ICS 35.040
L 80

中华人民共和国国家标准

GB/T 31497—2015/ISO/IEC 27004:2009

信息技术　安全技术
信息安全管理　测量

**Information technology—Security techniques—
Information security management—Measurement**

(ISO/IEC 27004:2009,IDT)

2015-05-15 发布　　2016-01-01 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。

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。

本标准使用翻译法等同采用 ISO/IEC 27004:2009《信息技术　安全技术　信息安全管理　测量》(英文版)。

本标准做了以下编辑性修改：

——引言部分增加了有关信息安全管理体系标准族情况的介绍。

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：中国电子技术标准化研究院、山东省计算中心、上海三零卫士信息安全有限公司、中电长城网际系统应用有限公司、北京信息安全测评中心。

本标准主要起草人：上官晓丽、周鸣乐、李刚、许玉娜、顾卫东、闵京华、赵章界、董火民、李旺、史艳华、李敏、张建成、韩庆良。

引　言

0.1　总则

信息安全管理体系标准族(Information Security Management System,简称 ISMS 标准族)是国际信息安全技术标准化组织(ISO/IEC JTC1 SC27)制定的信息安全管理体系系列国际标准。ISMS 标准族旨在帮助各种类型和规模的组织,开发和实施管理其信息资产安全的框架,并为保护组织信息(诸如,财务信息、知识产权、员工详细资料,或者受客户或第三方委托的信息)的 ISMS 的独立评估做准备。ISMS 标准族包括的标准:a)定义了 ISMS 的要求及其认证机构的要求;b)提供了对整个"规划-实施-检查-处置"(PDCA)过程和要求的直接支持、详细指南和(或)解释;c)阐述了特定行业的 ISMS 指南;d)阐述了 ISMS 的一致性评估。

目前,ISMS 标准族由下列标准组成:

——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)

——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)

——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)

——GB/T 31496—2015　信息技术　安全技术　信息安全管理体系实施指南(ISO/IEC 27003:2010)

——(本标准)　信息技术　安全技术　信息安全管理 测量(ISO/IEC 27004:2009)

——GB/T 31722—2015　信息技术　安全技术　信息安全风险管理(ISO/IEC 27005:2008)

——GB/T 25067—2010　信息技术　安全技术　信息安全管理体系审核认证机构的要求(ISO/IEC 27006:2007)

——ISO/IEC 27007:2011　信息技术　安全技术　信息安全管理体系审核指南

——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

——ISO/IEC 27010:2012　信息技术　安全技术　行业间及组织间通信的信息安全管理

——ISO/IEC 27011:2008　信息技术　安全技术　基于 ISO/IEC 27002 的电信行业组织的信息安全管理指南

——ISO/IEC 27013:2012　信息技术　安全技术　ISO/IEC 27001 和 ISO/IEC 20000-1 集成实施指南

——ISO/IEC 27014:2013　信息技术　安全技术　信息安全治理

——ISO/IEC TR 27015:2012　信息技术　安全技术　金融服务信息安全管理指南

为了评估按照 GB/T 22080—2008 规定的已实施的信息安全管理体系(Information Security Management System,简称 ISMS)和控制措施或控制措施组的有效性,本标准提供了如何编制测度和测量以及如何使用的指南。

为了有助于决定 ISMS 过程或控制措施是否需要改变或改进,本标准涉及方针策略、信息安全风险管理、控制目标、控制措施、过程和规程,并且支持其校验过程。切记任何控制措施的测量都不能保证绝对安全。

本标准的实施形成了信息安全测量方案。信息安全测量方案将有助于管理者识别和评价不相容

的、无效的 ISMS 过程和控制措施，并优化改进或改变这些过程和(或)控制的活动。它也可有助于组织证明 GB/T 22080—2008 的符合性，并提供管理评审和信息安全风险管理过程的额外证据。

本标准假设：制定测度和测量的出发点是按照 GB/T 22080—2008 要求充分掌握了组织所面临的信息安全风险，并假设已经正确实施了组织的风险评估活动(即基于 GB/T 31722—2015)。信息安全测量方案将鼓励组织向利益相关者提供可靠的关于信息安全风险和管理这些风险已实施的 ISMS 的状况的信息。

通过有效地实施信息安全测量方案，将提高利益相关者对测量结果的信任，并能使其利用这些测度实现对信息安全和 ISMS 的持续改进。

累积的测量结果将允许把一段时间内实现信息安全目标的进展当作组织的 ISMS 持续改进过程的一部分。

0.2 管理概述

GB/T 22080—2008 要求组织“在考虑有效性测量结果的基础上，进行 ISMS 有效性的定期评审”，并且“测量控制措施的有效性，以验证安全要求是否得到满足”。GB/T 22080—2008 也要求组织“确定如何测量已选控制措施或控制措施组的有效性，并指明如何用这些测量措施来评估控制措施的有效性，以产生可比较的和可再现的结果。”

组织用以满足 GB/T 22080—2008 规定的测量要求所采用的方法，将基于一些重要因素而变化，包括组织所面临的信息安全风险、组织规模、可用的资源、适用的法律法规、规章和合同要求。为了防止过多的资源被用于 ISMS 的一些活动而损害其他活动，慎重选择和证明用于满足测量要求的方法是非常重要的。理想情况下，持续的测量活动将把组织的正常运作和最小的额外资源需求结合在一起。

为满足 GB/T 22080—2008 规定的测量要求，本标准建议基于以下活动：

a) 制定测度(即基本测度、导出测度和指标)；
b) 实施和运行信息安全测量方案；
c) 收集和分析数据；
d) 产生测量结果；
e) 与利益相关者沟通产生的测量结果；
f) 将测量结果作为 ISMS 相关决策的有利因素；
g) 用测量结果识别已实施的 ISMS 的改进需要，包括 ISMS 的范围、策略、目标、控制措施、过程和规程；
h) 促进信息安全测量方案的持续改进。

组织规模是影响组织完成测量的能力的因素之一。一般来说，业务的规模和复杂性以及信息安全的重要性，都会影响需要的测量程度，其中测量程度是针对已选的测度数量以及收集和分析数据的频率来说的。对于中小型企业来说，一个不太全面的信息安全测量方案就足够了。而对大型企业，则需要实施和运行多个信息安全测量方案。

单个信息安全测量方案可满足小型组织，而大型企业可能需要多个信息安全测量方案。

本标准产生的文件，有助于证明正在被测量和评估的控制措施的有效性。

信息技术　安全技术
信息安全管理　测量

1　范围

为了评估按照GB/T 22080—2008规定实施的信息安全管理体系(Information Security Management System,简称ISMS)和控制措施或控制措施组的有效性,本标准提供了如何编制测度和测量以及如何使用的指南。

本标准适用于各种类型和规模的组织。

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 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 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中界定的以及下列术语和定义适用于本文件。

3.1

分析模型　analytical model

将一个或多个基本和/或导出测度关联到决策准则的算法或计算。

[GB/T 20917—2007]

3.2

属性　attribute

可由人或自动化工具定量或定性辨别的对象特征或特性。

[GB/T 20917—2007]

3.3

基本测度　base measure

用某个属性及其量化方法定义的测度。

[GB/T 20917—2007]

注:一个基本测度在功能上独立于其他测度。

3.4

数据　data

赋予基本测度、导出测度和(或)指标的值的集合。

[GB/T 20917—2007]