ICS 35.040
L 80

中华人民共和国国家标准

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

**Information security technology—
Evaluation framework for information systems security assurance—
Part 3: Management 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　信息安全管理保障框架 …… 2
5.1　信息管理保障概述 …… 2
5.2　信息安全管理保障控制 …… 2
5.3　信息安全保障管理能力级 …… 3
6　信息安全管理保障控制类结构 …… 4
6.1　概述 …… 4
6.2　管理保障控制类结构 …… 4
6.3　管理保障控制子类结构 …… 4
6.4　管理保障控制组件结构 …… 5
6.5　允许的操作 …… 6
7　MRM 管理保障控制类:风险管理 …… 6
7.1　对象确立(MRM_TEM) …… 6
7.2　风险评估(MRM_RAM) …… 8
7.3　风险控制(MRM_RCT) …… 8
7.4　沟通与监控(MRM_CAM) …… 9
8　MSP 管理保障控制类:信息安全策略 …… 10
8.1　信息安全策略(MSP_SPL) …… 10
9　MSO 管理保障控制类:信息安全组织机构 …… 12
9.1　信息安全的管理支持(MSO_SOM) …… 12
9.2　信息安全组织架构(MSO_ORG) …… 13
9.3　信息安全职责(MSO_RES) …… 13
9.4　沟通协作(MSO_CAC) …… 14
10　MPS 管理保障控制类:人员安全 …… 15
10.1　人员审查(MPS_PEC) …… 15
10.2　安全意识和培训(MPS_SAT) …… 17
10.3　考核和奖惩(MPS_CRP) …… 17
10.4　人事变更(MPS_PCM) …… 18
11　MAM 管理保障控制类:资产管理 …… 18
11.1　资产登记管理(MAM_ARM) …… 19
11.2　资产管理职责(MAM_AMR) …… 19
11.3　资产分类管理(MAM_ACM) …… 20
12　MPE 管理保障控制类:物理和环境安全 …… 20
12.1　物理安全区域管理(MPE_PSA) …… 21

12.2 支撑基础设施安全(MPE_SIS) …… 23
12.3 设备安全 (MPE_EMS) …… 24
13 MCM 管理保障控制类:符合性管理 …… 25
14 MSP 管理保障控制类:信息安全规划管理 …… 28
15 MSD 管理保障控制类:系统开发管理 …… 30
16 MOP 管理保障控制类:运行管理 …… 33
17 MBD 管理保障控制类:业务持续性和灾难恢复管理 …… 44
17.1 业务持续性管理(MBD_BCM) …… 44
18 MER 管理保障控制类:应急响应管理 …… 47
18.1 汇报安全事件和安全漏洞(MER_REW) …… 47
18.2 应急响应管理(MER_IMI) …… 48
19 安全管理能力级说明 …… 50
19.1 概述 …… 50
19.2 安全管理能力级别说明 …… 50
19.3 信息系统安全保障管理能力级别应用 …… 52
参考文献 …… 54

图 1 信息系统安全管理保障控制类 …… 3
图 2 管理保障控制类结构 …… 4
图 3 管理保障控制子类结构 …… 5
图 4 管理保障控制组件结构 …… 5
图 5 风险管理(MRM)管理保障控制类分解 …… 7
图 6 信息安全策略(MSP)管理保障控制类分解 …… 10
图 7 信息安全组织机构(MSO)管理保障控制类分解 …… 12
图 8 人员安全(MPS)管理保障控制类分解 …… 15
图 9 资产管理(MAM)管理保障控制类分解 …… 18
图 10 物理和环境安全(MPE)管理保障控制类分解 …… 21
图 11 符合性管理(MCM)管理保障控制类分解 …… 25
图 12 信息安全规划管理(MSP)管理保障控制类分解 …… 29
图 13 系统开发管理(MSD)管理保障控制类分解 …… 31
图 14 运行管理(MOP)管理保障控制类分解 …… 33
图 15 业务持续性和灾难恢复管理(MBD)管理保障控制类分解 …… 44
图 16 应急响应管理(MER)管理保障控制类分解 …… 47
图 17 信息系统安全保障管理能力要求级别示例图 …… 53

前　言

GB/T 20274《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3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、王贵驷、李守鹏、江常青、彭勇、张利、姚轶崭、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3部分:管理保障

1 范围

GB/T 20274的本部分建立了信息系统安全管理保障的框架,确立了组织机构内启动、实施、维护、评估和改进信息安全管理的指南和通用原则。本部分定义和说明了信息系统安全管理保障中反映组织机构信息安全管理保障能力的安全管理能力级,以及提供组织机构信息安全管理保障内容的管理保障控制类要求。

本部分适用于涉及信息系统安全管理工作的组织机构的所有用户、开发者和评估者。

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确立的以及以下术语和定义适用于GB/T 20274的本部分。

3.1

控制

管理风险的方法,包括策略、流程、指南、实践或组织机构结构,控制可以是管理的、技术的或工程的。

注1:控制也是控制措施、保护措施的同义语。

注2:本部分中,主要讨论管理风险的管理方面的控制,即管理控制。

3.2

信息处理设施

信息处理设施是所有服务或基础设施,或放置它们的物理场所。

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管理保障框架,并进一步概述了管理保障控制类和管理能力级;

f) 第6章描述了信息安全管理保障控制类的规范描述结构和要求;