ICS 35.030
CCS L 80

中华人民共和国国家标准

GB/T 31496—2023/ISO/IEC 27003:2017
代替 GB/T 31496—2015

信息技术　安全技术
信息安全管理体系　指南

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

（ISO/IEC 27003:2017，IDT）

2023-05-23 发布　　2023-12-01 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 …… Ⅲ
引言 …… Ⅳ
1　范围 …… 1
2　规范性引用文件 …… 1
3　术语和定义 …… 1
4　组织语境 …… 1
4.1　理解组织及其语境 …… 1
4.2　理解利益相关方的需求和期望 …… 3
4.3　确定信息安全管理体系范围 …… 4
4.4　信息安全管理体系 …… 5
5　领导 …… 5
5.1　领导和承诺 …… 5
5.2　方针 …… 6
5.3　组织的角色、责任和权限 …… 7
6　规划 …… 8
6.1　应对风险和机会的措施 …… 8
6.2　信息安全目标及其实现规划 …… 14
7　支持 …… 16
7.1　资源 …… 16
7.2　胜任力 …… 17
7.3　意识 …… 17
7.4　沟通 …… 18
7.5　文件化信息 …… 19
8　运行 …… 22
8.1　运行规划和控制 …… 22
8.2　信息安全风险评估 …… 23
8.3　信息安全风险处置 …… 23
9　绩效评价 …… 24
9.1　监视、测量、分析和评价 …… 24
9.2　内部审核 …… 25
9.3　管理评审 …… 27
10　改进 …… 28
10.1　不符合项及纠正措施 …… 28

10.2 持续改进 …… 30
附录 A（资料性） 策略框架 …… 32
参考文献 …… 34

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分:标准化文件的结构和起草规则》的规定起草。

本文件代替GB/T 31496—2015《信息技术　安全技术　信息安全管理体系实施指南》,与GB/T 31496—2015相比,除结构调整和编辑性改动外,主要技术变化如下:

——更改了范围,按照GB/T 22080—2016的要求进行解释并提供指南;

——上一版采用了项目的方法,每个项目包含一系列活动。在修订版中不再采用项目的方法,而是提供了针对每个要求的指南,不需要考虑这些要求的实现顺序。

本文件等同采用ISO/IEC 27003:2017《信息技术　安全技术　信息安全管理体系　指南》。

本文件做了下列最小限度的编辑性改动:

——增加了4.2的注。

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专利的责任。

本文件由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本文件起草单位:中国电子技术标准化研究院、中国网络安全审查技术与认证中心、中国合格评定国家认可中心、杭州安恒信息技术股份有限公司、中国石油天然气股份有限公司长庆石化分公司、腾讯云计算(北京)有限责任公司、中电长城网际系统应用有限公司、上海三零卫士信息安全有限公司、北京赛西认证有限责任公司、西安电子科技大学、黑龙江省网络空间研究中心、北京信息安全测评中心、中国科学院软件研究所、重庆邮电大学、安徽科技学院、北京神州绿盟科技有限公司、中通服咨询设计研究院有限公司、北京中科微澜科技有限公司。

本文件主要起草人:王惠莅、上官晓丽、许玉娜、付志高、任泽君、尤其、周亚超、赵丽华、范博、闵京华、张东举、马文平、干露、李媛、方舟、张立武、梁伟、黄永洪、张恒、曹浩、尹晓鹏、宋雪、高丽芬、陈洪、杨牧天、裴心平。

本文件及其所代替文件的历次版本发布情况为:

——2015年首次发布为GB/T 31496—2015;

——本次为第一次修订。

引　言

本文件提供了关于GB/T 22080中规定的信息安全管理体系(ISMS)要求的指南,并提供了与之相关的建议("宜")、可能性("可能")和允许("可")。本文件的目的不是提供信息安全的所有方面的一般指南。

本文件第4章～第10章反映了GB/T 22080—2016的结构。

本文件没有增加对ISMS的任何新要求及其相关术语和定义。组织宜参照GB/T 22080的要求和GB/T 29246的定义。实施ISMS的组织没有义务遵守本文件中的指南。

ISMS强调了以下几个阶段的重要性:

——理解组织的需求及建立信息安全方针和信息安全目标的必要性;

——评估组织与信息安全相关的风险;

——实施和运行信息安全过程、控制和其他风险处理措施;

——监视和评审ISMS的绩效和有效性;

——进行持续改进。

与其他类型的管理体系相似,ISMS包括以下关键组成要素。

a) 方针。

b) 有明确责任的人员。

c) 相关的管理过程:

1) 方针建立;

2) 意识和能力的提供;

3) 规划;

4) 实现;

5) 运行;

6) 绩效评估;

7) 管理评审;

8) 改进。

d) 文件化信息。

ISMS还有其他关键组成要素,诸如:

e) 信息安全风险评估;

f) 信息安全风险处置,包括控制的确定和实现。

本文件是通用的,旨在适用于所有组织,无论其类型、规模或性质。组织宜根据其特定的组织环境识别本文件对其适用的部分(见GB/T 22080—2016中第4章)。

例如,一些指南可能更适合大型组织,但对于非常小的组织(例如少于10人),这些指南中的一些内容可能是不必要的或不适合的。

第4章～第10章的描述结构如下:

——所需活动:提出GB/T 22080相应条款所要求的关键活动;

——解释:解释GB/T 22080要求的含义;

——指南:提供更详细或支持性的信息来实现"所要求活动",包括实施的示例;

——其他信息:提供了可能进一步考虑的信息。

GB/T 31496、GB/T 31497和GB/T 31722形成了一套文件,支持GB/T 22080—2016并提供指

南。其中，GB/T 31496 是对 GB/T 22080 的所有要求提供指南的一个基本的和全面的文件，但其没有关于“监视、测量、分析和评价”和信息安全风险管理的详细描述。GB/T 31497 和 GB/T 31722 侧重于特定内容，并分别对“监视、测量、分析和评价”和信息安全风险管理提供了更详细的指南。

在 GB/T 22080 中有多处明确地提及了文件化信息。尽管如此，组织仍可能确定持有对其管理体系有效性所需的附加文件化信息，并作为响应 GB/T 22080—2016 中 7.5.1 b)的部分。在这些情况下，本文件使用“仅在组织确定对其管理体系有效性所需的形式和范围内，有关该活动及其结果的文件化信息是强制性的[见 GB/T 22080—2016 中 7.5.1 b)]”的表述。

信息技术　安全技术
信息安全管理体系　指南

1　范围

本文件为GB/T 22080—2016提供了解释说明和指南。

2　规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；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 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)

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)

ISO/IEC 27001　信息技术、网络安全和隐私保护　信息安全管理体系　要求(Information security，cybersecurity and privacy protection—Information security management systems—Requirements)

3　术语和定义

GB/T 29246—2017界定的术语和定义适用于本文件。

4　组织语境

4.1　理解组织及其语境

所需活动

组织确定与其意图相关的，且影响其实现信息安全管理体系(ISMS)预期结果能力的外部和内部问题。

解释

作为ISMS的一项组成功能，组织持续分析自身及其所处环境。这种分析关注内部和外部问题，这些问题以某种方式影响信息安全以及如何管理信息安全，并与组织的目标相关。

分析这些问题有三个目的：

——理解语境，以决定ISMS的范围；

——分析语境，以确定风险和机会；