ICS 35.040
L 80

中华人民共和国国家标准

GB/T 38631—2020

信息技术　安全技术
GB/T 22080 具体行业应用　要求

Information technology—Security techniques—
Sector-specific application of GB/T 22080—Requirements

(ISO/IEC 27009:2016, Information technology—Security techniques—
Sector-specific application of ISO/IEC 27001—Requirements, MOD)

2020-04-28 发布　　2020-11-01 实施

国家市场监督管理总局
国家标准化管理委员会　发布

目　　次

前言 …… Ⅰ
1　范围 …… 1
2　规范性引用文件 …… 1
3　术语和定义 …… 1
4　概述 …… 1
4.1　总则 …… 1
4.2　本标准结构 …… 2
4.3　扩展 GB/T 22080 要求或 GB/T 22081 控制 …… 2
5　补充、细化或解释 GB/T 22080 要求 …… 2
5.1　总则 …… 2
5.2　补充要求 …… 3
5.3　细化要求 …… 3
5.4　解释要求 …… 3
6　补充或修改 GB/T 22081 指南 …… 3
6.1　总则 …… 3
6.2　补充指南 …… 4
6.3　修改指南 …… 4
附录 A（规范性附录）　制定与 GB/T 22080—2016 或 GB/T 22081—2016 相关的具体行业标准的模板 …… 5
附录 B（资料性附录）　面向医疗行业的信息安全管理体系指南示例 …… 8
参考文献 …… 11

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准使用重新起草法修改采用 ISO/IEC 27009:2016《信息技术　安全技术　ISO/IEC 27001 具体行业应用　要求》。

本标准与 ISO/IEC 27009:2016 的技术性差异及其产生的原因如下：

——范围增加“本标准适用于制定与 GB/T 22080 相关的具体行业标准”(见第 1 章)；

——4.1 删除“ISO/IEC 之外的组织也制定了实现具体行业需求的标准”；

——增加“依据附录 A,面向医疗行业的信息安全管理体系指南示例参见附录 B”(见 4.2)；

——附录 A 的 A.1 删除“具体行业标准宜命名如下:面向〈行业〉的信息安全管理体系”；

——附录 A 的 A.2 模板中,4.2 和 5 的〈控制目标号〉〈控制目标标题〉和〈控制号〉〈控制标题〉改为〈控制目标号〉[〈控制目标标题〉]、〈控制号〉[〈控制标题〉],以避免标题与其后文字混淆；

——附录 A 的 A.2 模板中,4.2 和 5 中,“对行业至少使用三个字母作为前缀”改为“对行业使用国民经济行业名称(见 GB/T 4754—2017)作为前缀”,4.2 中强制实施的控制,“使用(M)作为控制编号的前缀”改为“使用(强制)作为控制编号的前缀”。

本标准做了下列编辑性修改：

——增加了参考文献 ISO 27799:2016 和 ISO 22600；

——增加资料性附录 B“面向医疗行业的信息安全管理体系指南示例”,有利于标准落地实施。

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:山东省标准化研究院、中国网络安全审查技术与认证中心、成都秦川物联网科技股份有限公司、陕西省网络与信息安全测评中心、山东崇弘信息技术有限公司。

本标准主要起草人:王曙光、魏军、王庆升、公伟、张斌、来永钧、邵泽华、赵首花、杨锐、尤其、郭杨、权亚强、李怡、何果、路津、李红胜、路征、陈慧勤、刘勘伪、于秀彦、胡鑫磊、王栋、刘鑫。

信息技术　安全技术
GB/T 22080具体行业应用　要求

1　范围

本标准规定了GB/T 22080应用于具体行业(领域、应用)时的要求。本标准解释了如何在GB/T 22080要求上包含补充要求,如何细化GB/T 22080的要求,以及如何包含GB/T 22080—2016附录A之外的控制或控制集。

本标准确保补充的或细化的要求与GB/T 22080的要求不冲突。

本标准适用于制定与GB/T 22080相关的具体行业标准。

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。

GB/T 22080—2016　信息技术　安全技术　信息安全管理体系　要求(ISO/IEC 27001:2013,IDT)

GB/T 22081—2016　信息技术　安全技术　信息安全控制实践指南(ISO/IEC 27002:2013,IDT)

GB/T 29246—2017　信息技术　安全技术　信息安全管理体系　概述和词汇(ISO/IEC 27000:2016,IDT)

3　术语和定义

GB/T 29246—2017界定的以及下列术语和定义适用于本文件。

3.1

解释　interpretation

在具体行业背景下对GB/T 22080要求的说明(以要求或指南的形式),该说明不会使GB/T 22080的要求失效。

3.2

细化　refinement

GB/T 22080要求在具体行业的详述,该详述不会删除GB/T 22080任一要求或使其失效。

4　概述

4.1　总则

GB/T 22080规定了建立、实现、维护和持续改进信息安全管理体系的要求。这些要求是通用的,适用于各种类型、规模或性质的机构。

注:ISO管理体系标准的建立依据ISO/IEC导则　第1部分　融合的JTC1补充部分(2016)。

GB/T 22081为信息安全管理实践提供了指南,考虑了机构信息安全风险环境下控制的选择、实施和管理。该指南采用分层结构,包括章节、控制目标、控制、实现指南以及其他信息。指南是通用的,适