ICS 35.040
L 80

中华人民共和国国家标准

GB/T 28450—2012

信息安全技术
信息安全管理体系审核指南

Information security technology—
Guidelines for information security management system auditing

2012-06-29 发布　　2012-10-01 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：中国信息安全认证中心、中国电子技术标准化研究所、北京知识安全工程中心。

本标准主要起草人：张剑、上官晓丽、许玉娜、王新杰、闵京华、陈珍成。

引　言

本标准旨在为信息安全管理体系(简称 ISMS)审核员(包括内部审核员和外部审核员)执行 ISMS 审核提供指导,以确保 ISMS 审核:

——既符合 GB/T 22080—2008 的要求,又与 GB/T 19011—2003《质量和(或)环境管理体系审核指南》(ISO 19011:2002,IDT)和 ISO/IEC 27006:2007《信息技术　安全技术　信息安全管理体系审核认证机构要求》标准保持一致;

——成为帮助受审核的组织持续改进的一项有效活动。

本标准在 GB/T 19011—2003 的基础上为信息安全管理体系的审核原则、审核方案管理和审核实施提供了指导,并对审核员的能力及其评价提供了指导。本标准旨在适用于广泛的潜在使用者,包括审核员、实施 ISMS 的组织,因合同原因需要对 ISMS 实施审核的组织以及合格评定领域中与审核员注册或培训、管理体系认证注册、认可或标准化有关的组织。

当 ISMS 与其他管理体系一起实施时,由本标准使用者决定这些管理体系审核是分别进行还是一起进行。

本标准采纳 GB/T 19011—2003《质量和(或)环境管理体系审核指南》(ISO 19011:2002,IDT)的标准正文的格式与内容,在此基础上针对 ISMS 的特点增加了相关内容,用“IS”加以标识。另外,第 7 章针对 ISMS 提出了专门要求,还增加了 5 个资料性附录(见附录 D)。

此外,在监视与要求(如产品规范或法律法规)的符合性方面感兴趣的任何其他个人或组织,可以发现本标准中的指南是有用的。

信息安全技术
信息安全管理体系审核指南

1 范围

本标准在GB/T 19011—2003的基础上为信息安全管理体系(简称ISMS)的审核原则、审核方案管理和审核实施提供了指导,并对审核员的能力及其评价提供了指导。

本标准适用于需要实施ISMS内部审核、外部审核或对审核进行管理的所有组织。

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 19000—2008 质量管理体系 基础和术语(ISO 9000:2005,IDT)

GB/T 19011—2003 质量和(或)环境管理体系审核指南(ISO 19011:2002,IDT)

GB/T 22080—2008 信息技术 安全技术 信息安全管理体系 要求(ISO/IEC 27001:2005,IDT)

GB/T 22081—2008 信息技术 安全技术 信息安全管理实用规则(ISO/IEC 27002:2005,IDT)

3 术语和定义

GB/T 19000—2008、GB/T 19011—2003、GB/T 22080—2008和GB/T 22081—2008界定的术语和定义适用于本文件。

4 审核原则

4.1 通用的审核原则

GB/T 19011—2003的第4章中的原则适用。并且,以下ISMS特定的指南适用。

4.2 IS 4.1 审核原则

ISMS的审核还应遵循如下原则:

a) 保密性:ISMS的审核由于其特殊性,审核员应对保密性给予充分的重视,如注意受审核方的保密管理规程,关注受审核方对保密的特殊要求。

b) 基于风险:ISMS本身是基于业务风险管理的体系,需要审核员专注受审核方的业务风险,特别是实际残余风险;同时,对一些特殊的组织的审核会有特殊的风险,需要充分认识认证带来的风险。

5 审核方案的管理

5.1 总则

GB/T 19011—2003的5.1中的指南适用。并且,以下ISMS特定的指南适用。图1所示为审核方案的管理流程。