ICS 35.030
CCS L 80

中华人民共和国国家标准

GB/T 20274.2—2026
代替 GB/T 20274.2—2008，GB/T 20274.3—2008，GB/T 20274.4—2008

网络安全技术　信息系统安全保障评估框架　第2部分：安全保障要求

Cybersecurity technology—Evaluation framework for information systems security assurance—Part 2: Security assurance requirements

2026-05-25 发布　　2026-12-01 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《网络安全技术　信息系统安全保障评估框架》的第2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：安全保障要求。

本文件代替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》。本文件与GB/T 20274.2—2008、GB/T 20274.3—2008和GB/T 20274.4—2008相比，除结构调整和编辑性改动外，主要技术变化如下：

——增加了信息系统安全保障框架的描述（见第4章）；

——更改了技术保障组件的类别及相关描述（见第6章，GB/T 20274.2—2008版的第7章～第17章）；

——更改了管理保障组件的类别及相关描述（见第7章，GB/T 20274.3—2008版的第7章～第18章及GB/T 20274.4—2008版的第7章～第9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。

本文件由全国网络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、国家信息中心、南方电网数字电网集团信息通信科技有限公司、云南电网有限责任公司数智运营中心、南航数智科技（广东）有限公司、国家石油天然气管网集团有限公司、公安部第三研究所、吉林信息安全测评中心、广东省信息安全测评中心、启明星辰信息技术集团股份有限公司、天翼安全科技有限公司、浪潮电子信息产业股份有限公司、浪潮软件集团有限公司、北京数安行科技有限公司、中国移动通信集团有限公司、中国银联股份有限公司、昆仑数智科技有限责任公司、华润（集团）有限公司、国家计算机病毒应急处理中心、中国电子科技集团公司第十五研究所、清华大学、北京时代新威信息技术有限公司、广州市昊恒信息科技有限公司、国网思极网安科技（北京）有限公司、中国信息安全测评中心华中测评中心、陕西省网络与信息安全测评中心、中科信息安全共性技术国家工程研究中心有限公司、中国医学科学院北京协和医院、工业和信息化部电子第五研究所、北京源堡科技有限公司、北京中测安华科技有限公司、四川省数字经济研究中心、中贸促信息技术有限责任公司、杭州安恒信息技术股份有限公司、中国电力科学研究院有限公司、深圳开源互联网安全技术有限公司、山西轩辕信息安全技术有限公司、北京神州绿盟科技有限公司、奇安信网神信息技术（北京）股份有限公司、深信服科技股份有限公司、北京禹宏信安科技有限公司、上海观安信息技术股份有限公司。

本文件主要起草人：宋璟、温哲、邸丽清、王庆、张毅、李斌、任望、江常青、肖鹏、刘占丰、杨天识、梁露露、王文佳、梁伟、赵媛、张鹏、刘玉红、樊凯、黄伟键、王学力、杨杰、张雪莲、昌彦伟、叶晓俊、吴强、宋皓、孟晓阳、阮晶晶、孙晓丽、于园园、陈永刚、李祉岐、陈芳、张峰、崔庆虎、李滨丞、吴文超、谭近军、王作为、孙文龙、姚雨秋、胡建勋、董晶晶、袁泉、于敏、宋好好、程虎、张强、肖红阳、王颉、王丹琛、赖永晓、徐可、彭勇、张普含、杜宇鸽、田斌、杨光、赵佳璐、刘彦钊、胡超群、王新洋、孙子玉、伊玮珑、石磊、王文君。

本文件及其所代替文件的历次版本发布情况为：

——2008年首次发布为GB/T 20274.2—2008、GB/T 20274.3—2008、GB/T 20274.4—2008；

——本次为第一次修订，合并了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》的内容。

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《网络技术安全　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，确立在技术和管理方面的安全保障要求和能力等级要求，拟由两个部分构成。

——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：安全保障要求。目的在于确立信息系统安全保障评估框架和安全保障能力等级，规定技术保障组件和管理保障组件的要求。

为了确立信息系统在技术、管理和工程方面的安全保障要求和能力等级，我国在 2008 年发布了 GB/T 20274.2《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《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《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》。为了配合《中华人民共和国网络安全法》和《中华人民共和国数据安全法》的实施，进一步落实《反间谍安全防范工作规定》中非涉密信息系统的相关要求，适应新技术、新应用发展下信息系统安全保障体系的构建和能力评价工作的开展，需对 GB/T 20274.2、GB/T 20274.3、GB/T 20274.4 进行修改。本次修订以风险和策略为核心，借鉴通用评估准则(CC)的思想，围绕信息系统整个生存周期，合并 GB/T 20274.2、GB/T 20274.3、GB/T 20274.4 三个部分为一个部分 GB/T 20274.2，以确立信息系统安全保障评估框架和安全保障能力等级，规范技术保障组件和管理保障组件的要求。

网络安全技术　信息系统安全保障评估框架　第2部分:安全保障要求

1　范围

本文件确立了信息系统安全保障评估框架和安全保障能力等级,规定了技术保障组件和管理保障组件的要求。

本文件适用于指导信息系统建设者、运营者和评估者等开展信息系统安全保障相关工作。

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 20274.1　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 25069　信息安全技术　术语

GB/T 35273　信息安全技术　个人信息安全规范

GB/T 37964　信息安全技术　个人信息去标识化指南

GB/T 37988　信息安全技术　数据安全能力成熟度模型

GB/T 42460　信息安全技术　个人信息去标识化效果评估指南

GB/T 43697　数据安全技术　数据分类分级规则

GB 50174　数据中心设计规范

3　术语和定义

GB/T 25069 和 GB/T 20274.1 界定的以及下列术语和定义适用于本文件。

3.1

基本实践　base practices

在信息系统安全保障过程中,为了达成特定目标而执行一系列标准、规范或其他相关基础的活动。

注:这些实践是确保信息系统安全、稳定和高效运行的基础。

4　信息系统安全保障评估框架

4.1　安全保障评估模型

在 GB/T 20274.1 给出的信息系统安全保障模型的基础上,细化了保障要素,完善了信息系统安全保障评估框架,如图1所示。