ICS 03.060
A 11

JR

中华人民共和国金融行业标准

JR/T 0071.3—2020

金融行业网络安全等级保护实施指引 第3部分：岗位能力要求和评价指引

Implementation guidelines for classified protection of cybersecurity of financial industry—Part 3：Post competency requirements and guidelines for evaluation

2020－11－11 发布　　2020－11－11 实施

中国人民银行　发布

目　　次

前言 II
引言 III
1 范围 1
2 规范性引用文件 1
3 网络安全管理组织架构 1
4 网络安全岗位和职责 2
5 网络安全岗位的能力要求 5
6 网络安全人员能力评价 6
参考文献 8

前　言

JR/T 0071《金融行业网络安全等级保护实施指引》由以下6部分构成：

——第1部分：基础和术语；

——第2部分：基本要求；

——第3部分：岗位能力要求和评价指引；

——第4部分：培训指引；

——第5部分：审计要求；

——第6部分：审计指引。

本部分为JR/T 0071的第3部分。

本部分按照GB/T 1.1—2009给出的规则起草。

本部分由中国人民银行提出。

本部分由全国金融标准化技术委员会（SAC/TC 180）归口。

本部分起草单位：中国人民银行科技司、中国银行保险监督管理委员会统计信息与风险监测部、中国金融电子化公司、北京中金国盛认证有限公司。

本部分主要起草人：李伟、陈立吾、沈筱彦、车珍、咎新、夏磊、方怡、张海燕、唐辉、李凡、王海涛、张璐、潘丽扬、邓昊、侯漫丽、孙国栋、刘文娟、乔媛、崔莹、陈雪峰、马成龙、杜巍、李瑞锋、赵方萌。

引　言

网络安全等级保护是国家网络安全保障工作的一项基本制度，金融行业重要系统关系到国计民生，是国家网络安全重点保护对象，因此需要一系列适合金融行业的等级保护标准体系作为支撑，以规范和指导金融行业等级保护工作的实施。随着云计算、移动互联、物联网、大数据等新技术的广泛应用，金融机构正根据自身发展的需要，持续推进IT架构的转型。为适应新技术、新应用和新架构情况下金融行业网络安全等级保护工作的开展，现对JR/T 0071进行修订。修订后的JR/T 0071依据国家网络安全等级保护相关要求，为金融行业的网络安全建设提供方法论、具体的建设措施及技术指导，完善金融行业网络安全等级保护体系，更好适应新技术在金融行业的应用。

金融行业网络安全等级保护实施指引
第3部分：岗位能力要求和评价指引

1 范围

本部分规定了金融机构网络安全岗位设置要求、网络安全岗位能力要求以及网络安全人员能力评价要求。

本部分适用于指导金融机构按照网络安全等级保护要求设置网络安全岗位、制定网络安全岗位能力要求以及实施网络安全人员能力评价。

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 20269 信息安全技术 信息系统安全管理要求

GB/T 22239 信息安全技术 网络安全等级保护基本要求

GB/T 25058 信息安全技术 网络安全等级保护实施指南

GB/T 28448 信息安全技术 网络安全等级保护测评要求

3 网络安全管理组织架构

按照GB/T 20269、GB/T 22239、GB/T 25058、GB/T 28448的要求，网络安全管理组织架构如图1所示。

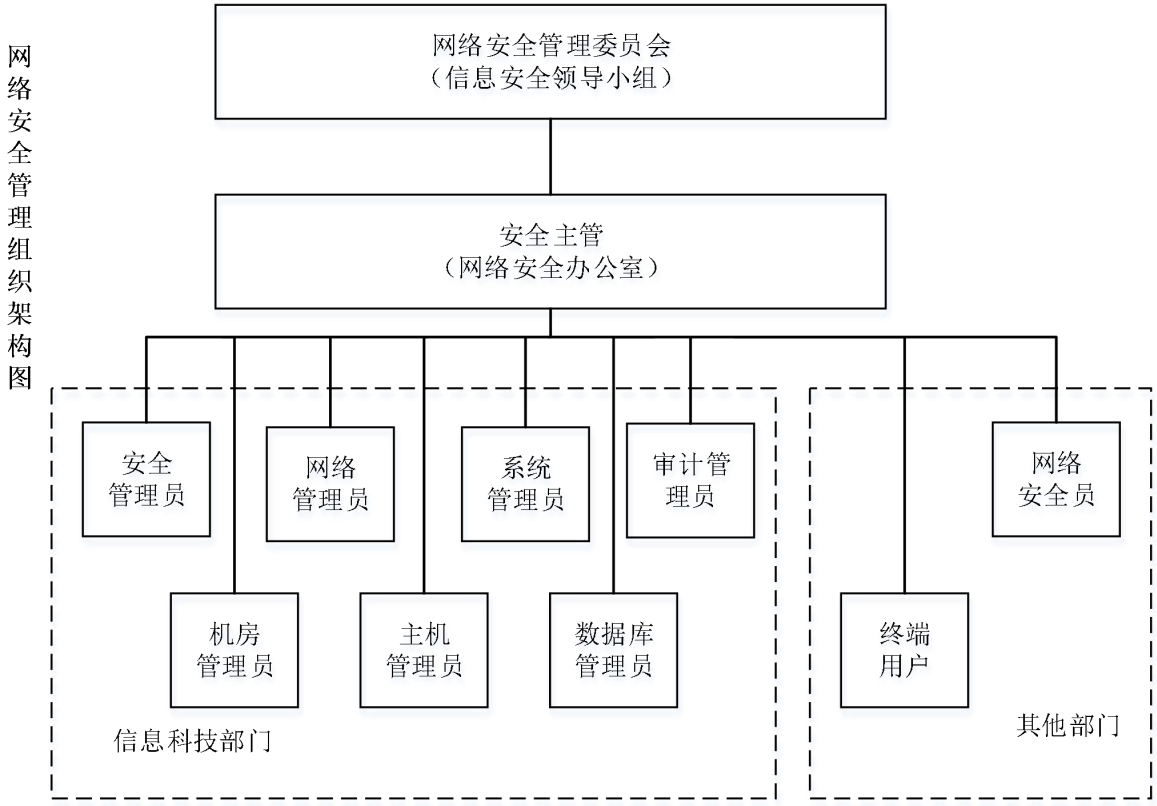

图 1　网络安全管理组织架构图

4　网络安全岗位和职责

4.1　岗位和职责

金融机构网络安全等级保护工作应遵循国家相关标准和要求，建设网络安全保障体系，确保金融机构信息资产的保密性、完整性和可用性；应划分职责并分配给相应岗位，确保所有重要的工作以有效方式执行并完成。

网络安全岗位涉及两类人员：

a)　承担网络安全职责的原有信息化工作人员。

b)　为网络安全工作单独设置的特定网络安全岗位人员。

4.2　网络安全管理委员会（领导小组）

金融机构应设立一个由高级管理层、信息科技部门和主要业务部门代表组成的网络安全管理委员会（或称信息安全领导小组）。

网络安全管理委员会应负责监督各项网络安全职责的落实，定期向董事会和高级管理层汇报网络安全战略规划的执行、网络安全预算和实际支出、网络安全的整体情况等，具体职责包括但不限于下列内容：

a)　审核并批准金融机构网络安全战略规划。

b)　作出与网络安全有关的重大事项的决策，包括网络安全组织架构调整、网络安全重大战略变更等。

c)　负责指挥、协调金融机构重大网络安全事件的处理。

d) 负责沟通协调网络安全工作中的重大事项。
e) 负责保障网络安全工作开展所需的资金、人员和设施等资源。

4.3 安全主管（网络安全办公室）

金融机构应设立安全主管（或建立网络安全办公室，可设在信息科技部门）。

安全主管应具备基本的网络安全意识，认识到网络安全工作的重要性，并提供足够的资源来支持金融机构网络安全工作的顺利开展，具体职责包括但不限于下列内容：

a) 组织落实网络安全管理委员会在网络安全管理方面的决策。
b) 负责组织网络安全保障体系的建立、实施和日常运行。
c) 负责与网络安全工作有关事项的具体协调和沟通。
d) 负责网络安全工作的执行与落实，监督、指导各部门网络安全工作的开展，并定期向网络安全管理委员会汇报。

4.4 安全管理员

金融机构信息科技部门应设立安全管理员，负责金融机构各项网络安全管理策略的制定和落实，具体职责包括但不限于下列内容：

a) 组织制定各项网络安全管理策略，并监督执行。
b) 负责防病毒和入侵检测等安全系统的选用、部署和维护。
c) 负责网络安全事件的响应和处置。
d) 组织制定网络安全应急预案，并定期组织演练。
e) 定期组织人员安全意识培训。

4.5 机房管理员

金融机构信息科技部门应设立机房管理员，负责金融机构机房安全管理策略的制定和落实，具体职责包括但不限于下列内容：

a) 负责机房的全面管理，其他人员未经允许不得入内。
b) 负责机房设备管理，其他人员未经允许不得自行使用、移动和调换设备，应确保机房各设备正常工作，出现故障及时处理。
c) 建立设备台账，记录使用、维修、软硬件升级变更等情况。
d) 负责机房环境安全管理，包括防盗窃和防破坏、防雷击、防火、防水和防潮、防静电、温湿度控制等。
e) 确保机房内设备无特殊情况下未随意关闭，所有设备与 UPS 电源连接。

4.6 网络管理员

金融机构信息科技部门应设立网络管理员，负责金融机构网络安全管理策略的制定和落实，具体职责包括但不限于下列内容：

a) 负责网络设备的维护和管理，对运行关键业务网络的主干设备配备相应的备份设备。
b) 掌握主干网络设备的配置情况及配置参数变更情况，备份各设备的配置文件。
c) 掌握用户端设备接入网络的情况，以便出现问题时可迅速定位。
d) 掌握与外部网络的连接配置，监督网络通信状况。
e) 实时监控整个局域网的运转和网络通信流量情况，及时发现故障征兆并进行处理。

4.7 主机管理员

金融机构信息科技部门应设立主机管理员，负责金融机构主机安全管理策略的制定和落实，具体职责包括但不限于下列内容：

a) 负责服务器、终端设备的维护和管理。
b) 掌握服务器的配置情况及配置参数变更情况，备份重要设备的配置文件。
c) 对运行关键业务的服务器配备相应的备份设备。
d) 实时监控服务器的运转情况，及时发现故障征兆并进行处理。
e) 负责主机设备操作系统及基本应用的配置、安装、管理及维护。

4.8 系统管理员

金融机构信息科技部门应设立系统管理员，负责金融机构系统应用安全管理策略的制定和落实，具体职责包括但不限于下列内容：

a) 负责各应用系统的选用、安装和维护工作。
b) 负责各应用系统日常巡检，根据各应用系统巡检结果以及日常事件处理情况报告系统状态。
c) 负责对应用系统使用人员进行使用和维护方面的培训工作，并提供日常使用指导。
d) 组织协调有关人员管理系统初始化和基础数据的录入和更新，保证其准确性和及时性。
e) 负责应用系统各用户密码的初始化和权限的分配、管理工作。

4.9 数据库管理员

金融机构信息科技部门应设立数据库管理员，负责金融机构数据安全及备份恢复管理策略的制定和落实，具体职责包括但不限于下列内容：

a) 对数据库的运行状态、日志文件、备份、空间使用情况、系统资源使用情况进行检查，及时发现并解决问题。
b) 对数据库对象的空间扩展和数据增长情况进行监控，定期检查数据库对象状态。
c) 定期检查数据库备份有效性，并将数据库备份进行异地保存。
d) 定期组织数据恢复演练，确保备份数据的有效性。
e) 定期检查数据库用户权限，及时清除不必要的用户和用户权限。

4.10 审计管理员

金融机构信息科技部门应设立审计管理员，负责审查金融机构各项网络安全策略和网络安全管理制度的执行情况，具体职责包括但不限于下列内容：

a) 实施网络安全审计制度和流程，制订和执行网络安全审计计划。
b) 审查各项网络安全策略的执行情况。
c) 审查各项网络安全管理制度的执行情况。
d) 对网络安全管理岗位相关人员的日常操作进行跟踪、分析和监督检查。
e) 对审计日志进行定期分析，以发现违规行为和可疑问题。

4.11 网络安全员（或信息安全员）

金融机构各部门应设立网络安全员（或信息安全员），负责各部门网络安全工作的组织和落实，具体职责包括但不限于下列内容：

a) 负责网络安全工作的联络和协调。
b) 负责在本部门内推广落实机构的各项网络安全管理策略。
c) 负责通过组织培训等活动，提高本部门员工的网络安全意识和技能。
d) 负责整理、核查本部门网络安全记录。

e） 负责配合机构安排的各种网络安全检查。

4.12 终端用户

金融机构所有终端用户应分配相应的网络安全职责，具体职责包括但不限于下列内容：

a） 熟悉机构的各项网络安全策略并遵照执行。

b） 及时报告发现的网络安全弱点和网络安全事件。

5 网络安全岗位的能力要求

5.1 网络安全管理委员会能力要求

网络安全管理委员会应了解网络安全的重要性，并积极支持金融机构开展网络安全工作。

5.2 安全主管能力要求

安全主管应熟悉网络安全政策法规和技术标准，具备整体网络安全规划的能力，能开发出符合业务战略的安全架构，并能够对其他级别的网络安全人员实施有效管理，保持对目前威胁和脆弱性的了解，掌握解决威胁和脆弱性的最新安全技术。

5.3 安全管理员能力要求

安全管理员应至少具备下列能力：

a） 熟悉风险评估、风险管理等网络安全管理相关知识。

b） 精通网络安全策略的规划及实施。

c） 了解网络安全策略推广、培训的方式方法。

d） 了解计算机病毒及防治、密码学和入侵检测等网络安全技术的原理及发展趋势。

e） 熟悉防病毒软件、入侵检测和漏洞扫描等常用安全产品的使用，并能够进行配置以及故障排查。

5.4 机房管理员能力要求

机房管理员应至少具备下列能力：

a） 熟悉机房管理相关知识。

b） 熟悉机房设备及其软件，能对机房设备进行熟练操作。

c） 能对机房设备进行日常维护和管理，确保设备的正常运行。

d） 熟悉 UPS、空调、消防、综合布线、门禁、CCTV（Closed Circuit Television）等领域的知识。

5.5 网络管理员能力要求

网络管理员应至少具备下列能力：

a） 精通计算机和网络维护，熟悉局域网架构，具备良好的网络规划、组建、维护和独立处理网络系统故障的能力。

b） 熟悉路由器、交换机、防火墙、VPN（Virtual Private Network）等网络设备的设置与管理。

c） 熟悉 IP 路由及交换技术，熟悉常用路由协议，掌握各种网络协议的基本配置方法。

d） 掌握操作系统的一般安装和配置方法，例如 Windows、Linux 和 UNIX 等系统。

e） 熟练使用基本的网络管理软件等。

5.6 主机管理员能力要求

主机管理员应至少具备下列能力：

a) 熟悉服务器和终端的安全运维、安全防护、负载平衡、漏洞检查、故障排查、备份和灾难恢复方法。
b) 熟练掌握 Windows、Linux 和 UNIX 等操作系统的安装、应用、维护及管理。
c) 熟悉掌握 Web、Mail、FTP、SQLServer、Mysql 等服务器的配置与管理。
d) 熟练使用基本的服务器管理软件等。

5.7 系统管理员能力要求

系统管理员应至少具备下列能力：

a) 熟悉系统的主流技术架构。
b) 熟悉 Windows、Linux 和 UNIX 等应用服务器的安装和配置。
c) 熟悉与应用系统相关的网络安全管理及控制：账户和权限创建、回收及监控等安全控制，权限检查及管理等。
d) 能够对应用系统性能进行监控及优化。

5.8 数据库管理员能力要求

数据库管理员应至少具备下列能力：

a) 熟悉数据库的安装和维护。
b) 能够对数据库的故障进行分析，并具备解决能力。
c) 熟练使用数据库管理软件，能对数据库运行状态进行监控。
d) 能够根据实际需求制定适当的备份策略，并实施备份。
e) 能够对数据库进行有效恢复。

5.9 审计管理员能力要求

审计管理员应至少具备下列能力：

a) 熟悉安全审计要求和流程等网络安全管理相关知识。
b) 了解网络安全策略的规划及实施，熟悉本机构网络安全策略。
c) 了解网络安全制度的制定及实施，熟悉本机构网络安全制度的要求。
d) 熟悉日志审计、分析和统计等技术。

5.10 网络安全员能力要求

各部门网络安全员（或信息安全员）应至少具备下列能力：

a) 了解网络安全的相关知识，例如风险评估、备份与恢复、防病毒、访问控制等。
b) 熟悉本机构制定的各项网络安全策略。
c) 熟悉本机构部署的各项网络安全产品。

5.11 终端用户能力要求

金融机构所有终端用户应具备基本的网络安全意识，了解网络安全的重要性，应熟悉其工作岗位所适用的网络安全策略要求，并能遵照执行。

6 网络安全人员能力评价

6.1 总则

为确保各金融机构网络安全工作人员具备所需的能力，应对其进行能力评价，并对评价进行策划、实施和记录，以提供客观、一致、公正和可信的评价结果。对金融机构网络安全工作人员的评价有以下不同的阶段：

a) 对希望从事网络安全工作的人员进行初始评价。
b) 对网络安全人员的能力评价。
c) 对网络安全人员表现的持续评价。

6.2 评价过程

6.2.1 识别岗位要求

对网络安全人员实施能力评价，应首先识别其工作岗位所需的能力要求，网络安全岗位能力要求的识别，见第5章。

6.2.2 设立评价准则

针对所识别的岗位要求，应设立能力评价准则，例如将在工作中已经证实的个人素质、知识或技能表现作为评价准则之一。

6.2.3 选择评价方法

评价可以由一人或一个小组使用下列一种或多种方法进行：

a) 面谈：采用提问交流方式，评价个人素质、知识和技能水平。
b) 考核：采用笔试或实际操作等方式，评价个人素质、知识和技能水平。
c) 观察：对员工的日常工作进行见证。
d) 反馈：采用调查表或问卷表等方式，获取其他员工的正面或负面意见。
e) 评审：采用会议讨论方式，对员工能力进行评价。

在使用上述评价方法时，注意：

a) 应至少选取“考核”作为其中一种评价方法。
b) 宜使用综合的方法以保证结果是客观、一致、公正和可信的。

6.2.4 实施评价

在这个步骤中，将收集到的网络安全人员相关信息与6.2.2所设立的评价准则进行比较，当人员不符合准则时，则应组织安排适当的培训，并进行再评价。

参 考 文 献

[1] GB 17859 计算机信息系统安全保护等级划分准则
[2] GB/T 22240 信息安全技术 网络安全等级保护定级指南