ICS 35.040
L 80

# 中华人民共和国国家标准

GB/T 30273—2013

# 信息安全技术
# 信息系统安全保障通用评估指南

**Information security technology—Common methodology for information systems security assurance evaluation**

2013-12-31 发布　　2014-07-15 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 …… Ⅲ
引言 …… Ⅳ
1　范围 …… 1
2　规范性引用文件 …… 1
3　术语和定义 …… 1
4　符号和缩略语 …… 2
5　概述 …… 3
5.1　GB/T 20274 系列标准和本标准结构之间的关系 …… 3
5.2　评估裁决 …… 3
6　通用评估模型 …… 4
6.1　评估模型概述 …… 4
6.2　评估输入任务 …… 4
6.3　评估活动 …… 5
6.4　评估输出任务 …… 5
7　信息系统保护轮廓评估 …… 9
7.1　概述 …… 9
7.2　目的 …… 9
7.3　评估相关要求 …… 9
7.4　评估活动 …… 9
8　信息系统安全目标评估 …… 18
8.1　概述 …… 18
8.2　目的 …… 18
8.3　评估要求 …… 18
8.4　评估活动 …… 19
9　信息系统安全保障措施评估 …… 30
9.1　信息系统安全技术保障措施评估 …… 30
9.2　信息系统安全管理保障措施评估 …… 74
9.3　信息系统安全工程保障措施评估 …… 113
10　信息系统保障级评估 …… 126
10.1　概述 …… 126
10.2　目的 …… 126
10.3　相互关系 …… 126
10.4　ISAL1(基本执行)评估活动 …… 126
10.5　ISAL2(计划和跟踪级)评估活动 …… 127
10.6　ISAL3(充分定义级)评估活动 …… 129

10.7 ISAL4(量化控制级)评估活动 …… 131
10.8 ISAL5(持续改进级)评估活动 …… 132
附录 A(规范性附录) 通用评估指南 …… 134
参考文献…… 135

# 前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

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。

本标准主要起草单位:中国信息安全测评中心、华北计算技术研究所、中国信息安全测评中心华中测评中心。

本标准主要起草人:江常青、张利、姚轶崭、佟鑫、班晓芳、翁正军、王鸿娴。

# 引　言

本标准是GB/T 20274系列标准《信息安全技术　信息系统安全保障评估框架》的配套指南文件。

本标准的目标读者是采用GB/T 20274系列标准对信息系统进行安全性评估的评估者以及评估申请者、开发者、ISPP/ISST编制者。

# 信息安全技术
# 信息系统安全保障通用评估指南

## 1 范围

本标准描述了评估者在使用 GB/T 20274 系列标准所定义的准则进行评估时需要完成的评估活动，为评估者在具体评估活动中的评估行为和活动提供指南。

本标准适用于采用 GB/T 20274 系列标准对信息系统进行安全性的评估和对 ISPP/ISST 的评估。

## 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 20274.1—2006 信息安全技术 信息系统安全保障评估框架 第 1 部分：简介和一般模型

GB/T 20274.2—2008 信息安全技术 信息系统安全保障评估框架 第 2 部分：技术保障

GB/T 20274.3—2008 信息安全技术 信息系统安全保障评估框架 第 3 部分：管理保障

GB/T 20274.4—2008 信息安全技术 信息系统安全保障评估框架 第 4 部分：工程保障

## 3 术语和定义

下列术语和定义适用于本文件。

3.1

**核查 check**

评估者采用简单比较形成一个裁决。

注：使用此动词的语句描述了需要核查的内容。

3.2

**评估交付件 evalution deliverable**

评估者为执行一个或多个评估活动所必需的，来自申请者或开发者的任何资源。

3.3

**评估证据 evaluation evidence**

有形的评估交付件。

3.4

**评估报告 evaluation technical report**

由评估者编写的以文档形式记录总体裁决及其理由的报告。

3.5

**检查 examination**

评估者采用专业技能分析形成一个裁决。

注：使用此动词的语句表明哪些是需要分析的以及什么样的性质需要分析。

3.6

**解释 interpretation**

对标准内容的一种澄清或详述。