ICS 03.060
A 11

JR

中华人民共和国金融行业标准

JR/T 0071.6—2020

金融行业网络安全等级保护实施指引 第6部分：审计指引

Implementation guidelines for classified protection of cybersecurity of financial industry—Part 6：Guidelines for audit work

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 审计目标 1
4 审计方案要求 1
5 审计程序 2
6 审计内容 8
参考文献 10

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6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6部分：审计指引

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指引。

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 审计方案要求

4.1 总则

根据受审计金融机构的规模、性质和复杂程度，金融行业网络安全等级保护主管部门应制定一个或多个审计方案，规划受审计金融机构的整体审计工作。

审计方案可包括一次或多次审计，策划和组织审计的类型和数目，以及在规定的时间内为有效和高效地实施审计提供的所有必要活动。

金融行业网络安全等级保护主管部门应对审计方案的管理进行授权。管理审计方案人员应制定、监督、评审及改进审计方案，并确保受审计金融机构提供必要的资源。

4.2 基本要素和主要内容

4.2.1 基本要素

审计方案的制定可基于以下考虑：

a) 法律法规和合同的要求。

b) 网络安全等级保护主管部门的要求。

c) 其他相关方的需求。

d) 金融机构的风险。

4.2.2 主要内容

基于审计金融机构的规模、性质与复杂程度，审计方案的内容包括：

a) 审计的范围、目的和期限。
b) 审计的频次。
c) 审计的内容。
d) 审计活动的数量和地点。
e) 审计活动的重要性、复杂性、相似性。
f) 审计参考的标准、法律法规、合同要求及其他审计准则。
g) 以往的审计结论或以往审计方案的评审结果。
h) 金融机构的变更情况。

4.3 审计方案负责人员和所需资源

4.3.1 审计方案负责人员职责

审计方案负责人员应了解审计原则、审计人员能力和审计技术应用。他们应具有管理技能，了解与受审计活动相关的技术和业务。

负责管理审计方案的人员应：

a) 确定审计方案的目的和内容。
b) 确定审计人员职责和审计程序，确保受审计金融机构提供必要的资源。
c) 确保审计方案的实施。
d) 确保保持审计方案记录。
e) 制定、监督、评审和改进审计方案。

4.3.2 所需资源

识别审计方案所需资源时应考虑：

a) 审计活动的制定、实施、管理和改进所必需的财务资源。
b) 审计技术。
c) 适合具体审计方案目的的审计人员。
d) 审计方案的内容。
e) 审计过程中的路途时间、食宿和其他审计所需要的资源。

4.4 审计方案的实施

审计方案的实施应明确以下方面：

a) 与被审计机构沟通审计方案。
b) 审计及其他与审计方案有关的活动的协调和日程安排。
c) 向审计组提供必需的资源。
d) 确保按审计方案进行审计。
e) 确保审计活动记录的完整性。
f) 确保审计报告的评审和批准，并确保分发给审计相关方。

5 审计程序

5.1 活动流程

审计组应在审计前策划完整的审计活动流程，审计活动流程参见图1。

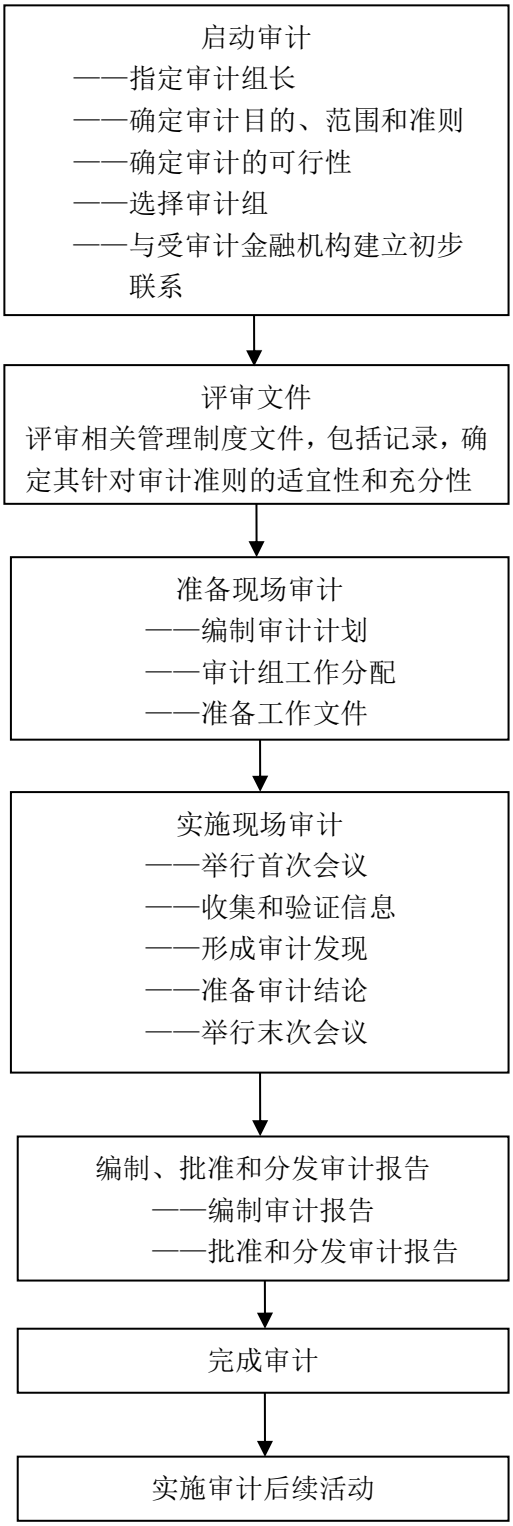

图1 审计活动流程

5.2 启动审计

5.2.1 指定审计组长

负责管理审计方案的人员应为审计活动指定的审计组长。

5.2.2 确定审计目的、范围和准则

审计应基于形成审计文件的目的、范围和准则。

审计目的可包括：

a) 确定受审计金融机构网络安全等级保护体系与审计准则的符合程度。

b) 评价受审计金融机构满足法律法规和合同要求的能力。

c) 评价网络安全等级保护体系实现规定目标的有效性。

d) 识别网络安全等级保护体系潜在的改进方面。

审计范围描述审计的内容和界限，例如：实际位置、受审计的活动和过程等。

审计准则确定审计符合性的依据，包括所适用的方针、程序、标准、法律法规、等级保护要求、合同要求或行业规范等。

5.2.3 确定审计的可行性

审计机构应判断审计的可行性，考虑下列因素的可获得性：

a) 策划审计所需的充分和适当的信息。

b) 受审计金融机构的充分合作。

c) 充分的时间和资源。

当审计不可行时，应在与受审计金融机构协商后向金融行业网络安全等级保护主管部门建议替代方案。

5.2.4 选择审计组

当已明确审计可行时，审计机构应选择审计组，同时考虑实现审计目的。当只有一名审计人员时，审计人员应承担审计组长的职责。

当决定审计组的规模和组成时，应考虑下列因素：

a) 审计目的、范围、准则以及预计的审计时间。

b) 为达到审计目的，审计组所需的整体能力。

c) 法律法规、合同的要求。

d) 确保审计组独立于受审计的活动并避免利益冲突。

e) 审计组成员与受审计金融机构的有效协作能力以及审计组成员之间共同工作的能力。

保证审计组整体能力的过程应包括下列步骤：

a) 识别为达到审计目的所需的知识和技能。

b) 选择审计组成员以使审计组具备所有必要的知识和技能。

c) 若审计组中的审计人员没有完全具备审计所需的知识和技能，可通过技术专家予以满足。

5.2.5 与受审计金融机构建立初步联系

审计机构与受审计金融机构就审计的事宜建立初步联系，可以是正式或非正式的，但应由负责管理审计方案的人员或审计组长进行。初步联系的目的是：

a) 与受审计金融机构的代表建立沟通渠道。
b) 提供建议的时间安排和审计组的信息。
c) 要求获得审计需要的相关文件，包括记录。
d) 确定适用的现场安全规则。
e) 对审计作出安排。

5.3 评审文件

在现场审计前应评审受审计金融机构的网络安全管理相关文件，以确定管理制度所述的内容与审计准则的符合性。评审文件可包括受审计金融机构的网络安全相关管理制度和记录。评审应考虑金融机构的规模、性质以及审计的目的、范围和工作开展的复杂程度，如果不影响审计实施的有效性，文件评审可以推迟至现场活动开始时。

5.4 准备现场审计

5.4.1 编制审计计划

审计组长应编制一份审计计划，使审计组和受审计金融机构之间就审计的实施计划达成一致。

审计计划的详细程度应反映审计的范围和复杂程度。审计计划应有充分的灵活性，应允许更改，例如随着现场审计活动的进展，审计范围的更改是必要的。

审计计划应包括：

a) 审计目的。
b) 审计准则和引用文件。
c) 审计范围，包括确定受审计的金融机构部门、职能单元及过程。
d) 现场审计活动的日期和地点。
e) 现场审计活动预期的时间和期限。
f) 审计组成员的作用和职责。
g) 为审计关键区域配置的资源。

根据具体情况，审计计划还宜包括：

a) 明确受审计金融机构的代表。
b) 后勤安排（交通、现场设施等）。
c) 保密事宜。
d) 审计后续活动。

在现场审计活动开始前，审计计划应经金融行业等级保护主管部门批准，并发至受审计金融机构。

受审计金融机构的任何异议应在审计组长和受审计金融机构之间解决。任何经修改的审计计划应在继续审计前征得各方的同意。

5.4.2 审计组工作分配

审计组长应与审计组协商，将具体的审计职责分配给审计组每位成员。审计组工作的分配应考虑审计人员的独立性和专业性、资源的有效利用。为确保实现审计目的，可随着审计的进展调整所分配的工作。

5.4.3 准备工作文件

审计组成员应收集与其所承担的审计工作有关的信息，并准备必要的工作文件，用于审计过程的参考和记录。这些工作文件可包括：

a) 检查表和审计抽样计划。
b) 记录信息（例如：支持性证据、审计发现和会议记录）的表格。
c) 检查表和表格的使用不应限制审计活动的内容，审计活动的内容可随着审计中收集信息的结果而发生变化。
d) 工作文件，包括其使用后形成的记录，应至少保存到审计结束。审计组成员在任何时候都应妥善保管涉及保密或知识产权信息的工作文件。

5.5 实施现场审计

5.5.1 召开首次会议

审计组应与受审计金融机构管理层（或审计过程的负责人）召开首次会议。首次会议的目的是：

a) 确认审计计划。
b) 简要介绍审计活动如何实施。
c) 确认沟通渠道，指定向导。
d) 向受审机构提供询问的机会。

金融机构应指定向导，以配合审计组的工作。向导可与审计组同行，但不是审计组成员，不应影响或干扰审计的实施。

向导应协助审计组并且根据审计组长的要求行动，职责可包括：

a) 建立联系并安排面谈时间。
b) 安排对办公场所或金融机构特定部分的访问。
c) 确保审计组成员了解和遵守有关场所的安全规则和安全程序。
d) 代表受审计金融机构见证审计过程。
e) 在审计过程中，作出问题澄清或提供帮助。

5.5.2 信息的收集和验证

在审计中，与审计目的、范围和准则有关的信息，包括与职能、活动和过程间接有关的信息，应通过适当的抽样进行收集并验证。只有可证实的信息可作为审计证据并记录。

收集信息的方法包括：

a) 访谈。
b) 对活动的观察。
c) 文件评审等。

审计组应定期讨论以交换信息，评定审计进展情况，需要时重新分派审计组成员的工作。

在审计中，审计组长应定期向受审计金融机构和金融行业网络安全等级保护主管部门通报审计进展及相关情况。在审计中收集的证据显示即将发生或可能存在重大风险时，应立即通知受审计金融机构，并向金融行业网络安全等级保护主管部门报告。对于超出审计范围之外的引起关注的问题，应指出并向审计组长报告，同时向金融行业网络安全等级保护主管部门和受审计金融机构通报。

当获得的审计证据表明不能达到审计目的时，审计组长应向金融行业网络安全等级保护主管部门和受审计金融机构报告理由以确定适当的措施。这些措施可包括重新确认或修改审计计划、改变审计目的、审计范围或终止审计。

随着现场审计的进展，若出现需要改变审计范围的任何情况，应经金融行业网络安全等级保护主管部门和受审计金融机构的评审和批准。

5.5.3 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、职能和过程。

审计人员应记录不符合的审计发现及其支持的审计证据，并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共同评审并确认审计证据的准确性，使受审计金融机构能够理解不符合的审计发现。审计组应解决对审计证据和（或）审计发现有分歧的问题，并记录尚未解决的问题。

5.5.4 准备审计结论

在末次会议召开前，审计组应讨论以下内容：

a) 针对审计目的，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) 如果审计目的有规定，准备建议性意见。
d) 如果审计计划有规定，讨论审计后续活动。

5.5.5 召开末次会议

末次会议应由审计组长主持，并以受审计金融机构能够理解和认同的方式提出审计发现和结论，适当时，双方就受审计金融机构提出的整改计划达成一致。参加末次会议的人员应包括受审计金融机构的代表和其他与审计相关的人员。审计组长应告知受审计金融机构在审计过程中遇到的可能降低审计结论可信程度的情况。

审计组和受审计金融机构应对有关审计发现和审计结论的不同意见进行讨论，并尽可能达成一致。如果未能达成一致，应记录所有的意见。

如果审计目的有规定，审计组应提出改进的建议，并强调该建议没有约束性。

5.6 编制、批准和分发审计报告

5.6.1 审计报告的编制

审计组长应对审计报告的编制和内容负责。

审计报告应提供完整、准确、简明和清晰的审计记录，并包括或引用以下内容：

a) 审计目的。
b) 审计范围，应明确受审计的金融机构部门、职能单元以及审计所覆盖的时期。
c) 明确审计组长和成员。
d) 现场审计活动实施的日期和地点。
e) 审计准则。
f) 审计发现。
g) 审计结论。

根据具体情况，审计报告可包括或引用以下内容：

a) 审计计划。
b) 受审计金融机构代表名单。
c) 审计过程综述，包括遇到的可能降低审计结论可靠性的不确定因素和（或）障碍。
d) 在审计范围内，已按审计计划达到的审计目的。
e) 在审计范围内，但没有覆盖到的区域。
f) 审计组和受审计金融机构之间没有解决的分歧意见。

g) 如果审计目的有规定，提出的改进建议。
h) 商定的审计后续活动计划（如有）。
i) 关于内容保密的声明。
j) 审计报告的分发清单。

5.6.2 审计报告的批准和分发

审计报告应在商定的时间期限内提交。如果不能完成，应向金融行业网络安全等级保护主管部门通报延误的理由，并就新的提交日期达成一致。

审计报告应根据审计方案的规定注明日期，并经评审和批准。

经批准的审计报告应分发给金融行业等级保护主管部门指定的接收者。

审计报告属金融行业网络安全等级保护主管部门所有，审计组成员和审计报告的所有接收者都应尊重并保持审计的保密性。

5.7 完成审计

当审计计划中的所有活动已完成，并分发了经过批准的审计报告时，审计结束。

审计的相关文件应根据参与各方的协议，并按照审计方案程序、适用的法律法规和合同要求予以保存或销毁。

除非法律要求，审计组和负责管理审计方案的人员若没有得到金融行业网络安全等级保护主管部门和受审计金融机构的明确批准，不应向任何其他方泄露文件的内容，审计中获得的其他信息和审计报告。如果需要披露审计文件的内容，应尽快通知金融行业网络安全等级保护主管部门和受审计金融机构。

5.8 实施审计后续活动

审计结论可以指出纠正、预防或改进措施。此类措施通常由受审计金融机构确定并在商定的期限内实施，不视为审计的一部分。受审计金融机构应将这些措施的状态告知金融行业网络安全等级保护主管部门。

应对纠正措施的完成情况及有效性进行验证。验证可以是后续审计活动的一部分。

6 审计内容

6.1 概述

按照GB/T 25058的要求，金融行业网络安全等级保护审计包括定级、备案、系统建设整改、等级测评和自查、安全检查等工作的审计。

6.2 定级

对各金融机构的定级工作进行审计，包括安全保护等级确定、评审、批准及重新定级等内容。

6.3 备案

对各金融机构的备案工作情况进行审计，包括备案材料准备、报送、审批等内容。

6.4 系统建设整改

对各金融机构的系统建设整改工作进行审计，包括系统建设整改方案、产品采购、自行软件开发、外包软件开发、工程实施、系统交付等内容。

6.5 等级测评和自查

对各金融机构的等级测评和自查工作进行审计，包括等级测评周期、测评机构选择、测评报告、问题整改等内容。

6.6 安全检查

对各金融机构的等级保护安全检查工作进行审计，包括检查报告、问题整改等内容。

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