ICS 35.040
L 80

中华人民共和国国家标准化指导性技术文件

GB/Z 32916—2016/ISO/IEC TR 27008:2011

信息技术　安全技术
信息安全控制措施审核员指南

Information technology—Security techniques—
Guidelines for auditors on information security controls

(ISO/IEC TR 27008:2011,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

本指导性技术文件按照 GB/T 1.1—2009 给出的规则起草。

本指导性技术文件使用翻译法等同采用国际技术报告 ISO/IEC TR 27008:2011《信息技术　安全技术　审核员信息安全控制措施审核指南》(英文版)。根据我国国情和 GB/T 1.1 的规定,做以下编辑性修改:

——盲测又称黑盒测试,加了标注"(黑盒测试)";

——透明盒测试又称白盒测试,加了标注"(白盒测试)"。

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。

本指导性技术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。

本指导性技术文件起草单位:中国电子技术标准化研究院、中国合格评定国家认可中心、工业和信息化部电子第五研究所、北京赛西认证有限责任公司、北京时代新威信息技术有限公司。

本指导性技术文件主要起草人:倪文静、董涛、刘健、张杰、刘晓红、韩硕祥、付志高、段淼、刘小茵、王新杰、黄俊梅、魏军。

引　言

本指导性技术文件支持 GB/T 22080 和 ISO/IEC 27005 中定义的信息安全管理体系(ISMS)风险管理过程,以及 GB/T 22081 中包含的控制措施。

本指导性技术文件提供对组织信息安全控制措施进行评审的指南,例如,在组织、业务过程和系统环境下进行技术符合性检查等。

有关管理体系要素的审核,请参考 ISO/IEC 27007。有关认证目的的 ISMS 符合性评审,请参考 GB/T 25067。

信息技术　安全技术
信息安全控制措施审核员指南

1　范围

本指导性技术文件为评审控制措施的实现和运行提供指南，包括对信息系统控制措施的技术符合性检查，以符合组织所建立的信息安全标准。

本指导性技术文件适用于所有类型和规模的组织，包括公有和私营公司、政府机构、非营利组织开展信息安全评审和技术符合性检查。本指导性技术文件不适用于管理体系审核。

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 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)

3　术语和定义

GB/T 29246—2012 界定的以及下列术语和定义适用于本文件。

3.1

评审对象　review object

要评审的指定项。

3.2

评审目的　review objective

描述所要达到评审结果的陈述。

3.3

安全实现标准　security implementation standard

授权的安全实现方式的规范文件。

4　本指导性技术文件的结构

本指导性技术文件包含信息安全控制措施评审过程的描述，其中包括技术符合性检查。第 5 章为背景信息，第 6 章为信息安全控制措施评审的概述，第 7 章为评审方法，第 8 章为评审活动。

技术符合性检查参见附录 A，初始信息收集参见附录 B。

5　背景

组织信息安全控制措施的选择宜基于风险评估的结果，并作为信息安全风险管理过程的组成部分，以将风险降低到可接受的水平。但对于决定不实施信息安全管理体系(ISMS)的组织，可通过其他方式