ICS 03.060
A 11

JR

中华人民共和国金融行业标准

JR/T 0073—2012

金融行业信息安全等级保护测评服务安全指引

Testing and evaluation service security guide for classified protection of information security of financial industry

2012-07-06 发布　　2012-07-06 实施

中国人民银行 发布

目　　次

前　言

本标准是“金融行业信息系统等级保护”系列标准中的第三项标准。该系列标准的结构及名称如下：
金融行业信息系统信息安全等级保护实施指引
金融行业信息系统信息安全等级保护测评指南
金融行业信息安全等级保护测评服务安全指引
本标准按照GB/T 1.1-2009给出的规则起草。
本标准由中国人民银行提出。
本标准由全国金融标准化技术委员会归口。
本标准负责起草单位：中国人民银行科技司。
本标准参加起草单位：中国金融电子化公司。
本标准主要起草人：王永红、王小青、张永福、王晓燕、王海涛、杨剑、白智勇、沈力克、徐明
本标准为首次发布。

引　言

金融行业重要的信息系统关系到国计民生，是国家信息安全重点保护对象，因此金融行业是落实和实施信息安全等级保护的重点行业之一。由于金融行业的信息系统多是技术密集、资金密集、大型复杂、网络化的人机系统，所以针对金融行业开展信息系统的信息安全等级保护测评，需要一批对金融行业业务系统有一定了解，并具有较强技术能力的测评机构来进行测评；金融行业定级为三级或四级的信息系统都是关系到国计民生的重要系统，有效规避等级保护测评工作中存在的风险，对保障金融行业重要信息系统的安全稳定运行，以及国计民生的稳定都具有重要意义。因此，对测评机构的约束与规范化，是在金融行业实施等级保护的重要一环。

为此，中国人民银行特制定《金融行业信息安全等级保护测评服务安全指引》（以下简称《安全指引》），以明确金融行业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，指导等级保护测评机构在金融机构开展的信息系统安全等级保护测评工作。

金融行业信息安全等级保护测评服务安全指引

1 范围

本标准总结了金融行业应用系统多年的安全需求和业务特点，并参考国际、国内相关信息安全标准及行业标准，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。

本标准适用于信息安全职能部门对从事金融行业信息系统开展信息安全等级保护测评的第三方机构（以下简称测评机构）和人员及其测评活动的监督管理。

2 规范性引用文件

下列文件对于本文件的应用是比不可少的。凡是注日期的引用文件，仅所注日期的版本适用于本文件。凡是不注日期的文件，其最新版本(包括所有的修改单)适用于本文件。

公通字〔2007〕43号 信息安全等级保护管理办法

3 资质能力要求

3.1 测评机构资质要求

从事金融行业信息系统信息安全等级保护测评的第三方机构其机构资质应具备并符合以下要求：

a) 具有公安部认可的信息安全等级保护测评资质，并在公安部等级保护测评机构推荐目录中；
b) 产权关系明晰，注册资金不低于500万元人民币；
c) 具有中国合格评定国家认可委员会（CNAS）实验室或检查机构认可证书；
d) 具有2年以上信息系统安全测评工作经验，且最近1年内至少从事过1次金融机构的信息系统安全测评工作；
e) 最近5年内在测评工作中无法律纠纷，违规记录，无重大信息安全泄露事件及其他重大安全事件等不良记录；
f) 测评机构人员学历比重应为本科（含）以上学历所占比例不低于60%；
g) 测评机构人员规模应不少于30人，且具有满足等级测评工作的专业技术人员和管理人员不少于20人，测评技术人员不少于15人。

3.2 测评机构管理要求

从事金融行业信息系统信息安全等级保护测评的第三方机构其机构管理应具备并符合以下要求：

a) 测评机构及其测评人员应当严格执行有关国家信息安全等级保护相关标准和金融行业有关规定，提供客观、公平、公正、有效的等级保护测评服务，并承担相应的法律责任；
b) 应具备能够保证其公正性、独立性的质量体系，确保测评活动不受任何可能影响测评结果的商业、财务等方面的压力；
c) 测评机构的岗位配置要至少配置测评技术员、项目经理、技术主管、质量主管、保密安全员和档案管理员，其中项目经理、技术主管、质量主管、保密安全员和档案管理员应独立配置，不能有兼任的情况；
d) 测评机构在对被测评单位开展等级保护测评服务之前需与被测评单位签订保密协议，测评过程中向被测评单位借阅的文档资料应在测评工作结束后全部归还被测评单位，未经被测评单位允许，不得擅自复制、保留。

3.3 测评人员要求

从事金融行业信息系统信息安全等级保护测评的第三方机构其测评人员应具备并符合以下要求：

a) 开展金融行业等级保护测评工作的人员仅限于中华人民共和国境内的中国公民，且无犯罪记录；

b) 开展金融行业等级保护测评工作的人员应由参加公安部举办的信息安全等级保护测评人员培训、考试，并取得公安部信息安全等级保护评估中心颁发的等级测评师证书（等级测评人员分为初级、中级和高级）的人员组成；

c) 开展金融行业等级保护测评工作的人员应具备从事信息系统安全测评相关工作三年以上工作经验，开展等级保护测评工作不少于一年，参与金融行业信息安全测评项目不少于两个；

d) 测评技术人员针对网络、安全方面应至少两人持有相关技术资格证书；

e) 测评项目组人员在对被测评单位开展等级保护测评工作之前需与被测评单位签订保密协议。

3.4 测评工具要求

a) 采用的测评工具必须获得正版授权，并在有效期内，不得使用盗版软件；

b) 采用的测评工具在功能、性能等满足使用要求前提下，应优先采用具有国内自主知识产权的同类产品；

c) 采用的测评工具的生产商应为正规厂商，具有一定的研发和服务能力，能够对产品进行持续更新并提供质量和安全保障；

d) 测评机构所使用的测评工具不会对系统产生破坏或负面影响。

4 测评过程要求

4.1 测评过程机构要求

从事金融行业信息系统信息安全等级保护测评的第三方机构可以从事等级测评活动以及信息系统安全等级保护定级、安全建设整改、信息安全等级保护宣传教育等工作的技术支持。但不得从事下列活动：

a) 泄露知悉的被测评单位及被测评信息系统的国家秘密和工作秘密；

b) 非授权占有、使用等级测评相关资料及数据文件；

c) 分包或转包等级测评项目；

d) 信息安全产品开发、销售和信息系统安全集成；

e) 要求被测机构购买、使用其指定的信息安全产品。

4.2 测评过程人员行为要求

从事金融行业信息系统信息安全等级保护测评活动的测评人员，不得从事下列活动：

a) 影响被测信息系统正常运行，危害被测信息系统安全；

b) 泄露知悉的被测机构及被测信息系统的国家秘密和工作秘密；

c) 测评人员未经授权不得将涉密文档带离现场；

d) 测评人员未经允许不得对被测系统进行任何操作；

e) 故意隐瞒测评过程中发现的安全问题，或者在测评过程中弄虚作假，未如实出具等级测评报告；

f) 未按等级保护相关要求规定格式出具等级测评报告；

g) 非授权占有、使用等级测评相关资料及数据文件；

h) 其他危害国家安全、社会秩序、公共利益以及被测机构利益的活动。测评过程管理要求

4.3 测评过程管理要求

4.3.1 文档管理要求

测评方案、测评记录、测评报告等测评文档的产生都离不开被测机构的关键或敏感信息，对于金融机构而言，这些信息对于其系统运行、业务运作异常重要，保密性要求高。因此，测评文档安全在测评过程中应予以高度关注。所有测评人员应遵照以下保密性要求，对测评文档实施保护，包括但不限于下

列措施：

a) 测评人员应在非联网计算机中编制测评文档，测评文档和相关信息均不得存放于联网计算机中；
b) 用于存放编制测评文档的机器应为专用机器，禁止U口使用，同被测评机构交换文档可通过内部网络传输；
c) 编制好的测评文档只能用于被测机构，禁止将被测机构测评文档用于其它机构或其他用途；
d) 测评完成后的测评文档应保存于测评机构的专用服务器中，并设置访问控制策略，未授权人员禁止访问；
e) 测评文档删除时，应采取安全重写方式进行删除；存放测评文档的存储介质在报废时，必须用专业的数据清除工具将介质上的所有数据进行清除，在旧数据被确认清除不可恢复之后，才能进行报废处置。

4.3.2 测评对象管理要求

测评机构在对实施信息安全等级保护测评服务过程中可能使被测评对象面临安全风险，在测评实施过程中，必须要保证测评对象的安全，主要保证业务信息安全、系统服务安全和物理环境安全。

4.3.2.1 业务信息安全管理要求

为保证被测评对象的业务信息安全，测评机构在测评实施过程中和测评实施结束后，应遵守以下要求：

a) 在测评过程中不得获取与测评活动无关的业务数据，不得在非授权情况下获取任何业务数据；
b) 在测评过程中不得修改与测评活动无关的业务数据，不得在非授权情况下修改任何业务数据；
c) 在测评过程中不得删除与测评活动无关的业务数据，不得在非授权情况下删除任何业务数据；
d) 在测评过程中不得使用照相机、摄像机等相关设备记录业务数据；
e) 被测评系统的拓扑图，网络设备与网络安全设备配置信息等，不得全部或部分用于任何与本次测评活动无关的场合，测评活动结束后，必须归还所有获取的拓扑图、网络设备与网络安全设备配置信息及其复印件，电子版必须使用安全删除工具将其从物理存储介质上彻底删除，确保不可恢复；
f) 所有测评过程中涉及的业务信息、相关配置信息等电子信息在被测评机构保存期间应存储在被测评机构授权使用的设备和存储介质中，并单独加密存储，不得使用与其他项目相同的密钥，不得在非授权的情况下复制数据；纸质文档必须严加保管，限制与本次测评无关的人员访问；
g) 所有测评过程中涉及的业务信息、相关配置信息等尽量不使用网络传输，必须使用网络传输的，在传输过程中必须进行对信息进行加密处理，建议使用国家有关部门认可的非对称密钥算法进行加密，使用对称密钥算法的，密钥必须通过其他途径传输。

4.3.2.2 测评系统安全要求

为保证被测评对象的系统服务安全，测评机构在测评实施过程中和测评实施结束后，应遵守以下要求：

a) 在测评过程中未经授权不得修改和删除被测系统的任何配置信息；
b) 测评机构应在测评前向被测单位提交详细的测评方案，方案中必须写明具体的测评方法及可能造成的所有影响；
c) 在测评过程中如需对被测系统配置进行修改，必须在测评方案中说明，并指出可能产生的影响，提出应对解决措施，并在获得被测评单位授权的情况下由被测评单位相关人员尽量在非业务高峰期实施；
d) 在测评过程中未经授权不得停止被测系统的任何服务；
e) 在测评过程中未经授权不得在被测评系统上使用可能造成大量资源消耗的命令；
f) 在测评过程中未经授权不得在被测评系统上执行任何命令与脚本文件，测评过程中使用的命令

应由被测评方审核通过后方可执行，执行命令前，需确认所输入命令与参数正确；

g) 在对被测系统的网络设备、主机系统、数据库、应用系统等进行检查操作时，必须有被检测方相关管理员在现场陪同时方可进行；

h) 测评过程发现的任何被测系统相关脆弱性信息，不得全部或部分用于任何与本次测评活动无关的场合。

4.3.2.3 物理环境安全管理

为保证被测评对象的物理环境安全，测评机构在测评实施过程中和测评实施结束后，应遵守以下要求：

a) 进出被测评系统相关机房等物理环境，应遵守被测评单位物理环境相关管理规定；

b) 应在指定场所进行相关测评工作，未经授权，不得出入其他无关区域；

c) 未经允许，不得插拔任何被测单位的网线、电源插头等；

d) 未经授权，不得以任何方式接入被测评系统网络；

e) 需要接入被测评网络的设备，需经病毒检查后方可接入，接入被测评网络后，禁止使用无线、3G、拨号等其他方式连接其他网络；

f) 禁止将测评期间获得的被测评单位临时出入证、卡等临时身份证明借给其他人使用，只能由被授权人员本人使用，并严格保管，以防丢失，丢失应及时通知被测评单位相关人员；

g) 测评现场阶段结束后，应及时归还相关出入证、卡等临时身份证明。

4.3.3 工具安全使用要求

测评机构在测评过程中使用测评工具对被测评系统进行测评，可能会对被测评系统造成影响，在使用中应满足以下几个方面的要求：

a) 未经授权，不得使用测评工具对被测系统进行测试；

b) 在使用测评工具对被测系统进行测试前，应编写测试方案，应明确使用的工具、测试的对象、测试方法及策略、测试时间、可能产生的影响、应对解决措施等，并由被测评单位授权后按方案实施；

c) 使用脆弱性扫描工具扫描生产系统，不应使用拒绝服务攻击尝试、溢出攻击尝试、数据修改尝试等扫描策略；

d) 使用扫描工具进行扫描检测时应根据扫描计划在指定的网段地址内进行扫描，严禁全网扫描；

e) 使用脆弱性扫描工具扫描生产系统，应尽量在非业务高峰期进行，在业务高峰期时进行扫描应对并行扫描主机数和线程数进行限制，以避免对业务系统和网络造成过高负载影响业务系统正常提供服务；

f) 在开展扫描工作前需征求被测单位相关人员同意，并通知相关人员做好数据备份等应急准备工作；

g) 使用渗透测试工具进行渗透测试时，必须由被测评单位相关人员陪同进行，在未授权情况下，严禁对被测评单位系统进行渗透测试；

h) 使用密码强度审核工具审核密码强度时，必须由被测评单位相关人员陪同进行，相关验证数据不得在测评方保存，必须使用安全删除方式从测评方电脑或存储设备安全删除；

i) 测评过程中禁止使用U盘传递数据和文档；

j) 使用源代码安全扫描系统对源代码扫描时，不得将源代码拷贝至测评方存储设备，如果确实需要拷贝至测评方存储设备，扫描结束后应进行安全删除；生成的扫描报告应妥善保管，应关闭源代码扫描软件，并检查在测评方扫描设备中是否存在缓存源代码，如果存在应对其进行安全删除。项目结束后应将源代码扫描报告进行安全删除。

4

参考文献

[1] 全国人民代表大会常务委员会 《中华人民共和国标准化法》 （1988 年月中华人民共和国主席令第 11 号）

[2] GB/T 1.1-2000 标准化工作导则 第 1 部分：标准的结构和起草规则

[3] GB/T 10112-1999 术语工作 原则与方法

[4] GB/T 20001.1-2001 标准编写规则 第 1 部分：术语

[5] GB/T 16785-1997 术语工作 概念与术语的协调

[6] GB/T 22239-2008 信息系统安全等级保护基本要求

[7] GB/T 25070-2010 信息系统等级保护安全设计技术要求

[8] GB/T 22240-2008 信息系统安全等级保护定级指南