将其作为鉴别特定位置和设备连接的方法。
- 远程诊断和配置端口的保护
  对于诊断和配置端口的物理和逻辑访问应加以控制。

11.4网络访问控制

- 目标：防止对网络服务的未授权访问。

- 网络隔离
  应在网络中隔离信息服务、用户及信息系统。
- 网络连接控制
  对于共享的网络，特别是越过组织边界的网络，用户的联网能力应按照访问控制策略和业务应用要求加以限制（见11.1）。
- 网络路由控制
  应在网络中实施路由控制，以确保计算机连接和信息流不违反业务应用的访问控制策略。

11.5 操作系统访问控制

- 目标：防止对操作系统的未授权访问。
- 安全登录程序
  访问操作系统应通过安全登录程序加以控制。
- 用户标识和鉴别
  所有用户应有唯一的、专供其个人使用的标识符（用户ID），应选择一种适当的鉴别技术证实用户所宣称的身份。
- 口令管理系统
  口令管理系统应是交互式的，并应确保优质的口令。
- 系统实用工具的使用
  可能超越系统和应用程序控制措施的实用工具的使用应加以限制并严格控制。
- 会话超时
  不活动会话应在一个设定的休止期后关闭。
- 联机时间的限定
  应使用联机时间的限制，为高风险应用程序提供额外的安全。

11.6应用和信息访问控制

- 目标：防止对应用系统中信息的未授权访问。

- 信息访问限制
  用户和支持人员对信息和应用系统功能的访问应依照已确定的访问控制策略加以限制。
- 敏感系统隔离
  敏感系统应有专用的（隔离的）运算环境。

11.7移动计算和远程工作

- 目标：确保使用移动计算和远程工作设施时的信息安全。

- 移动计算和通信
  应有正式策略并且采用适当的安全措施，以防范使用移动计算和通信设施时所造成的风险。
- 远程工作
  应为远程工作活动开发和实施策略、操作计划和程序。

12、信息系统获取、开发和维护

- 12.1信息系统的安全要求
- 12.2应用中的正确处理
- 12.3密码控制
- 12.4系统文件的安全
- 12.5开发和支持过程中的安全
- 12.6技术脆弱性管理

12.1信息系统的安全要求

- 目标：确保安全是信息系统的一个有机组成部分。

- 安全要求分析和说明
  在新的信息系统或增强已有信息系统的业务要求陈述中，应规定对安全控制措施的要求。

12.2 应用中的正确处理

- 目标：防止应用系统中的信息的错误、遗失、未授权的修改及误用。

- 输入数据验证
  输入应用系统的数据应加以验证，以确保数据是正确且恰当的。
- 内部处理的控制
  验证检查应整合到应用中，以检查由于处理的错误或故意的行为造成的信息的讹误。
- 消息完整性
  应用中的确保真实性和保护消息完整性的要求应得到识别，适当的控制措施也应得到识别并实施。
- 输出数据验证
  从应用系统输出的数据应加以验证，以确保对所存储信息的处理是正确的且适于环境的。

12.3密码控制

- 目标：通过密码方法保护信息的保密性、真实性或完整性。

- 使用密码控制的策略
  应开发和实施使用密码控制措施来保护信息的策略。
- 密钥管理
  应有密钥管理以支持组织使用密码技术。

12.4 系统文件的安全

- 目标：确保系统文件的安全。

- 运行软件的控制
  应有程序来控制在运行系统上安装软件。
- 系统测试数据的保护
  测试数据应认真地加以选择、保护和控制。
- 对程序源代码的访问控制
  应限制访问程序源代码。

12.5 开发和支持过程中的安全

- 目标：维护应用系统软件和信息的安全。

- 变更控制程序
  应使用正式的变更控制程序控制变更的实施。
- 操作系统变更后应用的技术评审
  当操作系统发生变更后，应对业务的关键应用进行评审和测试，以确保对组织的运行和安全没有负面影响。
- 软件包变更的限制
  应对软件包的修改进行劝阻，限制必要的变更，且对所有的变更加以严格控制。
- 信息泄露
  应防止信息泄露的可能性。
- 外包软件开发
  组织应管理和监视外包软件的开发。

12.6技术脆弱性管理

- 目标：降低利用公布的技术脆弱性导致的风险。

- 技术脆弱性的控制
  应及时得到现用信息系统技术脆弱性的信息，评价组织对这些脆弱性的暴露程度，并采取适当的措施来处理相关的风险。

13、信息安全事件管理

- 13.1报告信息安全事态和弱点
  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。

- 2个控制措施：
  报告信息安全事态
  报告安全弱点

- 13.2信息安全事件和改进的管理
  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。

- 3个控制措施：
  职责和程序
  对信息安全事件的总结
  证据的收集

14、业务连续性管理

- 14.1业务连续性管理的信息安全方面
  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。

- 5个控制措施：
  业务连续性管理过程中包含的信息安全
  业务连续性和风险评估
  制定和实施包含信息安全的连续性计划
  业务连续性计划框架
  测试、维护和再评估业务连续性计划

15、符合性

- 15.1 符合法律要求
  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。
- 15.2 符合安全策略和标准以及技术符合性
  目标：确保系统符合组织的安全策略及标准。
- 15.3 信息系统审核考虑
  目标：将信息系统审核过程的有效性最大化，干扰最小化。

15.1符合法律要求

- 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。

- 可用法律的识别
  对每一个信息系统和组织而言，所有相关的法令、法规和合同要求，以及为满足这些要求组织所采用的方法，应加以明确地定义、形成文件并保持更新。
- 知识产权（IPR）
  应实施适当的程序，以确保在使用具有知识产权的材料和具有所有权的软件产品时，符合法律、法规和合同的要求。
- 保护组织的记录
  应防止重要的记录遗失、毁坏和伪造，以满足法令、法规、合同和业务的要求。

15.1符合法律要求

- 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。

- 数据保护和个人信息的隐私
  应依照相关的法律、法规和合同条款的要求，确保数据保护和隐私。
- 防止滥用信息处理设施
  应禁止用户使用信息处理设施用于未授权的目的。
- 密码控制措施的规则
  使用密码控制措施应遵从相关的协议、法律和法规。

15.2 符合安全策略和标准以及技术符合性

- 目标：确保系统符合组织的安全策略及标准。

- 符合安全策略和标准
  管理人员应确保在其职责范围内的所有安全程序被正确地执行，以确保符合安全策略及标准。
- 技术符合性检查
  信息系统应被定期检查是否符合安全实施标准。

15.3 信息系统审计考虑

- 目标：将信息系统审计过程的有效性最大化，干扰最小化。

- 信息系统审计控制措施
  涉及对运行系统检查的审计要求和活动，应谨慎地加以规划并取得批准，以便最小化造成业务过程中断的风险。
- 信息系统审计工具的保护
  对于信息系统审计工具的访问应加以保护，以防止任何可能的滥用或损害。

本标准小结

- 包括11个主要安全类别，汇集了39个控制目标、133个安全控制措施；
- 是实施GB/T 22080:2008的支撑标准，给出了组织建立信息安全管理体系（ISMS）时可选择实施的控制目标和控制措施集；
- 是一个信息安全最佳实践的汇总；
- 不是用于认证和审核的标准。

Q&A

谢谢大家！