ICS 35.040
L 80

中华人民共和国国家标准

GB/T 22080—2016/ISO/IEC 27001:2013
代替 GB/T 22080—2008

信息技术　安全技术
信息安全管理体系　要求

Information technology—Security techniques—Information security management systems—Requirements

（ISO/IEC 27001:2013,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 22080—2008《信息技术安全技术信息安全管理体系要求》。

与 GB/T 22080—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 27001:2013《信息技术　安全技术　信息安全管理体系　要求》。

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：上官晓丽、许玉娜、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 22080—2008。

引　言

0.1　总则

本标准提供建立、实现、维护和持续改进信息安全管理体系的要求。采用信息安全管理体系是组织的一项战略性决策。组织信息安全管理体系的建立和实现受组织的需要和目标、安全要求、组织所采用的过程、规模和结构的影响。所有这些影响因素可能随时间发生变化。

信息安全管理体系通过应用风险管理过程来保持信息的保密性、完整性和可用性，并为相关方树立风险得到充分管理的信心。

重要的是，信息安全管理体系是组织的过程和整体管理结构的一部分并集成在其中，并且在过程、信息系统和控制的设计中要考虑到信息安全。期望的是，信息安全管理体系的实现程度要与组织的需要相符合。

本标准可被内部和外部各方用于评估组织的能力是否满足自身的信息安全要求。

本标准中所表述要求的顺序不反映各要求的重要性或暗示这些要求要予实现的顺序。条款编号仅为方便引用。

ISO/IEC 27000 描述了信息安全管理体系的概要和词汇，引用了信息安全管理体系标准族（包括 ISO/IEC 27003[2]、ISO/IEC 27004[3]、ISO/IEC 27005[4]），以及相关术语和定义。

0.2　与其他管理体系标准的兼容性

本标准应用 ISO/IEC 合并导则附录 SL 中定义的高层结构、相同条款标题、相同文本、通用术语和核心定义，因此维护了与其他采用附录 SL 的管理体系的标准具有兼容性。

附录 SL 中定义的通用途径对于选择运行单一管理体系来满足两个或更多管理体系标准要求的组织是有用的。

信息技术　安全技术
信息安全管理体系　要求

1　范围

本标准规定了在组织环境下建立、实现、维护和持续改进信息安全管理体系的要求。本标准还包括了根据组织需求所剪裁的信息安全风险评估和处置的要求。

本标准规定的要求是通用的，适用于各种类型、规模或性质的组织。当组织声称符合本标准时，不能排除第4章到第10章中所规定的任何要求。

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　组织环境

4.1　理解组织及其环境

组织应确定与其意图相关的，且影响其实现信息安全管理体系预期结果能力的外部和内部事项。

注：对这些事项的确定，参见ISO 31000:2009[5]，5.3中建立外部和内部环境的内容。

4.2　理解相关方的需求和期望

组织应确定：

a)　信息安全管理体系相关方；

b)　这些相关方与信息安全相关的要求。

注：相关方的要求可包括法律、法规要求和合同义务。

4.3　确定信息安全管理体系范围

组织应确定信息安全管理体系的边界及其适用性，以建立其范围。

在确定范围时，组织应考虑：

a)　4.1中提到的外部和内部事项；

b)　4.2中提到的要求；

c)　组织实施的活动之间的及其与其他组织实施的活动之间的接口和依赖关系。

该范围应形成文件化信息并可用。