



中华人民共和国国家标准

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

Information security technology—
Evaluation framework for information systems security assurance—
Part 4: Engineering assurance

2008-07-18 发布

2008-12-01 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	III
1 范围	1
2 规范性引用文件	1
3 术语和定义	1
4 本部分的结构	1
5 信息系统安全工程保障框架	2
5.1 信息系统安全工程保障概述	2
5.2 信息系统安全工程保障控制	2
5.3 信息系统安全工程能力成熟度级别	4
6 信息安全工程保障控制类结构	4
6.1 概述	4
6.2 安全工程保障控制类结构	4
6.3 安全工程保障控制子类结构	5
6.4 安全工程保障控制组件结构	5
7 PRM 安全工程保障控制类:风险过程	6
7.1 风险过程安全工程保障控制类介绍	6
7.2 系统定义(PRM_SDF)	7
7.3 评估威胁(PRM_ATT)	7
7.4 评估脆弱性(PRM_AVL)	10
7.5 评估影响(PRM_AIM)	12
7.6 评估安全风险(PRM_ASR)	15
8 PEN 安全工程保障控制类:工程过程	17
8.1 工程过程安全工程保障控制类介绍	17
8.2 确定安全要求(PEN_ISR)	18
8.3 高层安全设计(PEN_HSD)	21
8.4 详细安全设计(PEN_DSD)	22
8.5 安全工程实施(PEN_SEE)	23
8.6 提供安全输入(PEN_PSI)	26
8.7 监视安全态势(PEN_MSP)	29
8.8 管理安全控制(PEN_MSC)	32
8.9 协调安全(PEN_COS)	35
9 PAS 安全工程保障控制类:保障过程	36
9.1 保障过程安全工程保障控制类介绍	36
9.2 验证和确认安全(PAS_VVS)	37
9.3 建立保证证据(PAS_EAE)	39
10 安全工程保障控制类能力级	41
10.1 概述	41
10.2 安全工程能力级别说明	41

10.3 信息系统安全工程能力级别要求 44

参考文献 45

图 1 安全工程过程生命周期 3

图 2 安全工程保障控制类结构 4

图 3 安全工程保障控制子类结构 5

图 4 安全工程保障控制组件结构 6

图 5 风险过程说明 7

图 6 系统定义(PRM_SDF)安全工程保障控制子类分解 7

图 7 评估威胁(PRM_ATT)安全工程保障控制子类分解 8

图 8 评估脆弱性(PRM_AVL)安全工程保障控制子类分解 10

图 9 评估影响(PRM_AIM)安全工程保障控制子类分解 13

图 10 评估安全风险(PRM_ASR)安全工程保障控制子类分解 15

图 11 工程过程安全工程保障控制类介绍 18

图 12 确定安全要求(PEN_ISR)安全工程保障控制子类分解 18

图 13 高层安全设计(PEN_HSD)安全工程保障控制子类分解 21

图 14 详细安全设计(PEN_DSD)安全工程保障控制子类分解 22

图 15 安全工程实施(PEN_SEE)安全工程保障控制子类分解 24

图 16 提供安全输入(PEN_PSI)安全工程保障控制子类分解 26

图 17 监视安全态势(PEN_MSP)安全工程保障控制子类分解 29

图 18 管理安全控制(PEN_MSC)安全工程保障控制子类分解 32

图 19 协调安全(PEN_COS)安全工程保障控制子类分解 35

图 20 保障过程安全工程保障控制类说明 37

图 21 验证和确认安全(PAS_VVS)安全工程保障控制子类分解 37

图 22 建立保证证据(PAS_EAE)安全工程保障控制子类分解 39

图 23 信息系统安全工程能力要求级别图 44

表 1 安全工程生命周期和过程域对应表 3

前 言

GB/T 20274《信息安全技术 信息系统安全保障评估框架》分为以下四个部分：

——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

本部分是 GB/T 20274 的第 4 部分。

本部分由全国信息安全标准化技术委员会提出并归口。

本部分起草单位：中国信息安全产品测评认证中心。

本部分主要起草人：吴世忠、王海生、陈晓桦、王贵骊、李守鹏、江常青、彭勇、张利、姚轶崙、班晓芳、李静、王庆、邹琪、钱伟明、江典盛、陆丽、孙成昊、门雪松、杜宇鸽、杨再山。

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

1 范围

GB/T 20274 的本部分建立了信息系统安全工程保障的框架，确立了组织机构启动、实施、维护、评估和改进信息安全工程的指南和通用原则。GB/T 20274 的本部分定义和说明了信息系统安全工程保障工作中反映组织机构信息安全工程保障能力的安全工程能力级，以及提供组织机构信息安全工程保障内容的安全工程保障控制类要求。

GB/T 20274 的本部分适用于启动、实施、维护、评估和改进信息安全工程的组织机构和涉及信息系统安全工程工作的所有用户、开发人员和评估人员。

2 规范性引用文件

下列文件中的条款通过 GB/T 20274 的本部分的引用而成为本部分的条款。凡是注日期的引用文件，其随后所有的修改单（不包括勘误的内容）或修订版均不适用于本部分，然而，鼓励根据本部分达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件，其最新版本适用于本部分。

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

3 术语和定义

GB/T 20274.1 确定的以及以下术语和定义适用于 GB/T 20274 的本部分。

3.1.1

确认 validation

解决方案满足用户的运行安全需求。

3.1.2

验证 verification

解决方案满足安全要求。

4 本部分的结构

GB/T 20274 的本部分的组织结构如下：

- a) 第1章介绍了 GB/T 20274 的本部分的范围；
- b) 第2章介绍了 GB/T 20274 的本部分所规范引用的标准；
- c) 第3章描述了适用于 GB/T 20274 的本部分的术语和定义；
- d) 第4章描述了 GB/T 20274 的本部分的组织结构；
- e) 第5章描述了信息系统安全工程保障框架，并进一步概述了工程保障控制类和工程能力级；
- f) 第6章描述了信息安全工程保障控制类的规范描述结构和要求；
- g) 第7章到第9章详述了提供信息安全工程保障内容的3个信息安全工程类的详细要求；