ICS 03.060
A 11

JR

中华人民共和国金融行业标准

JR/T 0071.1—2020

金融行业网络安全等级保护实施指引 第1部分：基础和术语

Implementation guidelines for classified protection of cybersecurity of financial industry—Part 1：Fundamentals and vocabulary

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1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、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1部分：基础和术语

1 范围

本部分规定了金融行业网络安全等级保护工作的基础框架和术语定义。

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

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 17859—1999 计算机信息系统安全保护等级划分准则

GB/T 20269—2006 信息安全技术 信息系统安全管理要求

GB/T 20271—2006 信息安全技术 信息系统安全通用技术要求

GB/T 20272—2019 信息安全技术 操作系统安全技术要求

GB/T 20279—2015 信息安全技术 网络和终端隔离产品安全技术要求

GB/T 20282—2006 信息安全技术 信息系统安全工程管理要求

GB/T 20984—2007 信息安全技术 信息安全风险评估规范

GB/T 20988—2007 信息安全技术 信息系统灾难恢复规范

GB/T 21052—2007 信息安全技术 信息系统物理安全技术要求

GB/T 22239—2019 信息安全技术 网络安全等级保护基本要求

GB/T 22240—2020 信息安全技术 网络安全等级保护定级指南

GB/T 25070—2019 信息安全技术 网络安全等级保护安全设计技术要求

GB/T 28448—2019 信息安全技术 网络安全等级保护测评要求

GB/T 31167—2014 信息安全技术 云计算服务安全指南

JR/T 0071.2—2020 金融行业网络安全等级保护实施指引 第2部分：基本要求

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

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

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

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

JR/T 0072—2020 金融行业网络安全等级保护测评指南

JR/T 0073—2012 金融行业信息安全等级保护测评服务安全指引

3 术语和定义

下列术语和定义适用于本文件。

3.1 特定等级保护类

3.1.1

等级保护对象　target of classified security

网络安全等级保护工作直接作用的对象。

注：主要包括信息系统、通信网络设施和数据资源等。

[GB/T 22240—2020，定义3.2]

3.1.2

等级测评　testing and evaluation for classified cybersecurity protection

测评机构依据国家网络安全等级保护制度规定，按照有关管理规范和技术标准，对非涉及国家秘密的网络安全等级保护状况进行检测评估的活动。

[GB/T 28448—2019，定义3.6]

3.1.3

测评强度　testing and evaluation intensity

测评工作实际投入力量的表征，可以由测评广度和深度来描述。

3.2　通用技术类

3.2.1

信息系统安全　security of information system

信息系统所存储、传输和处理的信息的保密性、完整性和可用性的表征。

3.2.2

安全保证　security assurance

为确保安全要素的安全功能达到要求的安全性目标所采取的方法和措施。

3.2.3

用户鉴别　user authentication

用特定信息对用户身份的真实性进行确认。用于鉴别的信息一般是非公开的、难以仿造的。

[GB/T 20271—2006，定义3.1.12]

3.2.4

客体　object

信息的载体。

[GB 17859—1999，定义3.3]

3.2.5

主体　subject

引起信息在客体之间流动的人、进程或设备等。

[GB 17859—1999，定义3.4]

3.2.6

敏感标记 sensitivity label

表示客体安全级别并描述客体数据敏感性的一组信息，可信计算基中把敏感标记作为强制访问控制决策的依据。

[GB 17859—1999，定义3.5]

3.2.7

主、客体标记 label of subject and object

为主、客体指定敏感标记。这些敏感标记是等级分类和非等级类别的组合，是实施强制访问控制的依据。

[GB/T 20271—2006，定义3.1.14]

3.2.8

访问控制 access control

按确定的规则，对实体之间的访问活动进行控制的安全机制，能防止对资源的未授权使用。

[GB/T 20269—2006，定义3.3]

3.2.9

安全属性 security attribute

实施安全策略时，与主体、客体相关的信息。

注1：对于自主访问控制，安全属性包括确定主、客体访问关系的相关信息。

注2：对于采用多级安全策略模型的强制访问控制，安全属性包括主、客体的标识信息和安全标记信息。

3.2.10

自主访问控制 discretionary access control

由客体的所有者主体自主地规定其所拥有客体的访问权限的方法。有访问权限的主体能按授权方式对指定客体实施访问，并能根据授权，对访问权限进行转移。

[GB/T 20271—2006，定义3.1.16]

3.2.11

强制访问控制 mandatory access control

由系统根据主、客体所包含的敏感标记，按照确定的规则，决定主体对客体访问权限的方法。有访问权限的主体能按授权方式对指定客体实施访问。敏感标记由系统安全员或系统自动地按照确定的规则进行设置和维护。

[GB/T 20271—2006，定义3.1.17]

3.2.12

弱口令 weak password

过于简单或非常容易被破解的口令或密码。

3.2.13

可信路径 trusted path

为实现用户与SSF之间的可信通信，在SSF与用户之间建立和维护的保护通信数据免遭修改和泄漏的通信路径。

[GB/T 20271—2006，定义3.1.20]

3.2.14

公开用户数据 published user data

信息系统中需要向所有用户公开的数据。该类数据需要进行完整性保护。

[GB/T 20271—2006，定义3.1.21]

3.2.15

内部用户数据 internal user data

信息系统中具有一般使用价值或保密程度，需要进行一定保护的用户数据。该类数据的泄漏或破坏，会带来一定的损失。

[GB/T 20271—2006，定义3.1.22]

3.2.16

重要用户数据 important user data

信息系统中具有重要使用价值或保密程度，需要进行重点保护的用户数据，该类数据的泄露或破坏，会带来较大的损失。

[GB/T 20271—2006，定义3.1.23]

3.2.17

关键用户数据 key user data

信息系统中具有很高使用价值或保密程度，需要进行特别保护的用户数据，该类数据的泄漏或破坏，会带来重大损失。

[GB/T 20271—2006，定义3.1.24]

3.2.18

核心用户数据 nuclear user data

信息系统中具有最高使用价值或保密程度，需要进行绝对保护的用户数据，该类数据的泄漏或破坏，会带来灾难性损失。

[GB/T 20271—2006，定义3.1.25]

3.2.19

设备物理安全 facility physical security

为保证信息系统的安全可靠运行，降低或阻止人为或自然因素对硬件设备安全可靠运行带来的安全风险，对硬件设备及部件所采取的适当安全措施。

[GB/T 21052—2007，定义3.3]

3.2.20

环境物理安全 environment physical security

为保证信息系统的安全可靠运行所提供的安全运行环境，使信息系统得到物理上的严密保护，从而降低或避免各种安全风险。

[GB/T 21052—2007，定义3.4]

3.2.21

系统物理安全 system physical security

为保证信息系统的安全可靠运行，降低或阻止人为或自然因素从物理层面对信息系统保密性、完整性、可用性带来的安全威胁，从系统的角度采取的适当安全措施。

[GB/T 21052—2007，定义3.5]

3.2.22

容错 tolerance

通过一系列内部处理措施，将软、硬件所出现的错误消除掉，确保出错情况下信息系统安全子系统所提供的安全功能的有效性和可用性。

[GB/T 20271—2006，定义3.1.26]

3.2.23

云计算 cloud computing

通过网络访问可扩展的、灵活的物理或虚拟共享资源池，并按需自助获取和管理资源的模式。

注：资源实例包括服务器、操作系统、网络、软件、应用和存储设备等。

[GB/T 31167—2014，定义3.1]

3.2.24

灾难备份 backup for disaster recovery

为了灾难恢复而对数据、数据处理系统、网络系统、基础设施、专业技术支持能力和运行管理能力进行备份的过程。

[GB/T 20988—2007，定义3.2]

3.2.25

灾难备份中心 backup center for disaster recovery

用于灾难发生后接替主系统进行数据处理和支持关键业务功能运作的场所，可提供灾难备份系统、备用的基础设施和专业技术支持及运行维护管理能力，此场所内或周边可提供备用的生活设施。

[GB/T 20988—2007，定义3.1]

3.2.26

业务影响分析 business impact analysis；BIA

分析业务功能及其相关信息系统资源、评估特定灾难对各种业务功能的影响的过程。

[GB/T 20988—2007，定义3.5]

3.2.27

灾难恢复预案 disaster recovery plan

定义信息系统灾难恢复过程中所需的任务、行动、数据和资源的文件。用于指导相关人员在预定的灾难恢复目标内恢复信息系统支持的关键业务功能。

[GB/T 20988—2007，定义3.10]

3.2.28

灾难恢复能力 disaster recovery capability

在灾难发生后利用灾难恢复资源和灾难恢复预案及时恢复和继续运作的能力。

[GB/T 20988—2007，定义3.12]

3.2.29

演练 exercise

为训练人员和提高灾难恢复能力而根据灾难恢复预案进行活动的过程。包括桌面演练、模拟演练、重点演练和完整演练等。

[GB/T 20988—2007，定义3.13]

3.2.30

恢复时间目标 recovery time objective；RTO

灾难发生后，信息系统或业务功能从停顿到必须恢复的时间要求。

[GB/T 20988—2007，定义3.18]

3.2.31

恢复点目标 recovery point objective；RPO

灾难发生后，系统和数据必须恢复到的时间点要求。

[GB/T 20988—2007，定义3.19]

3.2.32

审计 audit

为获得审计证据并对其进行客观的评价，以确定满足审计准则的程度所进行的系统的、独立的并形成文件的过程。

3.2.33

审计准则 audit criteria

审计人员进行审计工作时必须遵循的行为规范，是审计人员执行审计业务、获取审计证据、形成审计结论、出具审计报告的标准。

3.2.34

审计证据 audit evidence

审计人员表示审计意见和作出审计结论所必须具备的依据。

3.2.35

审计发现 audit finding

将收集到的审计证据对照审计准则进行评价的结果。

3.2.36

审计结论 audit conclusion

审计组综合审计目的和所有审计发现后得出的审计结果。

3.2.37

审计人员 auditor
有能力实施审计的人员。

3.2.38

审计组 audit team
实施审计的一名或多名审计人员，需要时，由技术专家提供支持。

3.2.39

技术专家 technical expert
向审计组提供特定知识或技术的人员。

3.2.40

审计计划 audit plan
内部审计机构和人员为完成审计业务，达到预期的审计目的，对一段时期的审计工作任务或具体审计项目作出的事先规划。

3.2.41

审计范围 audit scope
审计的内容和界限。

3.2.42

审计机构 audit part
实施审计的部门或单位。

3.3 安全管理类

3.3.1

安全审计 security audit
按确定规则的要求，对与安全相关的事件进行审计，以日志方式记录必要信息，并作出相应处理的安全机制。
[GB/T 20269—2006，定义3.4]

3.3.2

鉴别信息 authentication information
用以确认身份真实性的信息。
[GB/T 20269—2006，定义3.5]

3.3.3

敏感性 sensitivity
表征资源价值或重要性的特性，也可能包含这一资源的脆弱性。
[GB/T 20269—2006，定义3.6]

3.3.4

安全策略 security policy

主要指为信息系统安全管理制定的行动方针、路线、工作方式、指导原则或程序。

[GB/T 20269—2006，定义3.8]

3.3.5

资产价值 asset value

资产的重要程度或敏感程度的表征。资产价值是资产的属性，也是进行资产识别的主要内容。

[GB/T 20984—2007，定义3.2]

3.3.6

业务战略 business strategy

组织为实现其发展目标而制定的一组规则或要求。

[GB/T 20984—2007，定义3.4]

3.3.7

机密性 confidentiality

数据所具有的特性,即表示数据所达到的未提供或未泄露给非授权的个人、过程或其他实体的程度。

[GB/T 20984—2007，定义 3.5]

3.3.8

完整性 integrity

保证信息及信息系统不会被非授权更改或破坏的特性。包括数据完整性和系统完整性。

[GB/T 20984—2007，定义 3.10]

3.3.9

可用性 availability

数据或资源的特性，被授权实体按要求能访问和使用数据或资源。

[GB/T 20984—2007，定义 3.3]

3.3.10

威胁 threat

可能导致对系统或组织危害的不希望事故潜在起因。

[GB/T 20984—2007，定义3.17]

3.3.11

脆弱性 vulnerability

可能被威胁所利用的资产或若干资产的薄弱环节。

[GB/T 20984—2007，定义3.18]

3.3.12

风险 risk

某种威胁存在利用一种资产或若干资产的脆弱性使这些资产损失或破坏的可能性。

[GB/T 20282—2006，定义3.5]

3.3.13

信息安全风险 information security risk

人为或自然的威胁利用信息系统及其管理体系中存在的脆弱性导致安全事件的发生及其对组织造成的影响。

[GB/T 20984—2007，定义3.6]

3.3.14

风险评估 risk assessment

通过对信息系统的资产价值/重要性、信息系统所受到的威胁以及信息系统的脆弱性进行综合分析，对信息系统及其处理、传输和存储的信息的保密性、完整性和可用性等进行科学识别和评价，确定信息系统安全风险的过程。

[GB/T 20269—2006，定义3.7]

3.3.15

残余风险 residual risk

采取了安全措施后，信息系统仍然可能存在的风险。

[GB/T 20984—2007，定义3.12]

3.3.16

检查评估 inspection assessment

由被评估组织的上级主管机关或业务主管机关发起的，依据国家有关法规与标准，对信息系统及其管理进行的具有强制性的检查活动。

[GB/T 20984—2007，定义3.9]

3.3.17

组织 organization

由作用不同的个体为实施共同的业务目标而建立的结构。一个单位是一个组织，某个业务部门也可以是一个组织。

[GB/T 20984—2007，定义3.11]

3.3.18

自评估 self-assessment

由组织自身发起，依据国家有关法规与标准，对信息系统及其管理进行的风险评估活动。

[GB/T 20984—2007，定义3.13]

3.3.19

安全事件 security incident

指系统、服务或网络的一种可识别状态的发生，其可能是对信息安全策略的违反或防护措施的失效，或未预知的不安全状况。

注：改写GB/T 20984—2007，定义3.14。

3.3.20

安全措施 security measure

保护资产、抵御威胁、减少脆弱性、降低安全事件的影响，以及打击信息犯罪而实施的各种实践、规程和机制。

[GB/T 20984—2007，定义3.15]

3.3.21

安全需求 security requirement

使设备、信息、应用及设施符合安全策略的要求而需要采取的保护类型及保护等级。

3.3.22

业务连续管理 business continuity management；BCM

为保护组织的利益、声誉、品牌和价值创造活动，找出对组织有潜在影响的威胁，提供建设组织有效反应恢复能力的框架的整体管理过程。包括组织在面临灾难时对恢复或连续性的管理，以及为保证业务连续计划或灾难恢复预案的有效性的培训、演练和检查的全部过程。

[GB/T 20988—2007，定义3.4]

4 金融行业网络安全等级保护基础

4.1 金融行业网络安全等级保护

根据网络安全等级保护对象在国家安全、经济建设、社会生活中的重要程度，遭到破坏后对国家安全、社会秩序、公共利益以及公民、法人和其他组织的合法权益的危害程度，将等级保护对象划分为不同的安全保护等级并对其实施不同的保护和监管。

4.2 金融行业网络安全等级保护工作的主要内容

根据国家网络安全等级保护管理办法要求，在金融行业开展网络安全等级保护工作，主要内容应该包括：

a) 金融行业系统分等级进行安全保护和监管。具体包括定级、备案、安全建设整改、测评、监督检查。
b) 金融行业网络安全产品分等级使用管理。
c) 金融行业网络安全事件分等级响应、处置等。

4.3 金融行业网络安全等级保护实施基本原则

根据相关政策要求，网络安全等级保护坚持“谁主管、谁负责，谁经营、谁负责，谁建设、谁负责，谁使用、谁负责”的基本原则。

金融行业网络安全等级保护对象的建设和使用单位应依照网络安全等级保护管理规定和技术标准，根据其单位在国民经济和社会发展中的地位作用、系统依赖程度和重要程度、信息内容或数据的重要程度、系统遭到攻击破坏后造成的危害程度等因素，科学、准确地设定其安全保护等级，开展网络安全等级保护工作和制度建设，落实安全管理措施和相关责任。金融领域和金融重点等级保护对象的上级主管部门要对所属对象的安全负起领导和管理责任，提高自主管理、自我保护能力。

4.4 金融行业网络安全等级保护监管要求

根据国家网络安全等级保护管理办法要求，网络安全等级保护实行“国家主导、重点单位强制、一般单位自愿，高保护级别强制、低保护级别自愿”的监管原则。

金融行业的重要等级保护对象应按照国家有关法规和技术标准建设安全保护设施和进行安全保护，并由金融行业主管部门予以核准，依法对其进行监督和检查。

金融行业的一般等级保护对象应按照国家有关法规和技术标准，由金融行业组织机构自行设定安全等级，建设安全保护设施和进行安全保护，报国家主管部门备案，实施自我保护和共同保护。

4.5 金融行业网络安全等级保护工作中相关部门的责任和义务

金融行业网络安全等级保护相关部门职责如下：

a) 国家网络安全职能部门职责分工：
   1) 公安机关：监督、检查、指导等级保护工作。
   2) 国家保密部门：负责等级保护工作中有关保密工作的监督、检查、指导。并负责涉及国家秘密系统的分级保护。
   3) 国家密码管理部门：负责等级保护工作中有关密码工作的监督、检查、指导。
   4) 工业和信息化部门：负责等级保护工作中部门间的协调。
b) 金融行业主管部门，其主要职责为督促、检查、指导本行业、本部门开展等级保护工作。
c) 运营使用单位，主要包括银行、非银行金融机构等运营机构，其主要职责包括：开展定级、备案、建设整改、等级测评、自查等工作，落实等级保护制度的各项要求。具体包括：等级保护对象运营、使用单位按照等级保护的管理规范和技术标准，确定其等级保护对象的安全保护等级；对新建、改建、扩建的等级保护对象进行安全规划设计、安全建设施工；按照与其安全保护等级相对应的管理规范和技术标准的要求，定期进行安全状况检测评估。
d) 安全服务机构：开展技术支持、服务等工作，并接受监督管理部门的监督管理。

4.6 金融行业网络安全等级保护政策体系

自网络安全等级保护制度确立以来，国家主管部门出台一系列文件，构成网络安全等级保护政策体系，金融机构应按照国家法律、政策文件要求，开展网络安全等级保护工作。

4.7 金融行业等级保护技术标准体系

4.7.1 总体概述

按照国家网络安全等级保护标准体系的要求，网络安全等级保护各个环节应符合如下标准要求：

a) 定级环节应符合 GB 17859—1999、GB/T 22240—2020 的要求。
b) 建设整改环节应符合 GB/T 22239—2019、GB/T 25070—2019 的要求。
c) 等级保护测评环节应符合 GB/T 28448—2019 和 GB/T 28449—2018 的要求。金融行业等级保护测评环节除满足上述要求外，还应符合 JR/T 0072—2020 和 JR/T 0073—2012 的要求。

金融行业网络安全等级保护标准体系参照国家等级保护技术标准体系，突出金融行业特点，其框架为三层架构设计，体系的第一层分类将金融行业网络安全等级保护标准按基础标准、要求标准、指南标准划分；第二层分类集中反映金融行业网络安全等级保护的工作需求子类等，第三层描述各子类对应的具体要求。金融行业网络安全等级保护标准体系分类如下：

a) 基础类标准，本部分为基础类标准，基础类标准是实施金融行业网络安全等级保护的前提，涉及的所有部门和人员必须有一个共同的基础、一致的认识，才能开展等级保护工作，因此首先要制定金融行业网络安全等级保护相关的术语和定义、基本原则方面的规范。

b) 要求类标准：金融行业网络安全等级保护的基本要求见 JR/T 0071.2—2020、金融行业网络安全等级保护审计实施要求见 JR/T 0071.5—2020。其中金融行业网络安全等级保护的基本要求是实施等级保护最关键的内容，也是满足国家和行业相关要求的基本保证。金融行业网络安全等级保护审计实施要求是行业网络安全工作管理的需求。

c) 指南类标准包括测评指南、人员管理指南和审计指南，指南类标准作为金融行业网络安全等级保护实施的具体指导性文件，对于等级保护工作的落地、满足国家和行业的要求，并对实施单位产生积极的影响，提高网络安全的防护能力等方面都有重要的作用：

1) 测评指南：金融行业网络安全等级保护的测评指南见 JR/T 0072—2020，金融行业网络安全等级保护的测评服务安全指引见 JR/T 0073—2012。

2) 人员管理指南:金融行业网络安全人员的岗位能力要求和评价指引见 JR/T 0071.3—2020，金融行业网络安全等级保护的培训指引见 JR/T 0071.4—2020。

3) 审计指南：金融行业网络安全等级保护的审计指引见 JR/T 0071.6—2020。

4.7.2 基础类标准

本部分为基础类标准，规定金融行业网络安全等级保护的基础和术语。金融行业实施网络安全等级保护工作涉及多方，例如实施单位、测评单位、主管单位等。具体实施单位内部也涉及多个部门和多种角色，例如部门涉及信息化部门、人力资源部门、行政部门、业务部门等，角色涉及领导层人员、技术人员、管理人员、普通员工等。

促使所有人员正确理解并有效实施网络安全等级保护的各项工作，必须具备可一致理解该工作的平台，例如金融行业网络安全等级保护的机制、方法、测评体系以及相关的术语等。因此，金融行业网络安全等级保护标准体系中，首先需要制定说明金融行业网络安全等级保护基础内容、基本原则、相关术语和定义的标准。

本部分主要包括两方面的内容：金融行业网络安全等级保护基础、金融行业网络安全等级保护术语和定义。金融行业网络安全等级保护基础主要阐述在金融行业开展网络安全等级保护工作的机制和原则，包括等级保护工作在金融行业实施的重要性、过程、关键要素、组织架构、部门分工、工作职责等，以及金融行业网络安全等级保护标准体系的架构和内容。金融行业网络安全等级保护术语和定义对实施金融行业网络安全等级保护工作所涉及的所有相关术语和定义进行归纳、分类，其他标准或文献有定义且符合金融行业网络安全等级保护工作内容的进行采纳；其他标准或文献没有的，按照实际需求进行描述。

4.7.3 要求类标准

要求类标准包括基本要求和审计要求：

a) 基本要求。

金融行业网络安全等级保护的基本要求见JR/T 0071.2—2020，基本要求规范金融行业网络安全等级保护工作中的安全控制选择、安全控制调整、安全控制实施以及安全运行管理等活动，具体作用如下：

1) 为金融行业等级保护对象建设单位和运营、使用单位规定要求:在等级保护对象的安全保护等级确定后，按照基本要求选择特定等级的安全要求进行建设、运营。

2) 为评估机构提供评估依据:基本要求为金融行业等级保护对象的运营、使用单位和金融行业网络安全等级保护测评机构对等级保护对象的检测评估提供依据。

3) 为金融行业网络安全等级保护主管部门提供审计依据:基本要求为主管部门的审计工作提供依据，用于判断一个特定等级的等级保护对象是否按照金融行业的相关要求进行了基本的保护。

基本要求主要借鉴国家相关标准，结合金融行业等级保护对象的特点和需求进行研究编制。各等级的基本安全要求，由安全物理环境、安全区域边界、安全通信网络、安全计算环境、安全管理中心等五个层面的基本安全技术措施和安全管理制度、安全管理机构、安全管理人员、安全建设管理和安全运维管理等五个方面的基本安全管理措施来实现和保证。

b） 审计要求。

等级保护工作的审计要求见JR/T 0071.5—2020，审计工作独立于目前等级保护工作的实施流程之外，从主管部门的角度，审计各单位在定级、备案、建设整改、测评、检查等各项工作中是否遵循了相关标准和文件的要求，重点在于检查其符合性和有效性。

审计要求主要内容包括：审计目标、审计原则、审计内容、审计机制、审计过程以及审计所使用的方法。

4.7.4 指南类标准

4.7.4.1 测评类指南

测评类指南包含测评指南、测评服务安全指引：

a） 测评指南。

金融行业网络安全等级保护测评要求见JR/T 0072—2020，等级保护对象运营、使用单位在进行定级、备案后，应选择测评机构进行等级测评。测评涉及以下内容：

在建设、整改阶段，等级保护对象运营、使用单位通过等级测评进行现状分析，确定等级保护对象的安全保护现状和存在的安全问题，并在此基础上确定安全整改需求。

在运维阶段，等级保护对象运营、使用单位定期委托测评机构开展等级测评，对等级保护对象的安全等级保护状况进行安全测试，对网络安全管控能力进行考察和评价，从而判定等级保护对象是否达到了金融行业网络安全等级保护的基本要求，是否具备了相应等级的安全保护能力。等级保护测评报告是开展整改加固的重要指导性文件，也是备案的重要附件材料。等级保护测评结论为未达到相应等级的基本安全保护能力的，运营、使用单位应当根据等级测评报告，制定方案并进行整改。

b） 测评服务安全指引。

金融行业测评服务安全指引见JR/T 0073—2012，测评服务安全指引明确等级保护测评服务机构安全、人员安全、过程安全、测评对象安全、工具安全等方面的基本要求。测评服务安全服务指引适用于网络安全职能部门对在金融行业开展网络安全等级保护测评的第三方机构和人员进行监督管理。

4.7.4.2 人员管理类指南

人员管理类指南包括岗位能力要求和评价指引、培训指引：

a） 岗位能力要求和评价指引。

应对人员进行完善管理，降低人为错误、盗窃、诈骗和误用设备的风险，减小等级保护对象遭受人员错误造成损失的概率。对于在等级保护工作中承担任务的岗位和角色，应予以明确的定义，并确定其应达到的网络安全能力要求。在人员满足基本能力要求之后，还应对其开展定期评价，以确保人员能够持续满足该岗位的网络安全能力要求。

金融行业等级保护对象的运营、使用单位可按照JR/T 0071.3—2020的要求进行安全管理组织架构设置、岗位设置、人员管理和能力评价。

b） 培训指引。

金融行业等级保护对象的运营、使用单位的相关人员应受到与其工作职能有关的安全意识教育和网络安全技能培训。金融行业网络安全人员培训指引见JR/T 0071.4—2020，培训指引主要包括两个方面：

1) 岗位能力培训，主要是针对不能满足岗位要求的人员提供岗位所需安全意识和技能的培训。
2) 持续技能改进培训，主要是针对各单位内的网络安全等级保护实施人员，提供持续改进的培训机制，确保这些人员实现技能的不断提高，满足网络安全的快速发展，更好的从事单位内的网络安全等级保护工作。

4.7.4.3 审计类指南

金融行业网络安全等级保护审计（以下简称金融等保审计）指南见 JR/T 0071.6—2020，审计指南主要描述金融等保审计目标、审计程序、审计内容。金融等保审计将涉及到规划、实施、监视和评审、改进等诸多环节，实施金融等保审计的机构可以参照审计指南的要求，制定金融等保审计方案、确定金融等保审计内容、实施金融等保审计活动。