ICS 35.030
CCS L 80

中华人民共和国国家标准

GB/T 32916—2023/ISO/IEC TS 27008:2019
代替 GB/Z 32916—2016

信息安全技术
信息安全控制评估指南

**Information security techniques—
Guidelines for the assessment of information security controls**

（ISO/IEC TS 27008:2019,Information technology—Security techniques—
Guidelines for the assessment of information security controls,IDT）

2023-09-07 发布　　2024-04-01 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

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/Z 32916—2016《信息技术　安全技术　信息安全控制措施审核员指南》,与GB/Z 32916—2016相比,除结构调整和编辑性改动外,主要技术变化如下:

——评估方法中增加了抽样的介绍(见7.5)。

本文件等同采用ISO/IEC TS 27008:2019《信息技术　安全技术　信息安全控制评估指南》,文件类型由ISO/IEC的技术规范调整为我国的国家标准。

本文件做了下列最小限度的编辑性改动:

a)　为与现有标准协调,将标准名称改为《信息安全技术　信息安全控制评估指南》;

b)　增加了附录NA。

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:北京赛西认证有限责任公司、中国电子技术标准化研究院、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、华为技术有限公司、长扬科技(北京)股份有限公司、北京神州绿盟科技有限公司、深圳红途科技有限公司、美的集团股份有限公司、中国软件评测中心(工业和信息化部软件与集成电路促进中心)、杭州安恒信息技术股份有限公司、国家计算机网络应急技术处理协调中心、国网新疆电力有限公司电力科学研究院、西安交大捷普网络科技有限公司、北京天地和兴科技有限公司、杭州趣链科技有限公司、浙江省电子信息产品检验研究院、远江盛邦(北京)网络安全科技股份有限公司、陕西省网络与信息安全测评中心、北京金山云网络技术有限公司、上海观安信息技术股份有限公司、北京邮电大学、杭州中正检测技术有限公司、马上消费金融股份有限公司、中国科学院信息工程研究所、智网安云(武汉)信息技术有限公司、启明星辰信息技术集团股份有限公司、西安邮电大学。

本文件主要起草人:韩硕祥、赵丽华、付志高、黄俊梅、王惠莅、周晓宇、刘海军、赵华、王凌、刘峰松、叶建伟、黄鹏程、张亮亮、李春琦、俞政臣、李松恬、梁伟、张世杰、贺创新、张杰、熊卫军、王秉政、蔡北方、王文磊、邹振婉、杨坤、何建锋、刘乐农、魏遵博、尹肖栋、王晶、杭肖、于丽芳、谢江、王东滨、曹宇、刘志强、韩冬旭、王燕青、王红亮、朱志祥、郑堃、张强、高珍祯、陆月明、田丽丹、权晓文。

本文件及其所代替的历次版本发布情况为:

——2016年首次发布为GB/Z 32916—2016;

——本次为第一次修订。

引　言

本文件支持GB/T 22080—2016中所给出的信息安全风险管理过程，以及所确定的相关信息安全控制措施集。

信息安全控制措施宜适用、有效和高效。针对缓解信息安全风险和其他目标，本文件说明了如何评估组织的信息安全控制措施，以确认其确实适用、有效且高效，或者确定变更（改进机会）的需求。信息安全控制措施作为一个整体，最终目的是以合理的成本效益和与业务一致的方式，充分缓解组织认为不可接受和不可避免的信息安全风险。根据业务使命和目标、组织策略和要求、发现的威胁与脆弱性、运行考虑、信息系统和平台的依赖性以及组织的风险考量定制必要的评估，本文件提供了该评估所需的灵活性。

有关信息安全管理体系审核指南见GB/T 28450—2020，有关信息安全管理体系审核和认证机构的要求见GB/T 25067—2020。

注：本文件中“信息安全控制措施”和“信息安全控制”可以互换使用。“控制”的定义见GB/T 29246—2017。

信息安全技术
信息安全控制评估指南

1 范围

本文件提供了评估信息安全控制措施的实施与运行及评估过程指导,包括对信息系统控制措施的技术性评估,该评估基于组织所建立的信息安全要求及技术性评估准则。

本文件在如何评估由 ISO/IEC 27001 规定的信息安全管理体系所管理的信息安全控制措施方面提供指南。

本文件适用于各种类型和规模的组织开展信息安全评估和技术符合性检查。

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。

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)

注: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

ISO/IEC 27000 界定的术语和定义适用于本文件。

4 本文件的结构

本文件描述了信息安全控制措施评估过程,包括技术性评估。

第 5 章提供背景信息。

第 6 章提供信息安全控制措施评估概述。

第 7 章介绍评估方法。

第 8 章介绍信息安全控制措施评估过程。

附录 A 指导初始信息收集。

附录 B 指导技术性评估。

附录 C 指导云服务技术性评估。

附录 NA 给出了 GB/T 22081—2016 与 ISO/IEC 27002:2022 中控制措施的对应关系。

5 背景

信息安全控制措施是处置不可接受的信息安全风险,使其处于组织可接受风险级别之内的主要手段。