ICS 35.030
CCS L 80

中华人民共和国国家标准

GB/T 20274.1—2023
代替 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

**Information security technology—
Evaluation framework for information systems security assuresure—
Part 1:Introduction and general model**

2023-03-17 发布　　2023-10-01 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

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

本文件是GB/T 20274《信息安全技术　信息系统安全保障评估框架》的第1部分。GB/T 20274已经发布了以下部分：

——第1部分：简介和一般模型；

——第2部分：技术保障；

——第3部分：管理保障；

——第4部分：工程保障。

本文件代替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》，与GB/T 20274.1—2006相比，除结构调整和编辑性改动外，主要技术变化如下：

a) 删除了不适用界限（见2006年版的第1章）；

b) 更改了“信息系统”和“信息系统安全保障”的定义，删除了其他术语，增加了“组织安全策略”术语和定义，删除了缩略语（见第3章，2006年版的3.1和3.2）；

c) 更改了目标读者的描述（见第4章，2006年版的4.2）；

d) 删除了“评估上下文”和“信息系统安全保障评估框架的文档结构”（见2006年版的4.3和4.4）；

e) 将“一般模型”更改为“信息系统安全保障模型和等级”，增加了保障能力等级概念（见第5章，2006年版的5.1和5.2）；

f) 将“信息系统安全保障描述材料”更改为“信息系统安全保障要素”，删除了ISPP和ISST的内容（见第6章，2006年版的5.5）；

g) 删除了“信息安全整体和应用”和“安全保障要求的使用”（见2006年版的5.3.4和5.5.3）；

h) 更改了“信息系统安全保障评估概念和关系”的图表及文字描述（见7.1，2006年版的5.3.2）；

i) 将“在信息系统生命周期中的安全保障”更改为“信息系统安全保障评估内容”（见7.2，2006年版的5.2.2.2）；

j) 更改了“信息系统安全保障评估内容”的文字描述和图表内容（见7.2，2006年版的5.3.3）；

k) 将“信息系统安全保障评估和评估结果”更改为“信息系统安全保障评估判定”，删除了有关ISPP和ISST相关的内容，增加了评估准则和保障等级判定要求（见7.3，2006年版的第6章）。

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专利的责任。

本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。

本文件起草单位：中国信息安全测评中心、国家信息技术安全研究中心、国家计算机网络与信息安全管理中心、公安部第一研究所、国家工业信息安全发展研究中心、国家信息中心、吉林信息安全测评中心、四川省信息安全测评中心、广东省信息安全测评中心、陕西省网络与信息安全测评中心、中国南方电网有限责任公司、南方电网数字电网集团有限公司、昆仑数智科技有限公司、泰康保险集团股份有限公司、中国医学科学院北京协和医院、华润数科控股有限公司、四川大学、北京百度网讯科技有限公司、浪潮云信息技术股份公司、浙江木链物联网科技有限公司、杭州安恒信息技术股份有限公司、沈阳东软系统集成工程有限公司、启明星辰信息技术集团股份有限公司、北京神州绿盟科技有限公司、鼎铉商用密码测评技术（深圳）有限公司、中国电子科技网络信息安全有限公司、山西轩辕信息安全技术有限公司。

本文件主要起草人：任望、邸丽清、江常青、李斌、徐秋伊、梁智溢、张普含、杜宇鸽、宋璟、谢丰、彭勇、

孟晓阳、郭昊、刘占丰、昌彦伟、庞智、梁伟、宫月、王丹琛、张晓娜、陈禹、高强、李秋香、史大为、陈永刚、赵增振、于盟、张格、潘承亚、杨天识、陶蓉、吕华辉、明哲、滕征岑、刘磊、陈靓、万娟、卿鄴波、王美玲、郭宾、王文佳、赵呈东、朱卫国、张敏、王海棠、唐晓莉、鲍捷、李滨丞、赵少飞、谭锐能、李智林、叶建伟。

本文件及其所代替文件的历次版本发布情况为：

——2006 年首次发布为 GB/T 20274.1—2006；

——本次为第一次修订。

引　言

GB/T 20274《信息安全技术　信息系统安全保障评估框架》以GB/T 18336《信息技术　安全技术　信息技术安全评估准则》为基础，从产品扩展到信息技术系统，并进一步同其他国内外信息系统安全领域的标准和规范进行结合，扩展和补充，以形成描述和评估信息系统安全保障内容和能力的通用框架。GB/T 20274是指导信息系统安全保障评估的基础性和框架性标准，为从事信息系统安全保障工作的所有相关方(包括设计开发者工程实施者，评估者、认证认可者等)提供一种标准化、规范化的通用描述语言、结构和方法。GB/T 20274旨在给出信息系统安全保障的基本概念和模型，确立在技术、管理和工程方面的安全保障要求和能力等级要求，由四个部分构成。

——第1部分：简介和一般模型。目的在于给出信息系统安全保障的基本概念和模型，提出信息系统安全保障评估的框架。

——第2部分：技术保障。目的在于确立信息系统在技术方面的安全保障基本要求及相应的能力等级要求。

——第3部分：管理保障。目的在于确立信息系统在管理方面的安全保障基本要求及相应的能力等级要求。

——第4部分：工程保障。目的在于确立信息系统在工程方面的安全保障基本要求及相应的能力等级要求。

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

1 范围

本文件给出了信息系统安全保障的基本概念和模型,提出了信息系统安全保障评估框架。

本文件适用于指导系统建设者、运营者、服务提供者和评估者等开展信息系统安全保障工作。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中,注日期的引用文件,仅该日期对应的版本适用于本文件;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 18336.1—2015 信息技术 安全技术 信息技术安全评估准则 第1部分:简介和一般模型

GB/T 25069—2022 信息安全技术 术语

3 术语和定义

GB/T 25069—2022 和 GB/T 18336.1—2015 中界定的以及下列术语和定义适用于本文件。

3.1

信息系统 information system

应用、服务、信息技术资产或其他信息处理组件的组合。

注1:信息系统通常由计算机或者其他信息终端及相关设备组成,并按照一定的应用目标和规则进行信息处理或过程控制。

注2:典型的信息系统如办公自动化系统、云计算平台/系统、物联网、工业控制系统以及采用移动互联网技术的系统等。

[来源:GB/T 29246—2017,2.39,有修改]

3.2

信息系统安全保障 information system security assurance

对信息系统的安全属性及功能、效率进行保障的一系列适当行为或过程。

3.3

组织安全策略 organizational security policies

组织为确保其运行而制定的若干安全规则、规程、实践和指南。

[来源:GB/T 25069—2022,3.817]

4 概述

与信息系统安全保障评估工作相关的相关方,一般包括信息系统建设者、信息系统运营者、服务提