ICS 03.060
A 11

JR

中华人民共和国金融行业标准

JR/T 0071.4—2020

金融行业网络安全等级保护实施指引 第4部分：培训指引

Implementation guidelines for classified protection of cybersecurity of financial industry—Part 4：Guidelines for training

2020－11－11 发布　　2020－11－11 实施

中国人民银行　　发布

目　　次

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4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、孙国栋、刘文娟、侯漫丽、赵方萌、乔媛、崔莹、陈雪峰、马成龙、杜巍、李瑞锋。

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4部分：培训指引

1 范围

本部分规定了网络安全培训的培训目标、培训原则、培训计划、培训对象、培训内容要求、培训实施、培训考核和培训档案管理。

本部分适用于实施网络安全等级保护的金融机构、测评机构和金融行业网络安全等级保护主管部门。

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 培训目标

按照GB/T 20269、GB/T 22239、GB/T 25058、GB/T 28448的要求，金融机构应开展网络安全培训工作。通过实施金融行业网络安全培训，使金融机构相关人员具备网络安全等级保护基本知识、网络安全基本知识和技能，为金融机构有效实施网络安全等级保护工作提供人力资源保障。

4 培训原则

培训应遵循以下原则：

a) 个人技能培训与企业培训相结合。

b) 短期培训为主，长期培训为辅。

c) 以网络安全等级保护相关岗位需求为牵引，开展多样化培训。

5 培训计划

培训计划应包含以下内容：

a) 年度培训计划：为贯彻落实网络安全等级保护制度要求，金融机构应制定网络安全年度培训计划，重点针对网络安全等级保护相关管理人员和新入职人员进行培训。网络安全年度培训应纳入机构总体年度培训计划。

b) 计划要求：培训计划应明确培训目标、培训内容、培训时间、参与培训人员、培训方式、培训所需资源、培训经费预算和考核要求等。

6 培训对象

以机构网络安全等级保护相应岗位要求为基础，培训对象主要包括管理层人员、网络安全等级保护实施人员及相关其他人员（或部门）：

a) 机构管理层：主要包括董事会成员、首席执行官、审计委员会、法律部门等。
b) 雇员。
c) 特定网络安全角色，包括：
   1) 安全主管。
   2) 网络安全内审员。
   3) 安全操作人员。
d) 网络安全等级保护工作相关人员，包括：
   1) 网络安全等级保护工作管理人员。
   2) 网络安全等级保护工作实施人员。
   3) 网络安全等级保护工作测评人员。

7 培训内容要求

金融机构应根据实施网络安全等级保护各岗位的要求，实施相应的培训，包括：

a) 针对全员培训，培训内容包括：
   1) 网络安全意识教育。
   2) 网络安全等级保护政策文件。
   3) 网络安全法律法规、标准。
b) 针对审计委员会，开展网络安全审计知识培训。
c) 针对安全主管开展培训，培训内容包括：
   1) 网络安全规划能力。
   2) 网络安全架构知识。
   3) 网络安全风险知识。
   4) 专业网络安全技术。
d) 针对网络安全审计员开展培训，培训内容包括：
   1) 网络安全、审计的基础知识培训。
   2) 相关网络安全法律法规。
   3) 各项网络安全策略要求。
e) 针对安全操作人员开展培训，培训内容包括：
   1) 所在业务部门的硬件、软件和所需的安全规程。
   2) 安全架构和方案的实施。
   3) 实施和维护安全实践和规程。
f) 针对网络安全等级保护人员开展培训，培训内容包括：技术标准和规范，以及等级保护测评的方法、流程和工作规范。

8 培训实施

金融机构应按照制定的年度培训计划，合理安排培训工作，积极组织员工参加各种形式的培训。

金融机构培训组织部门应提前发放培训通知，聘请讲师，设计课程，准备教材，安排培训场地。

金融机构培训组织部门或参加培训人员应在培训结束后认真填写培训记录表，并交人力资源部存档。

金融机构年度培训计划中没有安排，经评估属于工作急需的培训，由网络安全部门提出培训申请，经人力资源部批准后实施。

9 培训考核

9.1 培训考核依据和要求

金融机构网络安全部门应提出培训考核要求，对各类培训作出相应的考核或评定。

对正式培训，一般以培训方出具的培训证书为考核依据。如没有培训证书，宜提交个人培训心得。

对非正式培训，一般不作直接考核，培训效果评价在人员绩效考核时一并进行。

9.2 培训考核实施

金融机构网络安全部门负责实施培训考核。

9.3 培训考核结果

培训考核合格与否，应作为金融机构岗位技能评审和绩效考核的重要内容。

9.4 培训考核不合格处理

对岗位培训的考核不合格者，具体分成下列两类情形分别处理：

a) 非网络安全等级保护直接工作岗位培训，不合格者将接受再次培训，直至合格为止。

b) 网络安全等级保护工作的定岗培训（一旦该人员培训考核合格，即担任目标工作岗位），不合格者将接受再次培训；两次考核不合格者，将对其作出放弃担任目标工作岗位的处理。

10 培训档案管理

金融机构培训组织部门应对各类等级保护培训档案进行管理，培训档案内容包括：

a) 培训计划。

b) 培训人员名单。

c) 考核标准及考核成绩记录。

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