ICS 35.040
L 80

中华人民共和国国家标准

GB/T 22081—2016/ISO/IEC 27002:2013
代替 GB/T 22081—2008

信息技术　安全技术
信息安全控制实践指南

Information technology—Security techniques—Code of practice for information security controls

(ISO/IEC 27002:2013,IDT)

2016-08-29 发布　　2017-03-01 实施

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　发布

目　　次

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准代替 GB/T 22081—2008《信息技术　安全技术　信息安全管理实用规则》。

本标准与 GB/T 22081—2008 相比，主要技术变化如下：

——结构变化见附录 NA；

——术语变化见附录 NB。

本标准使用翻译法等同采用 ISO/IEC 27002:2013《信息技术　安全技术　信息安全控制实践指南》及其相应的技术勘误(ISO/IEC 27002:2013/COR 1:2014)。

与本标准中规范性引用的国际文件有一致性对应关系的我国文件如下：

——GB/T 29246—2012　信息技术　安全技术　信息安全管理体系　概述和词汇(ISO/IEC 27000:2009,IDT)。

本标准做了下列编辑性修改：

——增加了资料性附录 NA；

——增加了资料性附录 NB。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本标准由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本标准起草单位：中国电子技术标准化研究院、中电长城网际系统应用有限公司、中国信息安全认证中心、山东省标准化研究院、广州赛宝认证中心服务有限公司、北京江南天安科技有限公司、上海三零卫士信息安全有限公司、中国合格评定国家认可中心、北京时代新威信息技术有限公司、黑龙江电子信息产品监督检验院、浙江远望电子有限公司、杭州在信科技有限公司。

本标准主要起草人：许玉娜、上官晓丽、闵京华、尤其、公伟、卢列文、倪文静、王连强、陈冠直、于惊涛、付志高、赵英庆、卢普明、王曙光、虞仲华、韩硕祥、魏军、程瑜琦、孔祥林、邬敏华、李华、李阳。

本标准所代替标准的历次版本发布情况为：

——GB/T 22081—2008。

引　言

0.1　背景和环境

本标准可作为组织基于GB/T 22080[10]实现信息安全管理体系(ISMS)过程中选择控制时的参考，或作为组织在实现通用信息安全控制时的指南。在考虑具体信息安全风险环境后，本标准也可用于制定特定行业和特定组织的信息安全管理指南。

所有类型和规模的组织(包括公共和私营部门、商业组织、非盈利性组织)都会收集、处理、存储和传输包括电子、物理和语音(如会谈和演讲)等多种形式的信息。

信息的价值超越文字、数字和图像的本身，例如：知识、概念、观点和品牌都是无形信息。在互联世界中对于组织业务而言，信息和相关过程、系统、网络及其操作、处理与保护活动中所涉及的人员都是资产，与其他重要的业务资产一样，对组织的业务至关重要，因此值得或需要保护以防范各种危害。

资产易遭受故意和意外的威胁；且相关的过程、系统、网络和人员均有其固有脆弱性。业务过程和系统的变更或其他外部变更(如新的法律法规)可能产生新的信息安全风险。因此，考虑到威胁利用脆弱性损害组织的途径多种多样，信息安全风险始终存在。有效的信息安全通过防范威胁和脆弱性使组织得到保护来减少风险，从而降低对其资产的影响。

信息安全可通过实现一组合适的控制来达到，包括策略、过程、规程、组织结构和软硬件功能。必要时，需要建立、实现、监视、评审和改进这些控制，以确保其满足组织特定的安全和业务目标。GB/T 22080[10]规定的ISMS采用整体的、协调的观点看待组织的信息安全风险，以便在一致的管理体系总体框架下实现一套全面的信息安全控制。

从GB/T 22080[10]和本标准来看，许多信息系统的设计未达到是安全的。通过技术手段可获得的安全是有限的，宜通过适当的管理和规程给予支持。确定哪些控制应该存在，这需要仔细规划并注意细节。一个成功的信息安全管理体系需要得到组织内的所有员工的支持，股东、供应商或其他外部各方的参与，也需要外部各方的专家建议。

在更一般的意义上，有效的信息安全也向管理者及其他相关方保证组织资产处于合理的安全，并受到保护不被损害，因此其角色等同于业务推动者。

0.2　信息安全要求

组织识别其安全要求是必要的。安全要求的3个主要来源是：

a)　考虑组织的整体业务战略与目标，对组织风险的评估。通过风险评估，识别资产受到的威胁，评价易受威胁利用的脆弱性和威胁发生的可能性，估计潜在的影响；

b)　组织及其贸易伙伴、合同方和服务提供商必须满足的法律、法规、规章制度和合同要求，以及他们的社会文化环境；

c)　组织为支持其运行，针对信息的操作、处理、存储、通信和归档而建立的原则、目标和业务要求。

实现控制所使用的资源，必须权衡缺少这些控制而导致的安全问题以及可能导致的业务危害。风险评估的结果将有助于指导和确定合适的管理措施、信息安全风险管理的优先级以及为防范这些风险所选择控制实现的优先级。

ISO/IEC 27005[11]提供了信息安全风险管理指南，包括风险评估、风险处置、风险接受、风险沟通、风险监视和风险评审各方面的建议。

0.3 控制的选择

控制可以选自本标准或其他控制集，或适当时针对特定的需求设计新的控制。

控制的选择取决于组织决策，该决策基于风险接受准则、风险处置选项、组织采用的通用风险管理方法；控制的选择也必须遵守所有相关的国家法律法规。同时控制的选择也取决于控制交互方式以提供纵深防御。

本标准中的某些控制可被当作信息安全管理的指导原则，并且可用于大多数组织。在每个控制之下，详细地给出了其实现指南。有关选择控制的更详细信息以及其他的风险的处置选项，可参见ISO/IEC 27005[11]。

0.4 编制组织自己的指南

本标准可作为组织制定其特定指南的起点。对一个组织来说，本标准中的控制和指南并非全部适用。另外，可能还需要增加一些不包含在本标准中的控制和指南。当制定包含一些增加的控制和指南的组织文件时，给出一些对本标准可用条款的交叉应用，这可能是有用的，以支持审核员和和业务伙伴的符合性检查。

0.5 生命周期的考虑

信息有其固有的生命周期，即从其创建和产生，经过存储、处理、使用和传输到其最终销毁或消失。在其生命周期中，信息资产的价值和所面临的风险可能会变化（如在公司账目正式公布后，对它的窃取和未授权泄露所产生的危害将极大的降低），但在所有阶段，信息安全仍存在一定程度的重要性。

信息系统的生命周期包括构思、规约、设计、开发、测试、实现、使用、维护，并最终退役和销毁。在每一阶段均应考虑到信息安全。在每一阶段上均应考虑信息安全。开发新的系统或对现有系统的改变，为组织升级和改进安全控制提供了机会，同时应考虑实际的安全事件以及当前和预测的信息安全风险。

0.6 相关标准

本标准就一个广泛的、可通用于不同组织的信息安全控制集，提供了相应的指南；而信息安全管理体系标准族中的其他标准就信息安全管理全过程的其他方面提供了补充建议或要求。

信息安全管理体系标准的总体介绍参见ISO/IEC 27000。ISO/IEC 27000中提供的词汇表确定了信息安全管理体系标准中使用的绝大部分术语，并描述了每个标准的范围和目标。

信息技术　安全技术
信息安全控制实践指南

1　范围

本标准为组织的信息安全标准和信息安全管理实践提供了指南，包括考虑了组织信息安全风险环境的控制的选择、实现和管理。

本标准被设计用于组织：

a）　选择控制，即基于GB/T 22080[10]，在实现一个信息安全管理体系的过程中选择控制；

b）　实现通用的、可接受的信息安全控制；

c）　制定组织自己的信息安全管理指南。

2　规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本(包括所有的修改单)适用于本文件。

ISO/IEC 27000　信息技术　安全技术　信息安全管理体系　概述和词汇(Information technology—Security techniques—Information security management systems—Overview and vocabulary)。

3　术语和定义

ISO/IEC 27000界定的术语和定义适用于本文件。

4　标准结构

本标准包括14个安全控制的章节，共含有35个主要安全类别以及114项控制。

4.1　章节

定义安全控制的每个章节，包含一个或多个主要安全类别。

本标准中各章节的顺序不表示其重要性。根据不同的环境，任何或所有章节中的安全控制都可能是重要的，因此应用本标准的每一个组织，宜识别可应用的控制，这些控制多么重要，以及它们如何应用到各个业务过程。另外，本标准的列表没有优先顺序。

4.2　控制类别

每一个主要安全控制类别包括：

a）　一个控制目标，声明要实现什么；

b）　一个或多个控制，可被用于实现该控制目标。

控制的描述结构如下：

控制

为满足控制目标，给出定义特定控制的陈述。