ICS 03.060
A 11

JR

中华人民共和国金融行业标准

JR/T 0071.5—2020

金融行业网络安全等级保护实施指引 第5部分：审计要求

Implementation guidelines for classified protection of cybersecurity of financial industry—Part 5：Audit requirements

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5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、侯漫丽、潘丽扬、邓昊、赵方萌、乔媛、孙国栋、刘文娟、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5部分：审计要求

1 范围

本部分规定了金融机构网络安全等级保护工作实施审计的要求。

本部分适用于指导金融机构、测评机构和金融行业网络安全等级保护主管部门实施网络安全等级保护审计工作。

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 25058 信息安全技术 网络安全等级保护实施指南

3 审计目标

通过网络安全等级保护审计，获取金融机构开展网络安全等级保护工作的相关证据，并对其进行客观的评价，以确定各金融机构在定级、备案、建设整改、测评自查、安全检查等各项网络安全等级保护工作中是否遵循了网络安全等级保护的要求。

4 审计人员要求

4.1 审计原则

审计人员在审计过程中应遵循以下原则：

a) 道德行为：审计人员应诚信、正直并保守受审计机构的秘密。
b) 公正表达：审计人员应真实、准确地报告审计结果。
c) 职业能力：审计人员应具备必要的审计能力。
d) 独立性：审计人员应不带偏见，与受审计机构没有利益上的冲突，在审计过程中保持客观的心态，以保证审计发现和结论仅建立在审计证据的基础上。
e) 基于证据：审计证据应建立在可获得的信息样本的基础上。

4.2 能力要求

实施金融行业等级保护审计的审计人员应具备如下能力：

a) 熟悉网络安全等级保护相关政策、法规。
b) 正确理解网络安全等级保护标准体系和主要标准内容。
c) 熟悉等级保护工作的全过程，包括定级、备案、建设整改、测评自查、安全检查各个工作环节的要求。

d) 掌握网络安全基础知识，熟悉审计的方法和流程。
e) 具有综合分析和判断的能力，能够整体把握审计结论的客观性和准确性。具备较强的文字表达能力。

4.3 人员培训

实施金融行业网络安全等级保护审计的审计人员应参加金融行业网络安全等级保护主管部门组织的相关标准培训，掌握金融行业网络安全等级保护工作开展的各项要求。

4.4 人员记录

审计人员应提交其教育、工作经历、培训和审计经历的最新记录，作为审计机构安排审计工作时选择审计人员的依据。

5 审计信息管理要求

5.1 机密性要求

审计机构对在审计过程中获得的有关金融机构商业、技术以及审计过程等方面的信息负有保密责任，审计人员应对审计时获得或产生的所有信息按照审计机构的要求识别是否需要实施保密。审计人员及相关人员不应以任何形式和借口传播、扩散、泄露涉密信息。

当法律要求将涉密信息提供给第三方时，除非另有规定，否则审计机构应事先将法律要求提供的信息通知金融机构。当需要向其他机构（如公安部门、保密部门）提供保密信息时，审计机构应将此行动告知金融机构。

审计机构应对审计活动的信息实施密级管理，根据需要配置和使用相应的安全处理设备和设施。安全处理设备和设施主要用于涉密信息的建立、保管、储存、复制以及最终处置。

5.2 完整性要求

包含金融机构信息的介质（例如纸质文件或光盘）在物理运送时，应使用可靠的传输途径防止未授权的访问、信息篡改、不当使用或毁坏。必要时应采取专门的控制，以保护关键信息免遭未授权泄露或篡改，例如手工交付、使用防篡改包装等。

应对包含在电子消息发送中的信息给予适当的保护，防止信息遭受未授权访问、篡改，例如通过加密、哈希或电子签名的方式实施保护。

6 审计过程要求

6.1 总则

6.1.1 总体要求

审计机构应为每次审计编制审计计划，作为与金融机构就审计活动的日程安排和实施达成一致的依据。审计机构应提前与金融机构就审计计划进行沟通，并商定审计日期。

审计机构应正式组建审计组，明确审计组的任务，并告知金融机构。审计机构应要求审计组：

a) 检查和验证金融机构与网络安全等级保护工作相关的定级、备案、建设整改、测评自查、安全检查相关的文件和记录。
b) 确定上述方面满足金融行业等级保护文件和标准的所有要求。

c） 确定金融机构有效地建立、实施并持续开展了网络安全等级保护工作的各项活动。

d） 告知金融机构其与要求之间的任何不一致，以使其采取整改措施。

审计机构应为每次审计提供书面报告。审计组可以提供改进建议，但不应提出具体解决办法的建议。

对于审计中发现的不符合情况，审计机构应要求金融机构在规定期限内分析原因，并说明为消除不符合情况已采取或拟采取的具体纠正措施。

审计机构应审查金融机构提交的纠正措施，以确定其是否可被接受。

6.1.2 审计组

审计机构应正式组建审计组并为其提供相应的工作文件。审计机构应明确界定审计组的任务且使金融机构知晓。任务应包括检查金融机构的定级、备案、建设整改、测评自查和安全检查等活动，确认其满足相关要求。

6.1.3 审计范围

审计组应针对所有适用的审计要求，对包含在限定范围内的金融机构的网络安全等级保护工作进行审计。审计机构应确保根据金融机构等级保护对象的整体结构，清晰的确定等级保护对象的相关设备和组件。

6.1.4 审计报告

审计机构应在离开金融机构场所前与审计组和金融机构管理者召开一次会议，以书面或口头方式，向金融机构说明审计过程中的符合性审计发现、金融机构在网络安全等级保护过程工作中的不足以及整改要求。

审计机构应要求审计组提供审计报告，该报告包括金融机构与所有网络安全等级保护工作要求的符合性方面的审计发现。

6.2 审计准备

审计机构应组建审计组、分配审计任务，由审计组长编制审计计划，审计组成员应根据工作分配情况编制适用的检查表。

审计机构应要求金融机构为审计的实施做出必要的准备，这些准备包括：提供接受检查的文件，以及访问区域、记录和人员。

在现场审计之前，金融机构应至少提供以下信息：

a） 等级保护对象的总体描述文件。

b） 等级保护对象定级、备案、建设整改、测评自查、安全检查等工作证明文件。

6.3 现场审计

6.3.1 获取审计证据

审计组在审计过程中，应针对审计内容，收集与审计准则有关的信息，包括定级、备案、建设整改、测评自查、安全检查等活动相关的过程信息和结果信息。在金融机构等级保护对象数量多、范围广、场所分散的情况下，应通过适当的抽样方式进行收集并验证。只有可证实的信息可作为审计证据并予以记录。

6.3.2 形成审计发现

审计人员应对照审计准则评价审计证据以形成审计发现，审计发现能表明符合或不符合审计准则。

审计人员应汇总审计发现与审计准则的符合情况，指明审计的场所、职能或过程。

审计人员应记录审计发现，应记录不符合的审计发现及其支持的审计证据，可以对不符合的审计发现进行分级。如果审计计划有规定，还应记录符合的审计发现及其支持的审计证据。

审计组应根据需要共同评审审计发现。对不符合的审计发现，审计组应与受审计金融机构一起评审并确认审计证据的准确性，使受审计金融机构理解不符合的审计发现。审计组应努力解决对审计证据和（或）审计发现有分歧的问题，并记录尚未解决的问题。

6.3.3 准备审计结论

在审计组和金融机构管理者召开会议之前，审计组应讨论以下内容，并准备审计结论：

a) 评审审计发现以及在审计过程中所收集的其他信息。

b) 考虑审计过程中固有的不确定因素，对审计结论达成一致。

c) 讨论审计后续活动。

审计结论应针对金融机构网络安全等级保护工作是否符合标准或文件要求形成确定的结果，并对不符合情况作出清楚说明，审计结论还应指出采取纠正、预防或改进措施的要求。

6.4 编制审计报告

在现场审计结束后，审计组长应编制审计报告，提供完整、准确、简明和清晰的审计记录，并包括或引用以下内容：

a) 审计准则。

b) 审计范围。

c) 审计组长和成员。

d) 现场审计活动实施的日期和地点。

e) 审计覆盖的区域，包括所采用的主要审计路线。

f) 观察结果，包括正面的和负面的，即审计发现。

g) 识别的任何不符合的详细情况，包括客观证据及与这些不符合相关的标准或文件要求。

h) 审计结论。

6.5 审计后续活动

审计结束之后，审计组应要求金融机构针对审计过程中发现的不符合分析问题原因，并采取纠正措施。

审计组应对纠正措施的完成情况及有效性进行验证。

7 审计内容要求

按照GB/T 25058的要求，金融行业网络安全等级保护工作包括以下五项活动，网络安全等级保护审计也主要围绕以下五项活动开展：

a) 定级。

b) 备案。

c) 建设整改。

d) 等级测评和自查。

e) 安全检查等活动。

7.1 定级

审计机构应对各金融机构的定级工作进行审计，重点关注下列内容：

a) 应明确等级保护对象的边界和安全保护等级。
b) 应以书面的形式说明确定等级保护对象为某个安全保护等级的方法和理由。
c) 应组织相关部门和有关安全技术专家对等级保护对象定级结果的合理性和正确性进行论证和审定。
d) 应确保等级保护对象的定级结果经过相关部门的批准。
e) 当等级保护对象所承载的业务、服务范围、安全需求等发生变化时，是否对该等级保护对象进行重新定级。

7.2 备案

审计机构应对各金融机构的备案工作进行审计，重点关注下列内容：

a) 定级的等级保护对象备案的全面性，尤其是新建等级保护对象的备案情况。
b) 应指定专门的部门或人员负责管理等级保护对象备案的相关材料，并控制这些材料的使用。
c) 应将等级保护对象定级相关材料报主管部门备案。
d) 应将等级保护对象定级及其他要求的备案材料报送相应公安机关备案，查看定级备案表。
e) 应确保备案材料符合实际情况。

7.3 系统建设整改

审计机构应对各金融机构的系统建设整改工作进行审计，重点关注下列内容：

a) 应对等级保护对象的安全建设总体规划，制定安全建设工作计划。
b) 应根据等级保护对象的等级划分情况，统一考虑安全保障体系的总体安全策略、安全技术框架、安全管理策略、总体建设规划、安全性需求分析、安全性详细设计方案，并形成配套文件。
c) 应组织相关部门和有关安全技术专家对总体安全策略、安全技术框架、安全管理策略、总体建设规划、安全性需求分析、详细设计方案等相关配套文件的合理性和正确性进行论证和审定，并且经过批准后，才能正式实施。
d) 应指定或授权专门的部门负责产品的采购，采购产品应符合国家的相关规定，并对采购产品实行登记维护制度。
e) 如自行开发软件，应确保提供软件设计的相关文档和使用指南，并由专人负责保管，确保对程序资源库的修改、更新、发布进行授权和批准。
f) 如外包开发软件，应制定外包管理制度，要求开发单位提供软件源代码，并审查软件中可能存在的后门和隐蔽信道，并要求外包服务商每年至少开展一次网络安全风险评估或安全审计，提交评估或审计报告。
g) 应制定工程实施方面的管理制度，明确说明实施过程的控制方法和人员行为准则，并应指定或授权专门的部门或人员负责工程实施过程的管理。
h) 应制定详细的工程实施方案控制实施过程，并制定相关过程控制文档，并要求工程实施单位能正式地执行安全工程过程。
i) 应指定或授权专门的部门负责测试验收或交付工作，对测试验收报告或交付清单进行审定，并签字确认。

7.4 等级测评和自查

审计机构应对金融机构的等级测评和自查工作进行审计，重点关注下列内容：

a) 应定期开展等级测评工作，查看测评报告是否规范、完整。
b) 应选择公安部认可的等级保护测评机构开展测评工作。

c） 应对等级保护测评中发现问题进行整改，查看整改报告。
d） 应定期开展等级自查工作，查看自查报告。

7.5 安全检查

审计机构应对金融机构的等级保护安全检查工作进行审计，重点关注下列内容：
a） 应按时接受公安机关的检查，形成检查报告。
b） 应根据检查结果进行整改，形成整改报告。
c） 应将整改情况报送公安机关，并经过公安机关的检查。

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
[3] Q/PBC 00001—2014 中国人民银行信息技术审计规范