ICS 35.040
L 80

中华人民共和国国家标准

GB/T 28450—2020/ISO/IEC 27007:2017
代替 GB/T 28450—2012

信息技术　安全技术
信息安全管理体系审核指南

Information technology—Security techniques—Guidelines for information security management systems auditing

（ISO/IEC 27007:2017,IDT）

2020-12-14 发布　　2021-07-01 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

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准代替 GB/T 28450—2012《信息安全技术　信息安全管理体系审核指南》，与 GB/T 28450—2012 相比，主要技术性变化如下：

——删除了 ISMS 特定审核原则的内容(见 2012 年版的 4.2)；

——删除了审核方案管理流程图(见 2012 年版的 5.1)；

——删除了审核方案内容(见 2012 年版的 5.2.2)；

——增加了审核方案管理人员能力的内容(见 5.3.2)；

——增加了审核方案范围和详略程度确定的内容(见 5.3.3)；

——增加了审核方案风险识别和评估的内容(见 5.3.4)；

——修改了审核方案实施的内容(见 5.4，2012 年版的 5.4)；

——删除了审核方案记录的内容(见 2012 年版的 5.5)；

——删除了审核组长指定的内容(见 2012 年版的 6.2.1)；

——删除了实用帮助——信息收集注意事项(见 2012 年版的 6.5.4.1)；

——删除了审核报告批准的内容(见 2012 年版的 6.6.2)；

——删除了能力概念图(见 2012 年版的 7.1.1)；

——删除了个人素质的内容(见 2012 年版的 7.2)；

——增加了个人行为的内容(见 7.2.2)；

——删除了 ISMS 特定及相关专业知识和技能的内容(见 2012 年版的 7.3.3)；

——增加了管理体系审核员特定领域与专业知识和技能的内容(见 7.2.3.3)；

——增加了多领域管理体系审核知识和技能的内容(见 7.2.3.5)；

——删除了教育、工作经历、审核员培训和审核经历的内容(见 2012 年版的 7.4)；

——增加了审核员能力获得的内容(见 7.2.4)；

——修改了审核员评价的内容(见 7.3、7.4、7.5，2012 年版的 7.6)；

——重新组织了附录的内容，删除了原标准的五个附录，增加了附录 A：ISMS 审核实践指南，与 ISO/IEC 27007:2017 附录 A 保持一致。

本标准使用翻译法等同采用 ISO/IEC 27007:2017《信息技术 安全技术 信息安全管理体系审核指南》。

与本标准中规范性引用的国际文件有一致性对应关系的我国文件如下：

——GB/T 19011—2013　管理体系审核指南(ISO 19011:2011，IDT)

——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)

本标准做了下列编辑性修改：

——在引言中对本标准中涉及的部分术语和定义，与其他标准相关内容的关系进行了说明；

——在参考文献中增加了国际文件 ISO/IEC 27017。

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:北京时代新威信息技术有限公司、中国网络安全审查技术与认证中心、中国电子技术标准化研究院、全国组织机构统一社会信用代码数据服务中心。

本标准主要起草人:王新杰、王连强、张剑、上官晓丽、孙镇、赵捷、郑玮、陈剑博、郭乐宇、汪洋、曹宇、程瑜琦、王姣、孙泰、李晟飞。

本标准所代替标准的历次版本发布情况为:

——GB/T 28450—2012。

引　言

本标准提供了下列指南：

——信息安全管理体系(ISMS)审核方案的管理；

——遵循 GB/T 22080—2016 实施内部和外部审核；

——ISMS 审核员的能力和评价。

本标准宜与 GB/T 19011—2013 中包含的指南一起使用。

本标准遵循 GB/T 19011—2013 的结构，ISMS 审核所需的 ISMS 特定指南，用字母“IS”进行标识。

开展 ISMS 审核时，本标准新增的 ISMS 特定指南宜与 GB/T 19011—2013 配合使用，用字母“IS”进行标识”。

GB/T 19011—2013 提供了关于审核方案管理、管理体系内部或外部审核实施以及管理体系审核员能力和评价的指南。

本标准未声明组织规模要求，可适用于所有用户，包括中小型组织。

本标准中涉及的部分术语和定义，与其他标准相关内容的关系说明如下：

——国际标准中的“Procedure”，在 GB/T 19011—2013 中翻译为“程序”，而在 GB/T 22080—2016 中翻译为“规程”，因本标准同时引用了这两个标准的原文，故本标准中出现该术语的地方均采用其原标准中的定义；

——国际标准中的“Implement”，在 GB/T 19011—2013 中翻译为“实施”，而在 GB/T 22080—2016 中翻译为“实现”，因本标准同时引用了这两个标准的原文，故本标准中出现该术语的地方均采用其原标准中的定义；

——国际标准中的“Maintain”，在 GB/T 19011—2013 中翻译为“保持”，而在 GB/T 22080—2016 中翻译为“维护”，因本标准同时引用了这两个标准的原文，故本标准中出现该术语的地方均采用其原标准中的定义；

——国际标准中的“Documented information”，在 GB/T 29246—2017 中翻译为“文档化信息”，而在 GB/T 22080—2016 中翻译为“文件化信息”，因本标准引用了 GB/T 22080—2016 的原文，故本标准中出现该术语的地方均采用 GB/T 22080—2016 中的定义；

——国际标准中的“Context”，在 GB/T 29246—2017 中翻译为“语境”，而在 GB/T 22080—2016 中翻译为“环境”，因本标准引用了 GB/T 22080—2016 的原文，故本标准中出现该术语的地方均采用 GB/T 22080—2016 中的定义；

——国际标准中的“Continuity”，在 GB/T 29246—2017 中翻译为“持续性”，而在 GB/T 22080—2016 中翻译为“连续性”，因本标准引用了 GB/T 22080—2016 的原文，故本标准中出现该术语的地方均采用 GB/T 22080—2016 中的定义。

信息技术　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—2013的基础上，为信息安全管理体系（以下简称ISMS）审核方案管理和审核实施提供了指南，并对ISMS审核员能力提供了评价指南。

本标准适用于需要理解或实施ISMS的内部或外部审核，或需要管理ISMS审核方案的所有组织。

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 19011—2013　管理体系审核指南（ISO 19011:2011，IDT）

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）

3　术语和定义

GB/T 19011—2013和GB/T 29246—2017界定的术语和定义适用于本文件。

4　审核原则

GB/T 19011—2013的第4章审核原则适用。

5　审核方案的管理

5.1　总则

GB/T 19011—2013的5.1的指南适用。并且，以下ISMS特定的指南适用。

5.1.1　IS 5.1 总则

需要实施审核的组织宜建立审核方案，并考虑规划ISMS时所确定的风险和机会。

5.2　确立审核方案的目标

GB/T 19011—2013的5.2中的指南适用。并且，以下ISMS特定的指南适用。

5.2.1　IS 5.2 确立审核方案的目标

确立审核方案目标时，ISMS还宜考虑下列事项：