非金融机构支付服务业务系统检测认证管理规定

(征求意见稿)

第一章 总 则

第一条 为加强非金融机构支付服务业务的信息安全管理与
技术风险防范，保证其系统检测认证的客观性、及时性、全面性
和有效性，依据《非金融机构支付服务管理办法》（中国人民银
行令〔2010〕第 2 号，以下简称《办法》）、《非金融机构支付服
务管理办法实施细则》（中国人民银行〔2010〕公告第 17 号）
制定本规定。

第二条 非金融机构支付服务业务系统检测认证，是指对申
请《支付业务许可证》的非金融机构（以下简称非金融机构）或
《办法》所指的支付机构（以下简称支付机构）进行业务系统技
术标准符合性和安全性检测认证工作。

第三条 非金融机构在申请《支付业务许可证》前 6 个月内
应对其业务系统进行检测认证；支付机构应根据其支付业务发展
和安全管理的要求，至少每两年对其被核准的业务系统进行一次
全面的检测认证。

第四条 本规定所指的检测机构应获得中国合格评定国家认可委员会认可的检测机构证书并取得中国人民银行关于非金融机构支付服务业务系统检测认定资格。

第五条 本规定所指的认证机构应获得中国合格评定国家认可委员会认可的认证机构证书并取得中国人民银行关于非金融机构支付服务业务系统认证认定资格。

第六条 非金融机构或支付机构在检测认证过程中应与检测机构和认证机构建立信息保密工作机制。

第七条 支付机构不得连续两次将业务系统检测委托给同一家检测机构。

第二章 检测

第八条 非金融机构或支付机构在实施业务系统检测前，应作如下准备：

- （一）与检测机构签订书面合同，合同应明确规定保密条款；
- （二）与检测机构就检测的范围、内容、进度等进行沟通，制定详细的检测计划，并签字确认；
- （三）向检测机构提交所申请检测认证的业务系统与生产系统的一致性声明。

第九条 检测应严格遵守中国人民银行制定的技术标准和检测规范，真实反映非金融机构或支付机构业务系统技术标准符合

性和安全性状况，保证非金融机构或支付机构业务系统符合国家信息系统安全等级保护第三级的基本要求。

第十条 业务系统检测应包括但不限于：

（一）功能测试

验证业务系统的功能是否正确实现，测试其业务处理的准确性。

（二）风险监控测试

评估业务系统的风险监控、预警和管理措施，测试其业务系统异常交易、大额交易、非法卡号交易、密码错误交易等风险的监测和防范能力。

（三）性能测试

验证业务系统是否满足业务需求的多用户并发操作，是否满足业务性能需求，评估压力解除后的自恢复能力，测试系统性能极限。

（四）安全性测试

评估业务系统在网络安全、主机安全、应用安全、数据安全、运维安全、电子认证安全、业务连续性等方面的能力及管理措施，评价其业务系统的安全防控和安全管理水平。

（五）文档审核

验证业务系统的用户文档、开发文档、管理文档等是否完整、有效、一致，是否符合相关标准并遵从更新控制和配置管理的要求。

第十一条 检测机构应于检测完成后 10 个工作日内向非金融机构或支付机构提交正式的检测报告（一式四份）。

第十二条 检测报告应包括以下内容：

- （一）支付服务业务系统名称、版本；
- （二）检测的时间、范围；
- （三）检测设备、工具及环境说明；
- （四）检测机构名称、检测人员说明；
- （五）检测内容与检测具体结果描述；
- （六）检测过程中发现的问题及整改情况；
- （七）检测结果及建议；
- （八）申请检测认证的业务系统与生产系统的一致性声明；
- （九）其他需要说明的问题。

第十三条 非金融机构或支付机构在收到检测机构出具的检测报告后，应及时将检测报告及相关材料提交认证机构，并申请认证。

第三章 认证

第十四条 非金融机构或支付机构在实施支付服务业务系统认证前，应与认证机构签订书面合同，合同应明确规定保密条款。

第十五条 认证应秉承客观、公正、科学的原则，按照国家有关认证认可法律法规及中国人民银行关于非金融机构支付服务业务系统的技术标准和认证要求实施。

第十六条 认证机构应及时处理认证申请，并在收到认证申请后的 20 个工作日内向非金融机构或支付机构通告认证结果，对合格机构出具认证证书。

第四章 监督与管理

第十七条 支付机构正式开办支付业务后，有下列情况之一的，应及时进行检测：

- （一）出现重大安全事故；
- （二）业务系统应用架构变更、重要版本变更；
- （三）灾备系统的启用、停用及重大架构变更；
- （四）业务系统、生产数据存储环境及机房场地迁移；
- （五）其他中国人民银行要求的情况。

第十八条 检测认证程序、方法不符合国家检测认证相关规定和中国人民银行相关要求，或检测认证结果严重失真的，中国人民银行及其分支机构可以要求重新进行检测或认证，因此而产生的费用由违反规定的检测机构、认证机构承担。

第十九条 检测机构或认证机构未按照中国人民银行制定的检测认证规范和相关要求进行检测认证活动，或未严格坚持科学、公正的原则进行检测认证工作并造成不良后果的，中国人民银行视其情节轻重给予以下处罚：

- （一）通报批评；
- （二）责令限期改正，整改期间暂停相关检测认证工作；

(三) 整改不力的，取消其从事非金融机构支付服务业务系统检测或认证资格，并报国家认证认可监督管理部门备案。

第五章 附则

第二十条 本规定由中国人民银行负责解释。

第二十一条 本规定自发布之日起施行。