ICS 03.060
A 11
备案号：

JR

中 华 人 民 共 和 国 金 融 行 业 标 准

JR/T 0123.5—2014

非金融机构支付业务设施检测规范 第5部分：数字电视支付

Test specification of non-financial institutions payment service facilities
--Part 5：Digital TV payment

2014－11－24 发布　　2014－11－24 实施

中国人民银行　发布

目　　次

前　言

JR/T 0123-2014《非金融机构支付业务设施检测规范》分为五个部分：

——第1部分：互联网支付；

——第2部分：预付卡发行与受理；

——第3部分：银行卡收单；

——第4部分：固定电话支付；

——第5部分：数字电视支付。

本部分为JR/T 0123-2014《非金融机构支付业务设施检测规范》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、北京中金国盛认证有限公司、中国信息安全认证中心、中国金融电子化公司、上海市信息安全测评认证中心、银行卡检测中心、工业和信息化部计算机与微电子发展研究中心（中国软件评测中心）、中国信息安全测评中心、国家应用软件产品质量监督检验中心（北京软件产品质量检测检验中心）、信息产业信息安全测评中心、中金金融认证中心有限公司、中国电子科技集团公司信息化工程总体研究中心、支付宝（中国）网络技术有限公司、银联商务有限公司、拉卡拉支付有限公司、北京通融通信息技术有限公司、快钱支付清算信息有限公司、上海汇付数据服务有限公司、上海盛付通电子商务有限公司、钱袋网（北京）信息技术有限公司、联通支付有限公司、深圳市财付通科技有限公司等。

本部分主要起草人：潘润红、杜宁、邬向阳、李兴锋、吴晓光、陈实博、王磊磊、聂丽琴、唐立军、田洁、王翠、高天游、赵春华、郝晓花、王妍娟、付小康、陆碧波、李红曼、张奇、扈浩、布宁、吴迪、严妍、刘思蓉、甘杰夫、刘力凤、蒋朝阳、马国照、张瑞秀、刘文光、白智勇、周悦、王威、赵小帆、郑丽娜、孔昊、李宏达、陆嘉琪、金铭彦、刘健、张益、董晶晶、杜磊、李海滨、王睿超、段超、张金凤、熊军、吴祥富、高磊、宋铮、郭宇、孔嘉俊、罗文兵、唐刚、杨天识、漆添虎、潘莹、侯龙、王雅杰、张进、李鹏、牛跃华、王雄、唐凌、林志伟、王华锋、方海峰、张健、戴维、冷杉、程伟、冯建盟、林勇、刘锦祥、叶飞、王庆、罗旭、任震、赵传飞等。

引　言

为促进支付服务市场健康发展，规范非金融机构支付服务行为，防范支付风险，保护当事人的合法权益，根据《中华人民共和国标准化法》、《中华人民共和国认证认可条例》、《非金融机构支付服务管理办法》（中国人民银行令〔2010〕第2号）、《非金融机构支付服务管理办法实施细则》（中国人民银行公告〔2010〕第17号）及《非金融机构支付服务业务系统检测认证管理规定》（中国人民银行公告〔2011〕第14号）等相关法律法规的规定，制定非金融机构支付业务设施检测系列规范。

检测目标是在系统版本确定的基础上，对非金融机构支付业务设施（数字电视支付）功能、风险监控、性能、安全性、文档和外包六项检测类进行测试，客观、公正地评估其是否符合中国人民银行对支付业务设施的技术标准符合性和安全性要求，保障我国支付业务设施的安全稳定运行。

非金融机构支付业务设施检测规范
第5部分：数字电视支付

1 范围

本部分规定了非金融机构支付业务设施(数字电视支付)技术标准符合性和安全性检测方案,包括非金融机构的支付业务处理系统、网络通信系统以及容纳上述系统的专用机房的技术标准符合性和安全性检测方案。

本部分适用于第三方检测机构对非金融机构支付业务设施的检测,及可能涉及到的为非金融机构支付业务设施提供外包的第三方服务机构进行附加的测试。

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。

会计档案管理办法　财会字〔1998〕32号文印发

3 术语和定义

下列术语和定义适用于本文件。

3.1

非金融机构支付服务 non-financial institutions payment services

非金融机构在收付款人之间作为中介机构提供下列部分或全部货币资金转移服务：

a) 互联网支付；
b) 移动电话支付；
c) 固定电话支付；
d) 数字电视支付；
e) 预付卡发行与受理；
f) 银行卡收单；
g) 中国人民银行确定的其他支付服务。

3.2

数字电视支付 digital TV payment

依托交互机顶盒等数字电视支付终端发起的，使用IC卡或网络实现支付交易的行为。

数字电视支付业务不涉及IC卡的发行和管理。

4 启动准则

启动包括以下准则：

a) 非金融机构提交的支付业务处理系统被测版本与生产版本一致；

b) 非金融机构支付业务处理系统内部测试进行完毕；
c) 系统需求说明书、系统设计说明书、用户手册、安装手册等相关文档准备完毕；
d) 检测机构应在检测方案中分析支付业务设施在检测过程中出现的风险，并提出相应的应对措施，见附录 A；
e) 测试环境准备完毕，具体包括：
   1) 测试环境与生产环境一致或者基本一致，其中网络安全性、主机安全性、数据安全性和运维安全性测试尽量在生产环境下进行；
   2) 支付业务处理系统被测版本及其他相关外围系统和设备已完成部署并配置正确；
   3) 用于功能和性能测试的基础数据准备完毕，做好相关敏感数据的保护和屏蔽工作；
   4) 测试用机到位，系统及软件安装完毕；
   5) 测试环境网络配置正确，连接通畅，可以满足测试需求。

5 功能测试

验证支付业务设施的业务功能是否正确实现，测试系统业务处理的准确性，测试内容见表1。

表1 功能测试

编号	检测项		检测说明	类别
1.1.	客户管理	1.1.1 客户信息登记及管理	必测项（卡支付不适用）	技术类
		1.1.2 商业银行管理		技术类
		1.1.3 客户证书管理		技术类
		1.1.4 客户审核	必测项（卡支付不适用）	技术类
1.2.	账户管理	1.2.1 客户支付账户管理	必测项	技术类
		1.2.2 客户支付账户管理审核		技术类
		1.2.3 客户支付账户查询	必测项	技术类
		1.2.4 客户支付账户资金审核		技术类
1.3.	交易处理	1.3.1 消费	必测项	技术类
		1.3.2 消费撤销	必测项	技术类
		1.3.3 转账		技术类
		1.3.4 充值		技术类
		1.3.5 提现		技术类
		1.3.6 交易纠纷处理		技术类
		1.3.7 交易明细查询	必测项	技术类
		1.3.8 委托交易		技术类
		1.3.9 冲正交易	必测项	技术类
		1.3.10 退货		技术类
		1.3.11 销账		技术类
		1.3.12 预授权		技术类
		1.3.13 预授权撤销		技术类
		1.3.14 预授权完成		技术类
		1.3.15 预授权完成撤销		技术类
		1.3.16 IC 卡指定账户圈存		技术类

编号	检测项		检测说明	类别
		1.3.17 IC卡现金充值		技术类
		1.3.18 IC卡脱机交易上传		技术类
		1.3.19 账单费用查询		技术类
1.4.	资金结算	1.4.1 客户结算	必测项	技术类
1.5.	对账处理	1.5.1 客户发送对账请求		技术类
		1.5.2 客户下载对账文件		技术类
1.6.	差错处理	1.6.1 长款/短款处理	必测项	技术类
		1.6.2 单笔退款	必测项	技术类
		1.6.3 批量退款		技术类
1.7.	统计报表	1.7.1 业务类报表	必测项	技术类
		1.7.2 运行管理类报表	必测项	技术类

6 风险监控测试

验证支付业务设施的账户及交易风险，测试内容见表2。

表2 风险监控测试

编号	检测项	检测说明	技术要求细化	检测方法及步骤	预期结果及判定	类别
2.1.1	账户风险管理/实名认证	必测项	1.宜对个人客户进行实名认证； 2.应对商户进行实名认证。	1.检查系统是否对个人客户进行实名认证； 2.检查系统是否对商户进行实名认证。	1.对商户进行了实名认证； 2.未对个人客户实行实名认证，提建议性问题；如仅提供支付网关支付服务，可不在支付平台实名认证。	技术类
2.2.1	交易监控/监控规则管理	必测项	1.应对正常交易确定交易监控规则； 2.应对异常交易进行监控，如：金额、频率、流向、用途、性质等有异常情形的可疑交易确定交易监控规则； 3.应对违反规则的交易，如：超过密码错误上限、超过最大交易次数、单笔交易上限的交易、实时交易超时等情况，制定异常交易的等级，并明确交易	1.检测风险管理制度文档，查看是否对正常交易、可疑交易、违反规则的交易，有明确的划分和相应的监控规则； 2.抽取部分风控规则在系统中进行验证。	风险管理制度文档中有对正常交易、可疑交易、违反规则的交易，有明确的划分和相应的监控规则。	管理类

编号	检测项	检测说明	技术要求细化	检测方法及步骤	预期结果及判定	类别
			监控规则。			
2.2.2	交易监控/当日交易查询	必测项	1.应提供当日交易明细查询； 2.应提供当日每笔交易的交易详情查询； 3.应提供当日交易总笔数、总金额的查询结果统计； 4.宜提供按查询条件查询交易的功能； 5.宜提供按查询条件模糊查询交易的功能。	1.验证系统功能：对某账户当日存在的交易明细信息查询；查询某笔交易的详细信息；对当日交易的总笔数、总金额统计结果正确； 2.验证系统功能： 对某账户当日存在的交易具有按条件、模糊查询的功能。	1.对某账户当日存在的交易明细信息查询、详细信息，查询结果统计正确； 2.其他进一步的查询功能如果存在，则检查功能是否实现正确。	技术类
2.2.3	交易监控/历史交易查询	必测项	1.提供一段时间区间内（如1年/3年）的历史交易明细查询或历史交易详情查询； 2.应提供时间区间内交易总笔数、总金额的查询结果统计； 3.宜提供按查询条件查询交易的功能； 4.宜提供按查询条件模糊查询交易的功能。	1.验证系统功能：对某账户一段时间区间内存在的交易查询交易明细信息；查询某笔交易的详细信息；对当日交易的总笔数、总金额统计结果正确； 2.验证系统功能： 对某账户一段时间区间内存在的交易具有按条件、模糊查询的功能。	1.对某账户当日存在的交易查询交易明细信息、详细信息，查询结果统计正确； 2.其他进一步的查询功能如果存在，则检查功能是否实现正确。	技术类
2.2.4	交易监控/实时交易监控	必测项	1.应对正常交易、可疑交易、违反规则的交易，提供监控规则的设置并进行实时交易监控； 2.应对用户签约（如：与支付相关的签约）、登录、交易、付款、退款以及涉及账户变动的全过程实施监控，实现交易监控规则的设置，以实现对实时交易的监控； 3.应提供对违反规则的交易进行查询、处理、风险控制等服务。	1.验证系统功能：对正常交易、可疑交易、违反规则的交易，提供监控规则的设置并按照设置进行实时交易监控； 2.验证系统功能：对违反规则的交易监控进行查询、处理、风险控制。	1.对正常交易、可疑交易、违反规则的交易，提供监控规则的设置并能正确按照设置进行实时交易监控； 2.对违反规则的交易监控进行查询、处理、风险控制功能正确。	技术类

编号	检测项	检测说明	技术要求细化	检测方法及步骤	预期结果及判定	类别
2.2.5	交易监控/可疑交易处理	必测项	1.应有明确的划分可疑交易（如：中国人民银行规定的可疑支付交易行为）的方式及监控规则； 2.能对检测到可疑交易实现查询、分析处理等服务。	1.查看是否具有对可疑交易有明确的划分及监控规则； 2.验证系统功能，查询检测到可疑交易并对其进行分析处理等服务。	1.具有对可疑交易有明确的划分及监控规则； 2.具有对检测到可疑交易实现查询、分析处理等服务，功能实现正确。	技术类
2.2.6	交易监控/交易事件报警	必测项	1.应对监控到的违反规则的交易进行报警； 2.应对违反规则的交易事件提供查询和统计功能。	1.验证系统功能，对某账户进行异常交易进行报警； 2.验证系统功能，查询违反规则的交易事件，验证统计是否正确。	1.对某账户操作异常交易时，系统能够进行相应的报警处理； 2.可根据规定的相应违反规则正确的查询并统计违反规则的交易事件。	技术类
2.2.7	交易监控/支付限额	必测项	1.风险管理制度中应规定支付限额； 2.系统应实现制度中规定的支付限额功能。	1.检查风险管理制度中是否规定了支付限额； 2.检查系统是否实现了制度中规定的支付限额功能。	1.风险管理制度中规定了支付限额； 2.系统实现了制度中规定的支付限额功能。	
2.2.8	交易监控/单笔交易限额	必测项	超过单笔交易限额的交易应有记录并触发风控规则。	1.检查验证是否可以设置单笔交易限额； 2.验证是否在超过单笔交易限额后能够触发风控规则。	能够设置单笔交易限额，超过限额有记录并触发风控规则。	技术类
2.2.9	交易审核/当日累计交易限额	必测项	超过当日累计交易限额的交易应有记录并触发风控规则。	1.检查验证是否可以设置当日累计交易限额； 2.验证是否在超过当日累计交易限额后能够触发风控规则。	能够设置当日累计交易限额，超过限额有记录并触发风控规则。	技术类
2.3.1	交易审核/系统自动审核	必测项	1.应提供针对交易的审核规则设置功能，并确保系统能正确实现； 2.应提供违反规则的交易监控进行查询、处理、风险控制等服务。	1.验证系统功能：在系统设置界面，根据文档要求对交易审核规定进行正确的设置； 2.验证系统功能：模拟交易能够触发风控规则； 3.验证系统功能：进入交易监控界面，对违反规则的交易进行查询、处理、风险监控等操作。	1.根据文档要求成功设置交易审核规定； 2.根据已设置的交易审核规定来判断该交易是否审核通过； 3.界面成功显示交易的审核结果、处理结果及风险监控记录。	技术类

编号	检测项	检测说明	技术要求细化	检测方法及步骤	预期结果及判定	类别
2.3.2	交易审核/人工审核	必测项	1.具有完整、明确的定义需要人工审核的相关交易的管理制度文档； 2.可以提供人工审核的实现方法； 3.保存人工审核的历史记录。	1.查看相关管理制度并访谈确认是否有完整明确定义的需人工审核的相关交易； 2.验证所提供的人工审核方法是否正确实现； 3.查看是否保存人工审核的历史记录。	1.有完整明确定义的需人工审核的相关交易； 2.所提供的人工审核方法能够正确实现； 3.保存人工审核的历史记录。	管理类
2.4.1	风控规则/风控规则管理	必测项	1.在风险管理制度中，具有各项风控规则的变更、审核和确认制度； 2.按照风险管理制度进行日常操作。	1.检查管理制度文档，查看是否存在各项风控规则的变更、审核和确认制度； 2.公司风险管理方法的文件中明确规定：制定有效的风险防范措施，监测关键风险指标，建立风险预警机制等； 3.查看风控管理规则记录。	1.存在各项风控规则的变更、审核和确认制度； 2.有变更审核的操作记录。	管理类
2.4.2	风控规则/黑名单	必测项	1.系统应实现黑名单管理功能，包括商户和客户； 2.应有明确的黑名单的规则； 3.应实现黑名单新增、审核、查询、删除等功能； 4.应具有黑名单中的客户交易拒绝功能。	1.验证系统功能：在黑名单管理界面，将操作非法交易的客户移至到黑名单中； 2.查看黑名单规则； 3.可以对黑名单记录进行新增、审核、查询、删除等维护功能； 4.被拉入黑名单的客户，检查是否有效实现交易拒绝功能。	1.成功将某客户移至到系统的黑名单中； 2.可以成功查看黑名单规则； 3.可以成功对黑名单记录进行新增、审核、查询、删除等维护功能； 4.被拉入黑名单的客户，无法再进行交易。	技术类
2.4.3	风控规则/风险识别	必测项	在风险管理制度中，具有各种风险类别的完整明确的定义：如何划分、如何定级、如何监控、如何防范、如何处理等。	检查风险控制部门的相关作业文件（如风险识别、风险定义、风险防范等独立文档等），查看文档中是否完整、明确的定义了如何划分、定级、监控、防范及处理各种风险类别。	文档中明确定义了如何划分、定级、监控、防范及处理各种风险类别。	管理类
2.4.4	风控规则/事件管理	必测项	1.应在风险管理制度中，具有各项风险事件完整明	1.检查风险控制部门的相关作业文件（如风险识	1.文档或系统中存在对各种风险事件明确	管理

编号	检测项	检测说明	技术要求细化	检测方法及步骤	预期结果及判定	类别
			确的处理规则； 2.对已发生的风险事件，应保存有事件记录。	别、风险定义、风险防范等独立文档等），查看文档或系统中是否存在对各种风险事件明确的处理规则； 2.验证系统功能：在风险事件查询界面中，对风险事件进行保存。	的处理规则； 2.系统可成功对风险事件进行保存且可查询。	类
2.4.5	风控规则/风险报表	必测项	系统应具有能够提供一定时间区间内的风险事件报表，或系统对风险事件报表提供查询功能。	验证系统功能：在风险事件查询界面，对风险事件进行保存；或在风险事件报表界面，输入正确的时间段后查询。	系统可成功对风险事件进行保存；或界面成功显示查询时间段内的风险事件报表。	技术类

7 性能测试

对支付业务设施的性能测试的主要目的是验证系统是否满足未来三年业务运行的性能需求。

测试内容包括以下三个方面：一是验证系统是否支持业务的多用户并发操作；二是验证在规定的硬件环境条件和给定的业务压力下，考核系统是否满足性能需求和压力解除后系统自恢复能力；三是测试系统性能极限。

根据以上性能测试内容，并结合典型交易、复杂业务流程、频繁的用户操作、大数据量处理等原则，选取测试业务点见表3。

表3 性能测试业务点

编号	检测项	检测说明	类别
3.1	3.1.1 消费	必测项	技术类
3.2	3.2.1. 交易明细查询	必测项	技术类
3.3	3.3.1 充值		技术类
3.4	3.4.1 转账		技术类
3.5	3.5.1 日终批处理		技术类

8 安全性测试

8.1 网络安全性测试

对支付业务设施的网络环境进行检测，考察经网络系统传输的数据安全性以及网络系统所连接的设备安全性，评估系统网络环境是否能够防止信息资产的损坏、丢失，敏感信息的泄漏以及业务中断，是否能够保障业务的持续运营和保护信息资产的安全。检测内容见表4。

表4　网络安全性测试

编号	检测项	检测说明	技术要求细化	检测方法及步骤	预期结果及判定	类别
4.1.1.1	网络安全/结构安全/网络冗余和备份	必测项	1.应明确核心和边界网络设备承载能力； 2.核心网络设备应冗余，并明确备份方式为冷备份还是热备份； 3.应明确网络带宽是否满足高峰时流量。	1.访谈网络管理员，询问主要网络设备的性能以及目前业务高峰流量情况，询问采用何种手段对主要网络设备进行监控； 2.检查网络设计/验收文档，查看是否有核心和边界网络设备能满足基本业务需求，网络接入及核心网络的带宽能满足业务高峰期的需要，以及是否不存在带宽瓶颈等方面的设计或描述； 3.访谈网络管理员，询问核心网络设备是否冗余，采用的冗余备份策略是冷备份还是热备份。	1.网络管理员说明核心网络设备的性能满足业务需求，目前业务高峰流量为aMB，采用网管软件（如Quidview/Prime/OpenView)对网络设备性能和端口流量进行监视； 2.设计文档中写明了主要网络设备采用主流网络设备制造商产品满足业务需求，网络接入及核心网络的带宽为峰值应用1.2倍以上，满足业务高峰期的需要； 3.网络管理员说明核心网络设备均采用热备份的策略。	技术类
4.1.1.2	网络安全/结构安全/网络安全路由	必测项	1.应明确业务终端与业务服务器之间的访问路径； 2.应明确不同访问路径的路由控制措施。	1.访谈网络管理员，确认业务终端与业务服务器之间的访问路径； 2.查看在访问路径上是否采用安全路由技术的网络路由器或相关设备。	1.在内外网之间应该配备必要的路由访问控制设备； 2.查看内外网间路由器是否具备安全访问功能，如采用静态路由、动态路由（采用认证方式）。	技术类
4.1.1.3	网络安全/结构安全/网络安全防火墙	必测项	1.应在网络边界处部署具有网络访问控制功能的设备，如：防火墙或路由器等； 2.相关访问控制策略应有效实现。	1.访谈网络管理员，询问网络安全区域间划分情况； 2.查看网络拓扑，不同等级网络间是否使用网络访问控制设备； 3.登录网络访问控制设备管理界面查看配	1.根据网络承载业务重要程度，对网络进行了安全域划分； 2.网络拓扑显示在网络边界处应该部署了网络访问控制设备； 3.显示网络访问控制设备处于工作状态，已经配置了有效过滤规则。	技术类

编号	检测项	检测说明	技术要求细化	检测方法及步骤	预期结果及判定	类别
				置及状态。		
4.1.1.4	网络安全/结构安全/网络拓扑结构	必测项	网络拓扑记录与实际情况相一致。	采用现场抽查的方式，检查机房内的设备与网络拓扑图的一致性。	机房内的设备与网络拓扑情况一致。	技术类
4.1.1.5	网络安全/结构安全/IP 子网划分	必测项	1.应根据各部门的工作职能、重要性和所涉及信息的重要程度等因素，划分不同的子网或网段； 2.应按照方便管理和控制的原则为各子网、网段分配地址段。	1.访谈安全管理员，收集公司业务部门、工作职能、重要性等情况； 2.查看 IP 子网划分情况，与收集的公司业务情况进行比较。	1.公司应该建立起依据部门职能、重要性来划分安全等级的安全管理制度； 2.子网划分情况应该考虑单位各部门工作职能、重要性和所涉及信息的重要程度等因素，不同安全等级的机构不能划分在同一个子网内，应该进行必要隔离。	技术类
4.1.1.6	网络安全/结构安全/QoS 保证	必测项	宜按照对业务服务的重要次序来指定带宽分配优先级别，保证在网络发生拥堵的时候优先保护重要主机。	1.访谈网络管理员，询问系统业务部署情况； 2.访谈不同业务系统主机优先级别； 3.查看具有QoS功能的网络管理设备的带宽分配情况。	1.根据业务系统功能进行分布部署； 2.在设计规划主机使用前，根据承载业务的优先级别进行等级划分； 3.根据业务需求判断是否需要进行QoS设置来保证在网络发生拥堵的时候优先保护重要主机。	技术类
4.1.2.1	网络安全/网络访问控制/网络域安全隔离和限制	必测项	1.应在网络边界部署安全访问控制设备； 2.应启用网络设备访问控制功能。	1.访谈网络管理员，是否在网络边界部署安全访问控制设备； 2.对安全访问控制设备进行检查。	1.应该在网络边界部署安全访问控制设备（如防火墙，安全网关，负载均衡系统等）； 2.上述安全设备应该已经启用，设备管理界面显示基本安全策略已经启用（如 URL 过滤、访问列表等）。	技术类
4.1.2.2	网络安全/网络访问控制/地址转换和绑定	必测项	应针对重要网段应至少采取一种防护方式防止地址欺骗（如 ARP 静态列表、ARP 防火墙）。	1.访谈网络管理员，询问针对重要网络实施何种地址欺骗预防措施或使用什么设备； 2.查看相关设备的配置策略。	1.重要网络已实现预防地址欺骗设置； 2.配置策略已启用。	技术类
4.1.2.3	网络安全/网络访问控制/内容	必测项	应对进出网络的信息内容进行过滤，实现对应用	1.检查内容过滤设备（如防火墙）的配置信息；	1.该设备支持对应用层信息的过滤功能； 2.在设备设置过滤规则后，用户	技术类

编号	检测项	检测说明	技术要求细化	检测方法及步骤	预期结果及判定	类别
	过滤		层 HTTP、FTP、TELNET、SMTP、POP 等协议命令级的控制。	2.检查是否有对应用层协议的过滤控制（如禁止通过 http 协议访问互联网网站），通过内网终端访问互联网网站。	无法访问指定网络内容。	
4.1.2.4	网络安全/网络访问控制/访问控制	必测项	1.网络设备和系统应该根据用户权限列表，对用户进行访问控制，控制粒度为端口级； 2.用户和系统之间的访问控制规则，决定允许或拒绝用户对受控系统进行资源访问，控制粒度应为单个用户。	1.检查网络设备是否提供会话控制功能，控制粒度是否为端口级； 2.检查用户和系统之间的访问控制规则是否为单个用户。	1.网络设备提供会话控制功能，控制粒度为端口级； 2.用户和系统之间的访问控制规则为单个用户。	技术类
4.1.2.5	网络安全/网络访问控制/流量控制	必测项	1.应限制网络最大流量数； 2.应限制网络连接数。	1.对边界网络设备进行检查，如防火墙或路由器等，查看是否进行流量控制； 2.对边界网络设备进行检查，如防火墙或路由器等，查看是否进行网络连接数限制。	1 防火墙或路由器等网络设备，配置了流量控制策略； 2.防火墙或路由器等网络设备，对网络连接数进行了限制。	技术类
4.1.2.6	网络安全/网络访问控制/会话控制	必测项	1 当会话处于非活跃状态，应具备超时退出机制； 2.会话结束后，应终止网络连接，释放资源。	查询网络设备（交换机、防火墙等）的访问超时设置，使用预置用户访问网络设备登陆后闲置或执行签退操作。	网络设备设置了用户的访问超时参数，用户闲置时间超过规定后，会被自动签退，或主动注销后被成功签退。	技术类
4.1.2.7	网络安全/网络访问控制/远程拨号访问控制和记录	必测项	1.应限制管理用户通过远程拨号对服务器进行远程管理； 2.如必须使用情况，应进行相关	进入操作系统的管理平台，查看主机的远程访问控制规则配置情况，是否允许使用 Modem 拨号设备。	系统应该禁止通过远程拨号方式访问主机（如 modem 拨号方式）。	技术类

编号	检测项	检测说明	技术要求细化	检测方法及步骤	预期结果及判定	类别
			详细记录。			
4.1.3.1	网络安全/网络安全审计/日志信息	必测项	1.应对网络系统中的网络设备运行状况、网络流量、用户行为等进行日志记录； 2.审计记录应包括：事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息。	1.检查网络及主机设备是否具备日志记录功能； 2.检查日志记录是否包含事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息。	设备应该针对各自运行状况、网络流量、用户行为等产生记录，记录信息应该至少包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息。	技术类
4.1.3.2	网络安全/网络安全审计/网络系统故障分析	必测项	应对网络故障进行记录，根据记录结果查找原因形成分析结果。	1.访谈网络管理员，询问近期网络系统产生的故障及处理情况的记录； 2.现场对故障、处理记录（系统）进行检查。	1.对于近期发生的网络故障事件，应该留有故障记录及详细的处理情况； 2.当前系统网络运维至少应提供针对故障及处理情况的汇总记录查询功能，或形成故障处理知识库系统软件。	技术类
4.1.3.3	网络安全/网络安全审计/网络对象操作审计	必测项	1.应能够根据记录数据进行分析，并生成审计报表； 2.审计记录应生成审计报表。	1.检查审计系统保存的审计记录； 2.操作审计系统根据指定要求生成审计记录。	1.审计系统提供的审计范围应该至少包括网络设备信息、网络协议、受攻击情况等； 2.审计功能应该提供报表生成功能，对审计记录按照指定要求筛选分类生成统计记录。	技术类
4.1.3.4	网络安全/网络安全审计/日志权限和保护	必测项	应对审计记录进行保护，避免受到未预期的删除、修改或覆盖等。	1.现场检查审计系统，检查系统的访问控制功能； 2.检查现有审计记录与系统维护记录进行对比； 3.使用低权限的用户登录审计系统，执行删除记录或初始化审计系统操作。	1.审计系统应该提供必要的访问控制功能，并且提供ACL权限列表控制。或为审计功能提供独立的管控环境； 2.审计记录应该与系统运行维护情况基本一致，不能出现记录中断或明显跳跃情况； 3.低权限用户无法删除或初始化审计数据。	技术类
4.1.3.5	网络安全/网络安全审计/审计	必测项	1.网络应该提供安全审计工具； 2.审计工具应该	1.访谈网络管理员，询问是否配有网络审计工具；	1.网络应该具备安全审计工具； 2.审计服务应该处于开启状态，且能够按要求定制导出审计报	技术类

编号	检测项	检测说明	技术要求细化	检测方法及步骤	预期结果及判定	类别
	工具		提供日志规划功能、可以进行分析形成审计报告； 3.网络审计工具提供自我数据保护功能。	2.检查网络安全审计工具状态和配置； 3.操作审计工具进行定制导出操作。	告报表； 3.应定义审计跟踪极限的阈值，当存储空间接近极限时，能采取必要的措施，当存储空间被耗尽时，终止可审计事件的发生。	
4.1.4.1	网络安全/边界完整性检查/内外网非法连接阻断和定位	必测项	1.应能够对非授权设备私自连接到内部网络的行为进行检查，准确定出位置，并对其进行有效阻断； 2.应能够对内部网络用户私自连接到外部网络的行为进行检查，准确定出位置，并对其进行有效阻断。	1.访谈网络管理员，询问是否针对办公网设置了防私自接入的实时管控系统； 2.使用非授权电脑接入到内网的网络端口上，在网络管控系统端查看结果； 3.访谈网络管理员，询问是否针对内网用户接入外网设置了实时的管控系统； 4.使用内网电脑插入3G 上网卡或通过拨号设备连接到外部互联网，在网络管控系统端查看结果。	1.应该具有防外部设备私自接入内网的实时管控系统； 2.接入的电脑被立即阻断，无法获得有效 IP,无法访问内网中其他主机，管控系统端显示非法接入端口的位置信息； 3.应该具有防内部设备私自连入外网的实时管控系统； 4. 接入的电脑在插入移动上网卡后被管控系统发现后阻断（实行内网接入认证，禁止多网卡接入）。	技术类
4.1.5.1	网络安全/网络入侵防范/网络ARP 欺骗攻击	必测项	应对重要网段采取网络地址与数据链路地址双向绑定的措施，或采用其他有效防范机制。	1.检查边界和重要网络设备，查看是否有防范网络ARP欺骗攻击的措施（如对重要网段采取网络地址与数据链路地址绑定等）； 2.查看网络设备配置，是否进行地址绑定，或采用其他有效防范机制。	1.边界和重要网络设备配置信息中有对重要服务器采用 IP 地址和 MAC 地址绑定的措施； 2.查看网络设备配置，进行地址绑定，或采用其他有效防范机制。	技术类
4.1.5.2	网络安全/网络入侵防范/信息窃取	必测项	1.应有防范信息窃取的措施； 2.应启用防范信息窃取措施。	1.访谈网络管理员，询问网络中有无防范信息窃取的措施（如使用SSH 对所有传输数据进行加密等）； 2.检测是否启用防范	1.网络管理员说明网络中使用SSH 对所有传输数据进行加密； 2.查看系统进程中已启用SSH服务。	技术类

编号	检测项	检测说明	技术要求细化	检测方法及步骤	预期结果及判定	类别
				信息窃取措施。		
4.1.5.3	网络安全/网络入侵防范/DoS/DDoS攻击	必测项	应具有防DoS/DDoS安全设备或有效技术手段。	1.访谈网络管理员，询问部署何种安全设备来抵抗DoS/DDoS攻击。检查在安全设备中是否开启防DoS/DDoS攻击策略等； 2.访谈网络管理员，询问是否有除安全设备外的其他防DoS/DDoS措施，并检查相应技术措施是否已启用。	1.网络管理员说明已部署安全设备来抵抗DoS/DDoS攻击。查看安全策略设置中已启用防DoS/DDoS策略； 2.网络管理员说明针对DoS/DDoS攻击已购买运营商流量清洗服务，查看具有相应合同文件。	技术类
4.1.5.4	网络安全/网络入侵防范/网络入侵防范机制	必测项	1.应具备网络入侵防范措施； 2.应能监视到端口扫描等攻击行为； 3.应记录攻击行为的日志信息，并能提供报警。	1.访谈网络管理员，询问网络入侵防范措施有哪些；询问是否有专门的设备对网络入侵进行防范；询问采取什么方式进行网络入侵防范规则库升级； 2.检查网络入侵防范设备，查看是否能检测以下攻击行为：端口扫描、强力攻击、木马后门攻击、拒绝服务攻击、缓冲区溢出攻击、IP碎片攻击、网络蠕虫攻击等； 3.检查网络入侵防范设备，查看入侵事件记录中是否包括攻击源IP、攻击类型、攻击目的、攻击时间等；查看是否设置了安全警告方式（如采取屏幕实时提示、email告警、声音告警等）。	1.网络管理员说明采用的网络入侵防范措施，如部署网络入侵防范设备等。采取自动或手动及时更新的方式对网络入侵防范规则库进行升级； 2.网络入侵防范设备中有已检测到的攻击行为记录，如端口扫描、强力攻击、木马后门攻击、拒绝服务攻击、缓冲区溢出攻击、IP碎片攻击、网络蠕虫攻击等； 3.网络入侵防范设备的入侵事件记录中包含攻击源IP、攻击类型、攻击目的、攻击时间等；并设置了安全告警（如屏幕实时提示、email告警、声音告警等）。	技术类
4.1.6.1	网络安全/恶意代码防范/恶意	必测项	应具备网络防恶意代码防范措施。	1.访谈网络管理员，询问系统中的网络防恶意代码防范措施是什	1.网络管理员说明，系统中的网络防恶意代码防范措施是部署防恶意代码产品；	技术类

编号	检测项	检测说明	技术要求细化	检测方法及步骤	预期结果及判定	类别
	代码防范措施			么；询问防恶意代码产品的有哪些主要功能； 2.检查在网络边界及核心业务网段处是否有相应的防恶意代码的措施。	2.在网络边界及核心业务网段处有部署防病毒网关等产品。	
4.1.6.2	网络安全/恶意代码防范/定时更新	必测项	1.应具备恶意代码库更新策略（自动更新、定期手动更新）； 2.恶意代码库应为最新版本。	1.访谈网络管理员，询问恶意代码库的更新策略； 2.检查防恶意代码产品，查看恶意代码库是否为最新版本。	1.网络管理员说明，恶意代码库的更新策略为自动或手动定时更新； 2.防恶意代码产品的恶意代码库为最新版本。	技术类
4.1.7.1	网络安全/网络设备防护/设备登录设置	必测项	1.应具备身份鉴别措施，不允许管理员共用账户； 2.网络设备不允许使用默认口令； 3.主要网络设备宜对同一用户选择两种或两种以上组合的鉴别技术来进行身份鉴别。	1.访谈网络管理员，询问登录网络设备的用户是否进行了身份鉴别措施；采用了哪些鉴别技术实现身份鉴别（如用户名口令、挑战应答、动态口令等）；是否为每个管理员设置了单独的账户； 2.检查网络设备是否对登录用户进行了身份鉴别，是否修改了默认的用户名及密码； 3.登录网络设备，查看设置的用户是否有相同用户名； 4.在管理员的配合下验证主要网络设备上对同一用户启用的两种或两种以上组合的身份鉴别技术是否有效。	1.网络设备对登录用户进行了身份鉴别，而且修改了默认的用户名和密码； 2.网络设备上设置的用户不存在相同的用户名； 3.使用任何一种身份鉴别技术不能登录，使用规定的组合的身份鉴别技术可以登录。	技术类
4.1.7.2	网络安全/网络设备防护/设备登录口令安全性	必测项	1.应具有身份鉴别信息防冒用措施； 2.口令应具备复杂度要求并定期更换（至少8位，	1.访谈网络管理员，询问对网络设备的身份鉴别信息防冒用所采取的具体措施，如使用口令的组成、长度和更改周期等；	1.网络管理员说明，登录网络设备的口令由字母、数字、特殊字符组成，至少8位，定期更改； 2.使用双因素认证，符合本要求。	技术类

编号	检测项	检测说明	技术要求细化	检测方法及步骤	预期结果及判定	类别
			并包含字母数字及特殊字符)。	2.如登录符合双因素认证要求，则不对口令复杂度进行具体要求。		
4.1.7.3	网络安全/网络设备防护/登录地址限制	必测项	应对网络设备的管理员登录地址进行限制。	1.访谈网络管理员，询问网络设备的管理员登录地址是否进行了限制； 2.检查网络设备上的安全设置，查看是否对网络设备的管理员登录地址进行限制。	网络设备中限制了管理员登录地址。	技术类
4.1.7.4	网络安全/网络设备防护/远程管理安全	必测项	1.网络设备远程管理应具备防窃听措施； 2.应启用网络设备远程管理防窃听措施。	1.访谈网络管理员，询问对网络设备远程管理时，是否在网络传输过程中有防窃听措施； 2.检查网络设备上的安全设置，查看对网络设备远程管理时，是否有安全措施（如采用SSH、HTTPS 等加密协议）防止鉴别信息在网络传输过程中被窃听。	1.网络管理员说明，在对网络设备远程管理时，在网络传输过程中利用SSH防窃听； 2.网络设备中配置了传输协议SSH来防止鉴别信息在网络传输过程中被窃听。	技术类
4.1.7.5	网络安全/网络设备防护/设备用户设置策略	必测项	1.网络设备应具有登录失败处理功能； 2.网络设备应启用登录失败处理功能。	1.访谈网络管理员，询问网络设备是否有登录失败处理功能（如结束会话、限制非法登录次数和当网络登录连接超时自动退出等措施）； 2.检查网络设备上的安全设置，查看其是否有对鉴别失败采取相应的措施的设置；查看其是否有限制非法登录次数的功能；查看是否设置网络登录连接超时，并自动退出。	1.网络管理员说明，网络设备具有登录失败处理功能，如结束会话、限制非法登录次数和当网络登录连接超时自动退出等措施； 2.网络设备中已配置实现登录失败时结束会话、限制非法登录次数，网络登录连接超时时间，超时后自动退出。	技术类
4.1.7.6	网络安全/网络设备防护/权限	必测项	网络设备应进行特权用户权限分离。	1.访谈网络管理员，询问网络设备是否实现设备特权用户的权限	1.网络设备已实现特权用户权限分离，每个特权用户仅分配完成其任务的最小权限；	技术类

编号	检测项	检测说明	技术要求细化	检测方法及步骤	预期结果及判定	类别
	分离			分离； 2.检查网络设备是否实现设备特权用户的权限分离（每个管理员账户是否仅分配完成其任务的最小权限）； 3.测试网络设备的安全设置，验证设备特权用户的权限分离（如普通操作员账户的权限分配列表中是否含有审核权限）。	2.网络设备目前有不同的特权用户； 3.普通操作员账户的权限分配列表中不含有高阶的审核权限。	
4.1.7.7	网络安全/网络设备防护/最小化服务	必测项	1.网络设备应实现设备的最小服务配置； 2.应对配置文件进行定期离线备份。	1.访谈网络管理员，询问是否实现设备的最小化服务配置，并对配置文件进行定期离线备份； 2.检查网络设备是否已实现最小化服务配置（如开启的服务端口都是业务需要等），是否对网络设备的配置文件进行定期离线备份（查看离线备份记录是否满足定期备份）。	1.网络设备已实现最小服务配置，并对配置文件已进行定期离线备份，有相应备份记录； 2.网络设备目前开启的服务端口都是业务需要的，离线备份记录满足定期要求。	技术类
4.1.8.1	网络安全/网络安全管理/网络设备运维手册	必测项	1.应具备网络安全管理制度，至少包括对网络安全配置、日志保存时间、安全策略、升级与打补丁、口令更新周期等方面； 2.应保证所有与外部系统的连接均得到授权和批准； 3.应定期检查违反规定拨号上网或其他违反网络	1.检查网络安全管理制度，查看其是否覆盖网络安全配置、日志保存时间、安全策略、升级与打补丁、口令更新周期等内容； 2.访谈网络管理员，询问系统网络的外联种类有哪些（互联网、合作伙伴企业网、上级部门网络等），是否都得到授权与批准，由何部门/何人批准；是否有授权和批准记录； 3.检查是否定期检查	1.网络安全管理制度中含有对网络安全配置、日志保存时间、安全策略、升级与打补丁、口令更新周期等内容； 2.系统网络的外联种类是上级部门网络，所有外联行为均得到授权和批准，拥有授权和批准记录； 3.有定期检查违反规定拨号上网或其他违反网络安全策略的行为记录，满足定期检查要求。	技术类

编号	检测项	检测说明	技术要求细化	检测方法及步骤	预期结果及判定	类别
			安全策略行为的记录。	违反规定拨号上网或其他违反网络安全策略的行为。		
4.1.8.2	网络安全/网络安全管理/定期补丁安装	必测项	1.软件版本升级前，应对重要文件进行备份； 2.应及时更新重要安全补丁。	1.访谈网络管理员，询问是否根据厂家提供的软件升级版本对网络设备进行过升级，升级前是否对重要文件（账户数据、配置数据等）进行备份； 2.检查目前的软件版本号为多少，是否存在升级备份记录，采取什么方式进行备份重要文件（热备、冷备）。	1.根据厂家提供的软件升级版本及时对网络设备进行升级，升级前对重要文件（账户数据、配置数据等）进行备份； 2.及时更新重要安全补丁。	技术类
4.1.8.3	网络安全/网络安全管理/漏洞扫描	必测项	1.应至少半年对网络系统进行一次漏洞扫描，并提供扫描记录； 2.应对扫描发现的漏洞进行及时处理。	1.访谈网络管理员，询问是否对网络设备进行过漏洞扫描（多久一次），对扫描出的漏洞是否及时修补，使用的扫描工具是什么； 2.检查网络漏洞扫描报告，查看其内容是否覆盖网络存在的漏洞、严重级别、原因分析和改进意见等方面。	1.至少半年对网络设备进行漏洞扫描，并会对扫描出的漏洞进行及时修补，使用的扫描工具符合要求； 2.网络漏洞扫描报告内容覆盖网络存在的漏洞、严重级别、原因分析和改进意见等方面。	技术类
4.1.8.4	网络安全/网络安全管理/网络数据传输加密	必测项	服务器远程管理应启用防窃听措施。	1.访谈网络管理员，询问对服务器进行远程管理时，是否在网络传输过程中有防窃听措施； 2.检查服务器上的安全设置，查看对服务器管理时，是否有安全措施（如采用SSH、HTTPS等加密协议）防止鉴别信息在网络传输过程中被窃听； 3.测试对服务器进行远程管理时，防窃听措	1.在对服务器进行远程管理时，在网络传输过程中利用SSH防窃听； 2.服务器配置了传输协议SSH等来防止鉴别信息在网络传输过程中被窃听； 3.使用抓包工具抓取网络传输报文，传输报文已加密。	技术类

编号	检测项	检测说明	技术要求细化	检测方法及步骤	预期结果及判定	类别
				施的有效性（如使用抓包工具抓取网络传输报文，查看是否包含明文信息）。		
4.1.9.1	网络安全/网络相关人员安全管理/网络安全管理人员配备	必测项	应指定专人负责网络安全管理工作。	访谈网络管理员，询问是否指定专人负责维护网络运行日志、监控记录和分析处理报警信息等网络安全管理工作。	1.指定专人负责维护网络运行日志、监控记录和分析处理报警信息等网络安全管理工作； 2.提供运维配套记录。	技术类
4.1.9.2	网络安全/网络相关人员安全管理/网络安全管理人员责任划分规则	必测项	1.应具备网络安全管理岗位制度； 2.制度中应明确安全管理岗位的职责、分工和技能要求。	1.访谈网络管理员，询问是否明确安全管理岗位的职责、分工和技能要求； 2.检查网络安全管理岗位制度，查看各个岗位的职责范围是否清晰、明确；查看文件是否明确各个岗位人员应具有的技能要求。	网络安全管理岗位制度中含有各个岗位的职责范围以及各个岗位人员应具有的技能要求。	技术类
4.1.9.3	网络安全/网络相关人员安全管理/网络安全关键岗位人员管理	必测项	1.应从内部人员中选拔从事关键岗位的人员，并签署岗位安全协议； 2.应对关键岗位的人员进行全面、严格的安全审查和技能考核。	1.访谈人事工作人员，询问关键岗位的人员是如何选拔的，是否对被录用人的身份、背景、专业资格和资质进行审查，录用后是否与其签署岗位安全协议； 2.检查岗位安全协议，查看是否有岗位安全保密范围、岗位安全保密责任、违约责任、协议的有效期限和责任人签字等。检查关键岗位人员的技能考核文档或记录，查看是否记录考核内容和考核结果等。	1.人事工作人员说明，关键岗位的人员审慎选拔，并对被录用人的身份、背景、专业资格和资质进行审查，录用后与其签署岗位安全协议； 2.岗位安全协议或相关文档中含有岗位安全保密范围、岗位安全保密责任、违约责任、协议的有效期限和责任人签字等内容，而且关键岗位人员的技能考核记录中记录有考核内容和考核结果等。	技术类

8.2 主机安全性测试

对支付业务设施的主机安全防护进行检测，考察主机的安全控制能力。检测内容见表5。

表5　主机安全性测试

编号	检测项	检测说明	技术要求细化	检测方法及步骤	预期结果及判定	类别
4.2.1.1	主机安全/身份鉴别/系统与应用管理员用户设置	必测项	1.应具备身份鉴别措施，不允许管理员共用账户； 2.主机设备不允许使用默认口令； 3.主要主机设备宜对同一用户选择两种或两种以上组合的鉴别技术来进行身份鉴别。	1.访谈系统管理员，询问操作系统的身份标识与鉴别机制采取何种措施实现；访谈数据库管理员，询问数据库的身份标识与鉴别机制采取何种措施实现；采用了哪些鉴别技术实现身份鉴别（如用户名口令、挑战应答、动态口令等）； 2.检查服务器操作系统文档和数据库管理系统文档，查看用户身份标识的唯一性是由什么属性来保证的（如用户名或者 UID 等）； 3.测试服务器操作系统和数据库系统，当进入系统时，是否先需要进行标识（如建立账号），而没有进行标识的用户不能进入系统；测试重要服务器操作系统和重要数据库管理系统，添加一个新用户，其用户标识为系统原用户的标识（如用户名或 UID），查看是否不会成功；测试重要服务器操作系统和重要数据库管理系统，删除一个用户标识，然后再添加一个新用户，其用户标识和所删除的用户标识一样（如用户名或 UID），查看是否不能成功； 4.在管理员的配合下验证主机系统上对同一用户启用的两种或两种以上组合的身份鉴别技术是否有效。	1.登录服务器操作系统和数据库系统使用两种或两种以上用户身份鉴别方式； 2.服务器操作系统和数据库系统利用 UID 来保证用户身份标识唯一性； 3.进入服务器操作系统和数据库系统需要先进行标识才能进入；不能添加一个已存在的用户标识；不能成功添加一个已删除的用户标识； 4.使用任何一种身份鉴别技术不能登录，使用规定的组合的身份鉴别技术可以登录。	技术类

编号	检测项	检测说明	技术要求细化	检测方法及步骤	预期结果及判定	类别
4.2.1.2	主机安全/身份鉴别/系统与应用管理员口令安全性	必测项	1.身份鉴别信息防冒用措施； 2.口令应具备复杂度要求并定期更换（至少8位，并包含字母数字及特殊字符）。	1.访谈主机管理员，询问对主机设备的身份鉴别信息防冒用所采取的具体措施，如使用口令的组成、长度和更改周期等； 2.如登录符合双因素认证要求，则不对口令复杂度进行具体要求。	1.登录主机设备的口令由字母、数字、特殊字符组成，至少8位，定期更改； 2.使用双因素认证，符合本要求。	技术类
4.2.1.3	主机安全/身份鉴别/登录策略	必测项	1.主机设备应具有登录失败处理功能； 2.主机设备应启用登录失败处理功能。	1.访谈主机管理员，询问主机设备是否有登录失败处理功能（如结束会话、限制非法登录次数和当网络登录连接超时自动退出等措施）； 2.检查主机设备上的安全设置，查看其是否有对鉴别失败采取相应的措施的设置；查看其是否有限制非法登录次数的功能；查看是否设置主机登录连接超时，并自动退出。	1.主机设备具有登录失败处理功能，如结束会话、限制非法登录次数和当网络登录连接超时自动退出等措施； 2.主机设备中已配置实现登录失败时结束会话、限制非法登录次数，网络登录连接超时时间，超时后自动退出。	技术类
4.2.2.1	主机安全/访问控制/访问控制范围	必测项	主机设备应进行特权用户权限分离。	1.访谈主机管理员，询问主机设备是否实现设备特权用户的权限分离； 2.检查主机设备是否实现设备特权用户的权限分离（每个管理员账户是否仅分配完成其任务的最小权限）； 3.测试主机设备的安全设置，验证设备特权用户的权限分离（如普通操作员账户的权限分配列表中是否含有审核权限）。	1.主机设备已实现特权用户权限分离，每个特权用户仅分配完成其任务的最小权限； 2.主机设备目前有不同的特权用户； 3.普通操作员账户的权限分配列表中不含有高阶的审核权限。	技术类
4.2.2.2	主机安全/访问控制/主机信任关系	必测项	应避免不必要的主机信任关系。互相信任的主机之间无需进行身份认证即可登录进行操作。	1.访谈主机管理员，询问主机是否启用了信任关系； 2.检查服务器上的安全设置，查看信任主机是否在客户提供的可信任主机列	1.未启用非必要的主机信任关系； 2.主机中配置的可信任主机列表均在客户提供的可信任主机列表中； 3.可信任主机间的主机	技术类

编号	检测项	检测说明	技术要求细化	检测方法及步骤	预期结果及判定	类别
				表中； 3.测试可信任关系的有效性（如可信任主机间的主机 A 是否可以不用输入登录密码登录到它的可信任主机 B)。	A 可以不用输入登录密码登录到它的可信任主机 B。	
4.2.2.3	主机安全/访问控制/默认过期用户	必测项	1.应及时删除共用账户，过期账户，默认账户等； 2.应严格限制默认账户的访问权限，重命名系统默认账户，修改这些账户的默认口令。	1.访谈主机管理员，询问是否已及时删除了多余的、过期的账户，是否存在共享账户，是否修改了默认账户及口令； 2.检查操作系统和数据库系统的访问控制列表，查看授权用户中是否不存在过期的账号和无用的账号等；查看设置的用户是否有相同用户名； 3.查看操作系统和数据库系统的匿名/默认用户的访问权限是否已被禁用或者严格限制（如限定在有限的范围内)；以未授权用户身份/角色访问客体，验证是否不能进行访问。	1.及时删除了多余的、过期的账户，不存在共享账户，修改了默认账户及口令； 2.操作系统和数据库系统中不存在过期的账号、无用的账号、共用账户等； 3.操作系统和数据库系统的匿名/默认用户的访问权限已被禁用；以未授权用户身份/角色访问客体，不能进行访问。	技术类
4.2.3.1	主机安全/安全审计/日志信息	必测项	1.应开启安全审计； 2.审计范围应覆盖到服务器和重要客户端上的每个操作系统用户和数据库用户； 3.审计内容应包括重要用户行为、系统资源的异常使用和重要系统命令的使用等系统内重要的安全相关事件； 4.审计记录应包括事件的日期、时间、类型、主体标识、客体标识和结果等； 5.审计记录应真实有	1.访谈主机管理员，询问主机系统是否开启了安全审计功能，如果开启了安全审计功能是否有第三方审计工具或系统； 2.检查操作系统和数据库系统，查看当前审计范围是否覆盖到每个用户； 3.检查操作系统和数据库系统，查看审计策略是否包括系统内重要的安全相关事件，例如，用户标识与鉴别、自主访问控制的所有操作记录、重要用户行为（如用超级用户命令改变用户身份，删除系统	1.主机系统已开启了安全审计功能，使用的是第三方审计工具； 2.审计范围已经覆盖到每个操作系统用户和数据库用户； 3.审计策略包括系统内重要的安全相关事件，如用户标识与鉴别、自主访问控制的所有操作记录、重要用户行为(如用超级用户命令改变用户身份，删除系统表)、系统资源的异常使用、重要系统命令的使用（如删除客体）等；	技术类

编号	检测项	检测说明	技术要求细化	检测方法及步骤	预期结果及判定	类别
			效。	表）、系统资源的异常使用、重要系统命令的使用（如删除客体）等； 4.检查操作系统和数据库系统，查看审计记录信息是否包括事件发生的日期与时间、触发事件的主体与客体、事件的类型、事件成功或失败、身份鉴别事件中请求的来源（如末端标识符）、事件的结果等内容； 5.测试操作系统和数据库系统，在系统上以某个用户试图产生一些重要的安全相关事件（如鉴别失败等），测试安全审计的记录情况与要求是否一致。	4.审计记录信息包括事件发生的日期与时间、触发事件的主体与客体、事件的类型、事件成功或失败、身份鉴别事件中请求的来源（如末端标识符）、事件的结果等内容； 5.安全审计记录中含有用户鉴别失败的记录。	
4.2.3.2	主机安全/安全审计/日志权限和保护	必测项	1.应具有审计记录的存储和保护的措施； 2.应保护审计记录，避免受到未预期的删除、修改或覆盖等； 3.审计进程应受到保护。	1.访谈主机管理员，询问审计记录的存储和保护的措施（如配置日志服务器，启用日志守护进程syslogd等）； 2.测试服务器操作系统和数据库系统，在系统上以某个用户试图删除、修改或覆盖审计记录，测试安全审计的保护情况与要求是否一致； 3.测试操作系统和数据库系统，用户可通过非法终止审计功能或修改其配置，验证审计功能是否受到保护。	1.审计记录存储在日志服务器上，并已启用日志守护进程syslogd等； 2.用户删除、修改或覆盖审计记录失败； 3.用户不能非法终止审计功能或修改其配置。	技术类
4.2.3.3	主机安全/安全审计/系统信息分析	必测项	应能够根据记录数据进行分析，并生成审计报表。	1.访谈主机管理员，询问是否能根据记录数据进行分析，并生成审计报表； 2.测试服务器操作系统和数据库系统，查看是否为授权用户浏览和分析审计	1.可根据记录数据进行分析，并生成审计报表； 2.已为授权用户浏览和分析审计数据提供专门的审计工具，用于生成审计报表。	技术类

编号	检测项	检测说明	技术要求细化	检测方法及步骤	预期结果及判定	类别
				数据提供专门的审计工具（如对审计记录进行分类、排序、查询、统计、分析和组合查询等），并能根据需要生成审计报表。		
4.2.4.1	主机安全/系统保护/系统备份	必测项	1.应具有系统备份或系统重要文件备份； 2.应对备份方式、备份周期、备份介质进行要求； 3.备份应真实有效。	1.访谈主机管理员，询问主要对哪些系统备份或系统重要文件进行备份； 2.检查是否具有规定备份方式（热备、冷备）、备份周期文档； 3.检查备份数据的存放场所、备份介质（如磁带等）、备份记录等，是否对备份和冗余设备的有效性定期维护和检查。	1.主要对业务信息、系统数据及软件系统以及系统重要文件等进行备份； 2.按照要求对系统及文件进行了备份，并对备份记录进行了保管。	技术类
4.2.4.2	主机安全/系统保护/故障恢复策略	必测项	应具备各种主机故障恢复策略。	1.访谈主机管理员，询问是否具有主机故障恢复策略文档； 2.检查主机故障恢复策略文档是否包含故障恢复策略的操作流程、紧急联系人、恢复时间要求等； 3.定期执行恢复程序，确保各种主机故障恢复策略是否有效。	1.具有主机故障恢复策略文档； 2.主机故障恢复策略文档包含故障恢复策略的操作流程、紧急联系人、恢复时间要求等； 3.定期对主机故障恢复策略进行验证，具有验证记录。	技术类
4.2.4.3	主机安全/系统保护/磁盘空间安全	必测项	1.应具备磁盘监控措施； 2.应对主机磁盘空间进行合理规划，确保磁盘空间使用安全。	1.访谈主机管理员，询问是否对主机磁盘空间进行监控； 2.检查磁盘空间的划分策略是否合理，以及采取了哪些保证磁盘使用安全的措施。	1.对主机磁盘空间进行监控，并提供记录； 2.防止在单磁盘出现问题时影响服务（如RAID、磁盘阵列等）。	技术类
4.2.4.4	主机安全/系统保护/主机安全加固	必测项	1.应具有主机加固策略； 2.应进行过主机加固，并具备相应记录。	1.访谈主机管理员，询问是否有主机加固策略，是否进行过主机加固，是否有主机加固记录等； 2.依据主机加固策略测试主机加固是否有效，查看主机加固记录是否有操作	1.具有主机加固策略文档、进行过主机加固并具有主机加固记录； 2..主机已依照主机加固策略进行了加固，主机加固记录中包含有操作人、审核人、操作时间、加固	技术类

编号	检测项	检测说明	技术要求细化	检测方法及步骤	预期结果及判定	类别
				人、审核人、操作时间、加固策略等。	策略等。	
4.2.5.1	主机安全/剩余信息保护/剩余信息保护	必测项	1.应保证操作系统和数据库系统用户的鉴别信息所在的存储空间，被释放或再分配给其他用户前得到完全清除，无论这些信息是存放在硬盘上还是在内存中； 2.应确保系统内的文件、目录和数据库记录等资源所在的存储空间被释放或重新分配给其他用户前得到完全清除。	1.检查产品的测试报告、用户手册或管理手册，确认其是否具有相关功能；或由第三方工具提供了相应功能； 2.检查主要操作系统和主要数据库管理系统维护操作手册，查看是否明确用户的鉴别信息存储空间被释放或再分配给其他用户前的处理方法和过程；是否明确文件、目录和数据库记录等资源所在的存储空间被释放或重新分配给其他用户前的处理方法和过程。	1.如果测试报告、用户手册或管理手册中没有相关描述，且没有提供第三方工具增强该功能，则该项要求为不符合； 2.主要操作系统和主要数据库管理系统维护操作手册说明用户的鉴别信息存储空间被释放或再分配给其他用户前的处理方法和流程，以及明确文件、目录和数据库记录等资源所在的存储空间被释放或重新分配给其他用户前的处理方法和过程，且处理方法和流程确保剩余信息得到相应的保护。	技术类
4.2.6.1	主机安全/入侵防范/入侵防范记录	必测项	1.宜采取入侵防范措施； 2.宜能够检测到对重要服务器进行入侵的行为，能够记录入侵的源IP、攻击的类型、攻击的目的、攻击的时间，并在发生严重入侵事件时提供报警； 3.宜能够对重要程序的完整性进行检测，并在检测到完整性受到破坏后具有恢复的措施。	1.访谈系统管理员，询问是否采取入侵防范措施，入侵防范内容是否包括主机运行监视、特定进程监控、入侵行为检测和完整性检测等方面内容； 2.检查在主机系统层面是否有对入侵行为进行检测的相关措施：如主机系统本身是否提供并开启了相应的功能或是否部署了第三方工具提供了相应的功能； 3.检查在网络边界处是否有对网络攻击进行检测的相关措施：如部署并启用入侵检测系统； 4.检查入侵攻击检测日志； 5.检查采用何种报警方	1.系统管理员说明采取了入侵防范措施，入侵防范内容包括主机运行监视、特定进程监控、入侵行为检测和完整性检测方面； 2.主机层面提供并开启了相关功能或部署了第三方工具进行入侵行为的检测和完整性检测； 3.在网络边界处部署了IDS（IPS）系统，或UTM启用了入侵检测（保护）功能； 4.如果主机系统测试报告、用户手册或管理手册中没有相关描述，且在主机层面或网络层面没有提供第三方工具增强该功能，则该项要求为不符	技术类

编号	检测项	检测说明	技术要求细化	检测方法及步骤	预期结果及判定	类别
				式； 6.访谈系统管理员当检测到重要程序完整性受到破坏后的恢复措施。	合； 5.有入侵攻击相关日志记录； 6.在发生严重事件时应能够提供监控屏幕实时报警，最好有主动的声、光、电、短信、邮件等形式的一种或多种报警方式； 7.系统管理员说明在检测到重要程序完整性受到破坏后具有一定的恢复措施，如通过定期备份的文件进行恢复。	
4.2.6.2	主机安全/入侵防范/关闭服务和端口	必测项	1.应关闭不必要的服务； 2.应关闭不必要的端口。	1.访谈系统管理员，是否定期对系统中的服务和端口进行梳理，并关闭不必要的服务和端口； 2.查看系统中已经启动的或者是手动的服务，一些不必要的服务是否已启动,针对Windows系统可通过[开始]-[控制面板]-[管理工具]-[服务]查看服务的开启情况，针对Linux系统，可以查看/etc/inetd.conf文件查看服务开启情况； 3.输入netstat -an查看系统端口开放情况； 4.采用端口扫描工具，查看是否存在不必要的服务或端口。	1.定期对系统中的服务和端口进行了梳理，并关闭了不必要的服务和端口； 2.通过查看和扫描，系统中未发现不必要的服务和端口开启。	技术类
4.2.6.3	主机安全/入侵防范/最小安装原则	必测项	1.操作系统应遵循最小安装的原则，仅安装需要的组件和应用程序； 2.通过设置升级服务器等方式保持系统补丁及时得到更新。	1.访谈系统管理员，询问系统安装的组件和应用程序是否遵循了最小安装的原则； 2.查看系统中已经启动的或者是手动的服务，一些不必要的服务是否已启	1.系统安装的组件和应用程序遵循了最小安装的原则； 2.系统中不必要的服务没有启动,不必要的端口没有打开； 3.针对Windows操作系	技术类

编号	检测项	检测说明	技术要求细化	检测方法及步骤	预期结果及判定	类别
				动，输入 netstat －an 查看系统是否有不必要端口开启； 3.针对 Windows 操作系统，查看系统默认共享的开启情况： a)依次展开[开始]->[运行]，在文本框中输入 cmd 点确定，输入 net share，查看共享； b)依次展开[开始]->[运行]，在文本框中输入 regedit 点确定，查看 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\restrictanonymous 值是否为“0”； 4.访谈系统管理员，询问系统补丁升级的方法； 5.查看系统中补丁安装的情况，如对于 Windows 操作系统，可以通过[开始]->[运行]，在文本框中输入 regedit，查看 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Updates 下的安装补丁列表； 6.通过操作系统扫描工具对操作系统系统进行漏洞扫描，查看系统是否存在因补丁未及时更新而造成的风险漏洞。	统，非域环境中，关闭默认共享，即：a)“共享名”列为空，无 C$、D$、IPC$ 等默认共享，b)HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\restrictanonymous 值不为“0”(0 表示共享开启)； 4.通过部署升级服务器等方式进行了补丁升级，且补丁先测试，再升级； 5.系统中补丁号为较新版本； 6.漏洞扫描中未发现因补丁未及时更新而导致的风险漏洞。	
4.2.7.1	主机安全/恶意代码防范/防范软件安装部署	必测项	1.应安装防恶意代码软件； 2.防恶意代码软件的部署应覆盖所有生产设备。	1.查看系统中是否部署了防恶意软件； 2.访谈系统管理员，询问防恶意代码软件覆盖范围如何； 3.查看系统，是否生产系统的服务器均安装了防恶意代码软件。	1.安装了防恶意代码软件； 2.防恶意代码软件的覆盖范围至少包括生产系统的服务器。	技术类

编号	检测项	检测说明	技术要求细化	检测方法及步骤	预期结果及判定	类别
4.2.7.2	主机安全/恶意代码防范/病毒库定时更新	必测项	应及时更新防恶意代码软件版本和恶意代码库。	1.查看系统中是否部署了防恶意软件； 2.访谈系统管理员，询问防恶意代码软件版本和恶意代码库更新策略； 3.查看防恶意代码软件版本是否是最新版本以及恶意代码库的最新版本更新日期，是否超过一个星期。	1.安装了防恶意代码软件； 2.防恶意代码软件版本及时更新，恶意代码库及时更新。	技术类
4.2.7.3	主机安全/恶意代码防范/防范软件统一管理	必测项	应支持防范软件的统一管理。	访谈系统管理员，询问防恶意代码的管理方式，例如升级方式。	防恶意代码统一管理，统一升级。	技术类
4.2.8.1	主机安全/资源控制/连接控制	必测项	1.应通过设定终端接入方式、网络地址范围等条件限制终端登录； 2.应根据安全策略设置登录终端的操作超时锁定。	1.访谈系统管理员，询问是否设定了终端接入方式、网络地址范围等条件限制终端登录，并了解终端接入方式、网络地址范围等条件限制措施，即采用何种方式进行限制； 2.查看终端接入方式、网络地址范围等条件限制措施配置情况，如：a）查看主机防火墙或系统有无限制登录地址；b）针对Windows 操作系统，查看“TCP/IP 筛选”中是否对端口进行了限制；c）网络层面访问控制规则限制情况； 3.针对 Linux 操作系统，查看是否存在/etc/securetty 文件，是否合理设置每个登录账户的 ttys 参数，是否存在Console 项，通过查看/etc/ssh/sshd_config 是否禁止root 远程登录； 4.查看登录终端系统是否	1.设定了终端接入的方式、网络地址范围等条件限制终端登录； 2.采用了以下一种或几种措施对终端接入的方式、网络地址范围进行了限制：a)通过主机防火墙的配置对登录地址进行限制；b)针对 Windows 操作系统，在“TCP/IP 筛选”中对端口做了限制；c)在网络层面通过设置访问控制规则进行限制； 3. 存在/etc/secretty 文件，tty 参数尽量少，且在/etc/securetty 文件中存在 console 项，且禁止 root 远程登录，即/etc/ssh/sshd_config 中的 PermitRootLogin 为 no； 4.登录终端系统中设置了操作超时时间应在 10 分钟以下，且针对 Windows 操作系统在恢	技术类

编号	检测项	检测说明	技术要求细化	检测方法及步骤	预期结果及判定	类别
				都进行了操作超时锁定的配置：针对 Windows 操作系统，依次展开[开始]->[控制面板]->[显示]的屏幕保护程序，查看登录该服务器的终端是否设置了屏幕锁定，且是否勾选了恢复时使用密码保护；针对Linux操作系统，通过使用“cat /etc/profile”命令查看超时退出时间 TMOUT 参数的设置情况。	复时使用密码保护的选项勾选。	
4.2.8.2	主机安全/资源控制/资源监控和预警	必测项	1.应使用必要的服务器的资源监控手段； 2.监控的范围应包括重要的服务器，且监控内容是否覆盖服务器CPU、硬盘、内存、网络等资源； 3.服务器资源的分配应能满足其业务需求； 4.当系统服务水平降低到预先规定的最小值时，应能检测和报警。	1.访谈系统管理员，询问系统资源使用情况的监控方式，是否采用人工监控或有无第三方主机监控软件； 2.查看第三方主机监控软件，监控的范围是否覆盖所有的重要服务器，监控的内容是否包括服务器的CPU、硬盘、内存、网络等资源； 3.访谈系统管理员针对系统资源控制的管理措施，询问服务器是否为专用服务器； 4.如果是专用服务器，查看系统资源如 CPU 使用率等，实时利用率是不是不高；如果不是专用服务器，查看是否设置了单个用户对系统资源的最大或最小使用限度，当前资源的分配是否满足业务的需求； 5.针对系统服务水平的报警，人工监控不满足要求，询问系统管理员有无第三方主机监控程序。如果采用第三方主机监控程序，	1.如果人工监控，每日至少三次查看系统资源使用状况并记录。或使用集中监控平台实时监控系统资源使用情况； 2.集中监控平台的监控范围覆盖所有的重要服务器，且监控内容包括服务器的CPU、硬盘、内存、网络等资源； 3.如果服务器不是多业务竞争使用硬件资源且实时利用率不是很高，那么认为不存在资源紧张情况，则该项要求为不适用。确实需要多业务公用资源的，确定当前的资源分配方式能满足业务需求，如果存在资源争夺情况且没有采取其他措施实现该要求，则该项要求为不符合； 4.针对系统服务器水平报警，如果采用人工监控，本条判定为不符合，但在综合风险分析中可降低本条风险如采用第三方主机监控程序，且其	技术类

编号	检测项	检测说明	技术要求细化	检测方法及步骤	预期结果及判定	类别
				则查看是否有报警功能。	提供主动的声、光、电、短信、邮件等形式的一种或多种报警方式 ，本条判为符合。	
4.2.9.1	主机安全/主机安全管理/主机运维手册	必测项	1.应建立系统安全管理制度； 2.应对系统安全策略、安全配置、日志管理和日常操作流程等方面做出具体规定。	1.访谈系统管理员，询问是否对系统安全进行制度化管理； 2.应检查系统安全管理制度，查看其内容是否覆盖系统安全配置（包括系统的安全策略、授权访问、最小服务、升级与打补丁）、系统账户（用户责任、义务、风险、权限审批、权限分配、账户注销等）、审计日志以及配置文件的生成、备份、变更审批、符合性检查等方面。	1.具有系统安全管理制度； 2.制度中系统安全策略、安全配置、日志管理和日常操作流程等内容完备。	管理类
4.2.9.2	主机安全/主机安全管理/漏洞扫描	必测项	应定期进行漏洞扫描，对发现的系统安全漏洞及时进行修补。	1.检查系统漏洞扫描策略文档，文档中是否规定了扫描周期、对象等； 2.访谈系统管理员，询问是否对系统进行过漏洞扫描，扫描周期多长，发现漏洞是否及时修补； 3.检查系统漏洞扫描报告，查看其内容是否描述了系统存在的漏洞、严重级别、原因分析和改进意见等方面，检查扫描时间间隔与扫描周期是否一致； 4.检查漏洞修复记录表或相应的系统加固报告，查看其内容是否针对发现的安全漏洞进行修复或加固。	1.具有系统漏扫策略文档，文档中规定了扫描周期、对象等； 2.系统管理员说明对系统进行定期漏洞扫描，并及时修补发现的漏洞； 3.具有漏洞扫描报告，且扫描报告和策略中的扫描周期一致，且其内容描述了系统存在的漏洞、严重级别、原因分析和改进意见等方面； 4.具有漏洞修复记录表或相应的系统加固报告，其内容是针对发现的安全系统漏洞的修复或加固。	管理类
4.2.9.3	主机安全/主机安全管理/	必测项	1.应具有主机系统补丁安装方案或制度，并根据方案或制度及时	1.检查系统补丁安装或升级策略文档，文档中是否规定了补丁安装周期、安	1.具有系统补丁安装或升级策略文档，规定了补丁安装周期、安装流程	管理类

编号	检测项	检测说明	技术要求细化	检测方法及步骤	预期结果及判定	类别
	系统补丁		更新系统补丁； 2.在安装系统补丁前，应首先在测试环境中测试通过，并对重要文件进行备份后，方可实施系统补丁程序的安装。	装流程等； 2.应访谈系统管理员，询问是否定期对系统安装安全补丁程序，在安装系统补丁程序前是否经过测试，并对重要文件进行备份； 3.应检查是否有补丁测试记录和系统补丁安装操作记录，检查记录和策略要求的周期是否一致； 4.查看系统中系统补丁的安装情况及安装时间。	等； 2.系统管理员说明定期对安装系统补丁程序，在安装前，进行测试并备份重要文件； 3.具有补丁测试记录和系统安装操作记录，且记录和策略要求的周期一致； 4.系统中安装较新系统补丁（参考技术检查结果）。	
4.2.9.4	主机安全/主机安全管理/操作日志管理	必测项	1.应具有完备的系统操作手册，其内容是否覆盖操作步骤、维护记录、参数配置等方面； 2.应具有详细操作日志； 3.应定期对系统运行日志和审计数据进行分析； 4.应具有审计分析报告。	1.检查系统操作手册，查看其内容是否覆盖操作步骤、维护记录、参数配置等方面； 2.检查是否有详细操作日志（包括重要的日常操作、运行维护记录、参数的设置和修改等内容）； 3.应访谈审计员，询问是否定期对系统运行日志和审计数据进行分析； 4.应检查是否有定期对系统运行日志和审计数据的分析报告，查看报告是否能够记录账户的连续多次登录失败、非工作时间的登录、访问受限系统或文件的失败尝试、系统错误等非正常事件。	1.系统操作手册内容完备，覆盖系统操作步骤、维护记录、参数配置等方面； 2.操作日志内容详细，包括重要的日常操作、运行维护记录、参数的设置和修改等内容； 3.审计员说明定期对系统运行日志和审计数据进行分析； 4.具有定期的日志分析报告，能够记录账户的连续多次登录失败、非工作时间的登录、访问受限系统或文件的失败尝试、系统错误等非正常事件。	管理类
4.2.10.1	主机安全/主机相关人员安全管理/主机安全管理人员配备	必测项	1.应指定专人对系统进行管理； 2.应划分系统管理员角色，明确各个角色的权限、责任； 3.权限设定应遵循最小授权原则。	1.访谈系统管理员，询问是否指定专人负责系统管理工作，是否对系统账户进行分类管理，权限设定是否遵循最小授权原则； 2.检查系统安全管理制度，查看是否对系统管理员用户进行分类（比如：	1.指定了专人负责系统管理工作，系统账户进行了分类管理并遵循最小授权原则； 2.系统安全管理制度中有对角色划分、权限等的说明（比如：划分不同的管理角色，系统管理权限	管理类

编号	检测项	检测说明	技术要求细化	检测方法及步骤	预期结果及判定	类别
				划分不同的管理角色，系统管理权限与安全审计权限分离等）； 3.查看系统中管理用户及角色的分配的情况，是否按照系统安全管理制度对系统账户进行了分类设置，且权限设定遵循最小授权原则。	与安全审计权限分离等）； 3.技术检查结果说明按照系统安全管理制度进行了系统管理员用户的分类（至少应该有系统管理员和安全审计员），权限设定遵循最小授权原则（参考技术检查结果）。	
4.2.10.2	主机安全/主机相关人员安全管理/主机安全管理人员责任划分规则	必测项	1.应具有主机管理员等相关岗位职责的正式文件； 2.文件内容应包含主机管理员等相关岗位的职责、分工和技能要求。	检查岗位职责文件，查看文件是否明确主机管理岗位的职责范围和分工。查看文件是否明确主机管理岗位人员应具有的技能要求。	1.具有岗位职责的正式文件； 2.文件中明确了主机管理员等相关岗位的工作职责分工，包含主机管理岗位人员的技能要求。	管理类
4.2.10.3	主机安全/主机相关人员安全管理/主机安全关键岗位人员管理	必测项	1.应设定关键岗位； 2.应签署岗位安全协议； 3.岗位安全协议内容应包含安全责任定义、协议有效期限和责任人签字等； 4.应对关键岗位进行安全审查。	1.访谈人事负责人，询问是否设定关键岗位，对从事关键岗位的人员是否从内部人员中选拔，是否要求其签署岗位安全协议； 2.检查岗位安全协议，查看是否具有岗位安全责任定义、违约责任、协议的有效期限和责任人签字等内容； 3.访谈人员录用负责人员，询问对关键岗位人员的安全审查和考核与一般岗位人员有何不同，审查内容是否包括操作行为和社会关系等。	1.设定了关键岗位，对从事关键岗位的人员从内部人员选拔，并签署岗位安全协议； 2.具有岗位安全协议，且岗位安全协议中包含安全责任定义、违约责任、协议的有效期限和责任人签字等内容； 3.对关键岗位人员的安全审查和考核与一般岗位不同，审查内容包括操作行为和社会关系等。	管理类

8.3 应用安全性测试

对支付业务设施的应用安全性检测，主要检测应用系统对非法访问及操作的控制能力。检测内容见表6。

表6　应用安全性测试

编号	检测项	检测说明	技术要求细化	检测方法及步骤	预期结果及判定	类别
4.3.1.1	应用安全/身份鉴别/系统与普通用户设置	必测项	1.业务系统、管理系统应提供专用的登录控制模块对登录用户进行身份标识和鉴别； 2.应提供系统管理员和普通用户的设置功能。	1.查看系统是否提供专用模块对用户进行身份标识和鉴别,如登录模块； 2.验证身份鉴别模块是否有效，身份鉴别是否正确。	1.系统提供登录模块对用户进行身份标识和鉴别； 2.系统身份鉴别模块有效，且身份鉴别结果正确。	技术类
4.3.1.2	应用安全/身份鉴别/系统与普通用户口令安全性	必测项	1.业务系统、管理系统应有口令长度及复杂度要求，至少8位，要求至少包含数字字母特殊字符； 2.业务系统、管理系统如提供密码初始化功能,应要求用户对初始化密码进行修改。	1.查看系统是否有口令长度、复杂度要求； 2.如系统提供密码初始化功能的,首次登录后是否要求用户修改密码。	1.系统对用户口令有复杂度要求，口令要求长度不少于8位,数字、字母、特殊字符混合； 2.系统提供密码初始化功能,用户第一次登录系统时系统要求用户修改初始密码。	技术类
4.3.1.3	应用安全/身份鉴别/登录访问安全策略	必测项	应对同一用户采用两种或两种以上组合的鉴别技术实现用户身份鉴别。	查看系统是否采用多种身份鉴别技术。	系统采用两种身份鉴别技术（用户/口令、数字证书、动态令牌等）。	技术类
4.3.1.4	应用安全/身份鉴别/非法访问警示和记录	必测项	1.业务系统、管理系统应提供登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施； 2.业务系统、管理系统应对登录成功、失败进行日志记录。	1.检查系统是否提供多次登录失败处理功能，如账户锁定、关闭浏览器、结束会话等； 2.检查登录错误提示是否过于详细（错误明确提示用户名错误、密码错误）； 3.是否对登录成功、失败进行日志记录，用户登录后系统是否提示上次登录情况（如登录时间、IP、登录成功/失败情况等）。	1.系统提供多次登录失败处理功能，口令多次错误后账户锁定/关闭浏览器/结束会话； 2.系统用户名/口令错误时，系统提示； 3.系统对用户登录成功、失败进行日志记录，用户登录后系统提示上次登录情况，提示内容包括上次登录时间、IP、登录成功/失败情况等。	技术类
4.3.1.5	应用安全/身份鉴别/客户端鉴别信息安全	必测项	客户端鉴别信息应不被窃取和冒用。	1.查看是否采用安全控件等措施保护用户输入的鉴别信息； 2.如果允许保存身份鉴别信息，是否采取加密措施； 3.通过截包工具进行截包测试，查看鉴别信息是否	1.支付密码等鉴别信息采用安全控件防止被窃取； 2.加密保存身份鉴别信息； 3.通过截包分析，用户口令以密文方式在网	技术类

编号	检测项	检测说明	技术要求细化	检测方法及步骤	预期结果及判定	类别
				加密传。	络中传输。	
4.3.1.6	应用安全/身份鉴别/口令有效期限制	必测项	业务系统、管理系统应限制口令的有效期限，并进行提醒。	查看系统是否有定期口令更改提示功能，对一段时间内未修改口令的账户进行提醒。	系统提供定期口令更改提示功能，对到期未修改口令的账户进行提醒。	技术类
4.3.1.7	应用安全/身份鉴别/限制认证会话时间	必测项	业务系统、管理系统应对客户端认证会话时间进行限制。	查看系统是否具有空闲会话超时功能，如对于 Web 应用系统，可检查是否对中间件相关配置进行了设置。	系统具有空闲会话超时功能，空闲会话超时时间合理。	技术类
4.3.1.8	应用安全/身份鉴别/身份标识唯一性	必测项	1.应提供用户身份标识唯一性和鉴别信息复杂度检查功能，保证应用系统中不存在重复用户身份标识，身份鉴别信息不易被冒用； 2.应启用身份鉴别、用户身份标识唯一性检查、用户身份鉴别信息复杂度检查以及登录失败处理功能，并根据安全策略配置相关参数。	1.检查系统是否提供用户身份标识唯一性检查功能，如通过新建用户等方式验证； 2.检查系统是否提供鉴别信息复杂度检查功能，如创建用户时，口令至少为8位，至少包括数字、字母及特殊字符； 3.检查系统是否启用了身份鉴别、用户身份标识唯一性检查、用户身份鉴别信息复杂度检查以及登录失败处理功能，并根据安全策略配置相关参数。	1.提供了用户身份标识唯一性和鉴别信息复杂度检查功能； 2.启用了身份鉴别、用户身份标识唯一性检查、用户身份鉴别信息复杂度检查以及登录失败处理功能，并根据安全策略配置相关参数。	技术类
4.3.1.9	应用安全/身份鉴别/及时清除鉴别信息	必测项	业务系统、管理系统会话结束后应及时清除客户端鉴别信息。	1.如该系统为 B/S 模式，可通过下列步骤进行测试： a、登录系统，并复制某功能模块URL； b、正常退出后，通过浏览器访问该URL，查看是否可以访问并继续进行操作； c、直接关闭浏览器，模拟非正常退出，再打开浏览器，通过浏览器访问该URL，查看是否可以访问并	1.系统为B/S模式，模拟正常/非正常退出系统，均无法通过访问URL的方式继续进行操作，会话结束后，系统及时清除了客户端鉴别信息； 2.系统为C/S模式，模拟正常/非正常退出系统，均未发现安装目录中存在鉴别信息。	技术类

编号	检测项	检测说明	技术要求细化	检测方法及步骤	预期结果及判定	类别
				继续进行操作； 2.如该系统为 C/S 模式，模拟正常/非正常退出系统，检查客户端程序的安装目录中的文件，是否有未删除的临时文件，临时文件中是否含有用户鉴别信息。		
4.3.2.1	应用安全/WEB 页面安全/登录防穷举	必测项	1.业务系统、管理系统应提供登录防穷举的措施，如图片验证码等； 2.登录失败后图形验证码应能自动更换； 3. 图形验证码应该具备一定的复杂度，防止能够轻易地被自动化工具识别。	1.检查是否提供图形验证码机制防范对用户名、口令穷举攻击； 2.输入错误的口令、错误的验证码后查看图形验证码是否会及时更新； 3.检查图形验证码是否采用了字体变形、黏连、背景干扰信息等技术防止被自动化工具识别。	1.系统使用图形验证码技术防范登录穷举； 2.图形验证码在登录失败后自动更换； 3.系统使用的图形验证码采用了字体变形、黏连、背景干扰信息等技术防止被自动化工具识别。	技术类
4.3.2.2	应用安全/WEB 页面安全/安全控件	必测项	1.业务系统登录、支付等模块应使用安全控件； 2.所使用的安全控件应能提供第三方检测机构的检测报告。	1.查看需要输入支付密码或 PIN 码的输入框是否使用安全控件进行保护； 2.查看安全控件是否能提供第三方检测机构的检测报告（只针对互联网业务）。	1.系统支付密码/PIN 码的输入框使用安全控件进行保护； 2.安全控件通过了机构的检查，并提供了第三方检测机构出具的检测报告。	技术类
4.3.2.3	应用安全/WEB 页面安全/使用数字证书	必测项	业务系统、管理系统应使用服务器数字证书。	查看系统是否使用有效的服务器数字证书进行网上身份标识和通信加密。	系统使用了数字证书。	技术类
4.3.2.4	应用安全/WEB 页面安全/独立的支付密码	必测项	1.业务系统应采用独立的支付密码进行支付； 2.应具有健全的密码找回机制。	1.查看系统是否使用独立的支付密码； 2.查看系统是否具有健全的密码找回机制。	1.系统在进行支付时需要输入支付密码才能进行支付，只知道登录密码无法进行支付； 2 具有健全的密码找回机制。	技术类
4.3.2.5	应用安全/WEB 页面安全/网站页面	必测项	业务系统、管理系统应无 SQL 注入、Path 注入和 LDAP 注入等漏洞。	通过 Web 扫描软件及手工测试，查看系统是否存在 SQL 注入、Path 注入和 LDAP 注入等漏洞。	通过 Web 扫描软件及手工测试，未发现系统存在 SQL 注入、Path 注入和 LDAP 注入等漏洞。	技术类

编号	检测项	检测说明	技术要求细化	检测方法及步骤	预期结果及判定	类别
	注入防范					
4.3.2.6	应用安全/WEB页面安全/网站页面跨站脚本攻击防范	必测项	业务系统、管理系统应无跨站脚本漏洞。	通过Web扫描软件及手工测试，查看系统是否存在跨站脚本漏洞。	通过Web扫描软件及手工测试，未发现系统存在跨站脚本漏洞。	技术类
4.3.2.7	应用安全/WEB页面安全/网站页面源代码暴露防范	必测项	业务系统、管理系统应无源代码暴露漏洞。	通过Web扫描软件及手工测试，查看系统是否存在源代码暴露漏洞。	通过Web扫描软件及手工测试，未发现系统存在源代码暴露漏洞。	技术类
4.3.2.8	应用安全/WEB页面安全/网站页面黑客挂马防范	必测项	应采取防范网站页面黑客挂马的机制和措施。	1.检查网站是否存在黑客挂马情况； 2.根据Web扫描软件及手工测试，是否发现网站有被黑客挂马的风险； 3.查看系统是否使用了网页防篡改系统。	1.通过检测，未发现系统存在黑客挂马情况； 2.通过检测，未发现网站存在被黑客挂马的风险； 3.系统使用了网页防篡改系统防止黑客挂马。	技术类
4.3.2.9	应用安全/WEB页面安全/网站页面防篡改措施	必测项	应部署防篡改措施或设备。	访谈系统管理员，询问是否部署了网站页面防篡改措施或设备。	部署了网站页面防篡改措施或设备。	技术类
4.3.2.10	应用安全/WEB页面安全/网站页面防钓鱼	必测项	1.网站页面应支持用户设置预留防伪信息； 2.防伪信息应能够正确显示。	1.访谈系统管理员，询问网站是否配置了用户预留防伪信息功能； 2.检查预留防伪信息功能，并尝试对其进行配置； 3.用户登录后能正确显示预留的防伪信息。	1.网站支持用户设置预留防伪信息； 2.防伪信息能够正确显示。	技术类
4.3.3.1	应用安全/访问控制/访问权限设置	必测项	1.应提供访问控制功能； 2.控制粒度应达到文件、数据库级； 3.访问控制策略的授权	1.应访谈应用系统管理员，询问应用系统是否提供访问控制措施，以及具体措施和访问控制策略有	1.系统提供了访问控制功能，控制粒度主体为用户级，客体为文件、数据库表级；	技术类

编号	检测项	检测说明	技术要求细化	检测方法及步骤	预期结果及判定	类别
			主体； 4.如设置默认用户，其权限有应被严格限制； 5.各用户权限划分应依据最小权限原则，相互之间应存在制约关系。	哪些，访问控制的粒度如何； 2.应检查应用系统，查看访问控制的粒度是否达到主体为用户级，客体为文件、数据库表级；查看其是否有由授权用户设置其它用户访问系统功能和用户数据的权限的功能，是否限制默认用户的访问权限； 3.应检查应用系统，查看系统是否授予不同账户为完成各自承担任务所需的最小权限，特权用户的权限是否分离，权限之间是否相互制约； 4.应测试应用系统，可通过以不同权限的用户登录系统，查看其拥有的权限是否与系统赋予的权限一致，验证应用系统访问控制功能是否有效； 5.应测试应用系统，可通过以默认用户登录系统，并进行一些合法和非法操作，验证系统是否严格限制了默认账户的访问权限； 6.在不登录的情况下，或通过低权限用户登录后通过 URL 直接跳转到高权限用户的功能模块，验证是否得到限制。	2.访问控制措施由授权主体设置，并限制了默认用户的访问权限； 3.各用户按照最小权限原则进行权限划分，并在相互之间形成制约关系。	
4.3.3.2	应用安全/访问控制/自主访问控制范围	必测项	访问控制的覆盖范围应包括与资源访问相关的主体、客体及它们之间的操作。	应检查应用系统，查看其访问控制的覆盖范围是否包括与信息安全直接相关的主体、客体及它们之间的操作，如对客体的增、删、改、查等操作。	访问控制的覆盖范围包括了与资源访问相关的主体、客体及它们之间的操作。	技术类

编号	检测项	检测说明	技术要求细化	检测方法及步骤	预期结果及判定	类别
4.3.3.3	应用安全/访问控制/业务操作日志	必测项	应提供业务操作审计功能。	1.应访谈安全审计员，系统是否具备对所有业务操作的审计功能； 2.应检查应用系统，查看系统是否记录了所有业务操作日志； 3.应测试应用系统，可通过业务操作产生相关审计日志，并查看是否能够正确记录。	系统具有对所有业务操作进行日志记录的功能。	技术类
4.3.3.4	应用安全/访问控制/关键数据操作控制	必测项	应严格控制用户对关键数据的操作。关键数据如：敏感数据、重要业务数据、系统管理数据等。	1.访谈系统管理员，系统内关键数据有哪些，是否配置了针对关键数据的访问控制策略； 2.应渗透测试应用系统，进行试图绕过访问控制的操作，验证应用系统的访问控制功能是否不存在明显的弱点。	严格控制了用户对关键数据的操作，无法绕过访问控制对其进行操作。	技术类
4.3.3.5	应用安全/访问控制/异常中断防护	必测项	1.应提供用户访问中断的保护措施； 2.应保证数据不丢失。	1.应访谈系统管理员，用户访问异常中断的防护手段有哪些； 2.应测试应用系统，在用户访问异常中断后，查看用户数据是否丢失。	用户访问异常中断后，能够保证用户数据不丢失。	技术类
4.3.3.6	应用安全/访问控制/数据库安全配置	必测项	1.应具备数据库安全配置手册； 2.对数据库进行安全配置。	1.应查看是否编制了数据库安全配置手册； 2.应依据安全手册检查数据库是否按照手册进行了相关安全配置。	1.具备数据库安全配置手册； 2.按照手册进行了相关安全配置。	技术类
4.3.4.1	应用安全/安全审计/日志信息	必测项	1.应具备安全审计功能； 2.审计记录的内容至少应包括事件的日期、时间、发起者信息、类型、描述和结果等。	1.应访谈安全审计员，询问应用系统是否有安全审计功能； 2.应检查应用系统，查看其审计记录信息是否包括事件发生的日期与时间、触发事件的主体与客体、事件的类型、事件成功或失败、身份鉴别事件中请求的来源、事件的结果等	1.系统具备安全审计功能； 2.审计要素包括了事件的日期、时间、发起者信息、类型、描述和结果等。	技术类

编号	检测项	检测说明	技术要求细化	检测方法及步骤	预期结果及判定	类别
				内容； 3.应测试应用系统，在应用系统上试图产生一些重要的安全相关事件（如用户登录、修改用户权限等），查看应用系统是否对其进行了审计；如果进行了审计则查看审计记录内容是否包含事件的日期、时间、发起者信息、类型、描述和结果等。		
4.3.4.2	应用安全/安全审计/日志权限和保护	必测项	1.应保证无法单独中断审计进程； 2.无法删除、修改或覆盖审计记录。	1.应访谈安全审计员，对审计日志的保护措施有哪些； 2.应测试应用系统，可通过非审计员的其他账户试图中断审计进程，验证审计进程是否受到保护； 3.应测试应用系统，试图非授权删除、修改或覆盖审计记录，验证安全审计的保护情况是否无法非授权删除、修改或覆盖审计记录。	1.无法单独中断审计进程； 2.提供了审计记录保护措施，无法删除、修改或覆盖审计记录； 3.审计数据进行了备份。	技术类
4.3.4.3	应用安全/安全审计/系统信息查询与分析	必测项	应提供对审计记录数据进行统计、查询、分析及生成审计报表的功能。	检查应用系统，查看其是否为授权用户浏览和分析审计数据提供专门的审计分析功能，并能根据需要生成审计报表。	系统提供了审计记录数据进行统计、查询、分析及生成审计报表的功能。	技术类
4.3.4.4	应用安全/安全审计/对象操作审计	必测项	应提供覆盖到每个用户的安全审计功能，对应用系统重要安全事件进行审计。	1.检查应用系统，查看其当前审计范围是否覆盖到每个用户； 2.检查应用系统，查看其审计策略是否覆盖系统内重要的安全相关事件，例如，用户标识与鉴别、访问控制的所有操作记录、重要用户行为、系统资源的异常使用、重要系统命令的使用等；	1.审计范围覆盖到每个用户； 2.审计策略覆盖系统内的重要安全事件，包括用户标识与鉴别、访问控制的所有操作记录、重要用户行为、系统资源的异常使用、重要系统命令的使用等。	技术类

编号	检测项	检测说明	技术要求细化	检测方法及步骤	预期结果及判定	类别
				3.测试应用系统，在应用系统上试图产生一些重要的安全相关事件（如用户登录、修改用户权限等），查看应用系统是否对其进行了审计，验证应用系统安全审计的覆盖情况是否覆盖到每个用户。		
4.3.4.5	应用安全/安全审计/审计工具	必测项	1.系统应该提供安全审计工具； 2.审计工具应该提供日志规划功能、可以进行分析形成审计报告； 3.系统审计工具提供自我数据保护功能。	1.访谈系统管理员，询问是否配有系统审计工具； 2.检查系统安全审计工具状态和配置； 3.操作审计工具进行定制导出操作。	1.系统应该具备安全审计工具； 2.审计服务应该处于开启状态，且能够按要求定制导出审计报告报表； 3.应定义审计跟踪极限的阈值，当存储空间接近极限时，能采取必要的措施，当存储空间被耗尽时，终止可审计事件的发生。	技术类
4.3.4.6	应用安全/安全审计/事件报警	必测项	应具有交易事件报警功能。	1.应访谈安全审计员，系统是否具备交易事件报警功能，报警形式有哪些； 2.应测试应用系统，产生报警事件，验证报警策略是否有效。	能够对交易事件进行报警。	技术类
4.3.5.1	应用安全/剩余信息保护/过期信息、文档处理	必测项	应对无用的过期信息、文档进行完整删除。	应测试应用系统，用某用户登录系统并进行操作后，在该用户退出后用另一用户登录，试图操作（读取、修改或删除等）其他用户产生的文件、目录和数据库记录等资源，查看操作是否成功，验证系统提供的剩余信息保护功能是否正确（确保系统内的文件、目录和数据库记录等资源所在的存储空间，被释放或重新分配给其他用户前得到完全清除）。	1.能够对无用、过期信息和文档进行完成删除； 2.采取了技术手段对剩余信息进行保护。	技术类

编号	检测项	检测说明	技术要求细化	检测方法及步骤	预期结果及判定	类别
4.3.6.1	应用安全/资源控制/连接控制	必测项	1.应能够根据业务需求，对系统的最大并发会话连接数进行限制； 2.应能够对一个时间段内可能的并发会话连接数进行限制。	1.应访谈应用系统管理员，询问应用系统是否有资源控制的措施，具体措施有哪些； 2.应检查应用系统，查看系统是否有最大并发会话连接数的限制。	1.实现了最大并发会话数限制； 2.能够对一段时间内的可能并发会话数进行了限制。	技术类
4.3.6.2	应用安全/资源控制/会话控制	必测项	1.当应用系统的通信双方中的一方在一段时间内未作任何响应，另一方应能够自动结束会话； 2.应能够对单个账户的多重并发会话进行限制。	1.检查应用系统，查看是否限制单个账户的多重并发会话； 2.测试应用系统，可通过对系统进行超过规定的单个账户的多重并发会话数进行连接，验证系统是否能够正确地限制单个账户的多重并发会话数； 3.测试重要应用系统，当应用系统的通信双方中的一方在一段时间内未作任何响应，查看另一方是否能够自动结束会话。	1.会话超时会自动结束会话； 2.限制了单个用户的多重并发会话。	技术类
4.3.6.3	应用安全/资源控制/进程资源分配	必测项	1.应能够对一个访问用户或一个请求进程占用的资源分配最大限额和最小限额； 2.应提供服务优先级设定功能，并在安装后根据安全策略设定访问用户或请求进程的优先级，根据优先级分配系统资源。	1.应检查应用系统，查看是否能根据安全策略设定主体的服务优先级，根据优先级分配系统资源； 2.应检查应用系统，查看是否对一个访问账户或一个请求进程占用的资源分配最大限额和最小限额。	1.能够对一个访问用户或一个请求进程占用的资源分配最大限额和最小限额； 2.提供服务优先级设定功能，并在安装后根据安全策略设定访问用户或请求进程的优先级，根据优先级分配系统资源。	技术类
4.3.6.4	应用安全/资源控制/资源检测预警	必测项	应能够对系统服务水平降低到预先规定的最小值进行检查和报警。	应检查应用系统，查看是否有服务水平最小值的设定，当系统的服务水平降低到预先设定的最小值时，系统是否能够报警。	1.对服务水平进行了配置； 2.能够对降低到预设最小值时进行检查和报警。	技术类
4.3.7.1	应用安全/应用容错/数据有效性校	必测项	应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的数据格式或长度符	1.应访谈应用系统管理员，询问应用系统是否具有保证软件容错能力的措施，具体措施有哪些；	对通过人机接口输入或通过通信接口输入的数据格式或长度进行了严格限制。	技术类

编号	检测项	检测说明	技术要求细化	检测方法及步骤	预期结果及判定	类别
	验		合系统设定要求。	2.应检查应用系统，查看应用系统是否对人机接口输入或通信接口输入的数据进行有效性检验，是否存在SQL注入、XSS跨站脚本漏洞、框架注入钓鱼和远程命令执行等； 3.应测试应用系统，可通过对人机接口输入的不同长度或格式的数据，查看系统的反应，验证系统人机接口有效性检验功能是否正确。		
4.3.7.2	应用安全/应用容错/容错机制	必测项	应提供自动保护功能，当故障发生时自动保护当前所有状态，保证系统能够进行恢复。	检查应用系统是否具备冗余机制，如双机热备、集群等。	具备冗余机制，如双机热备、集群等。	技术类
4.3.7.3	应用安全/应用容错/故障机制	必测项	发生故障后，系统应能够及时恢复。	1.访谈管理员，了解业务系统故障恢复机制和时间要求； 2.查看故障恢复日志或记录； 3.检查保障系统及时恢复的措施”。	1.系统故障恢复功能正常，恢复时间符合要求； 2.提供恢复日志或记录； 3.系统具有保障发生故障后及时恢复的措施。	技术类
4.3.7.4	应用安全/应用容错/回退机制	必测项	应具备回退机制，当故障发生时能够成功回退。	1.应访谈系统管理员，系统是否具备回退功能； 2.查看历史回退记录。	1.提供了回退功能； 2.能够及时回退到故障发生前的状态。	技术类
4.3.8.1	应用安全/报文完整性/通信报文有效性	必测项	通信报文应采用密码技术保证通讯过程中交易数据的完整性。	1.应访谈相关人员，询问应用系统是否具有在数据传输过程中保护其完整性的措施，具体措施是什么； 2.应检查设计或验收文档，查看其是否有关于保护通信完整性的说明，如果有则查看其是否有用密码技术来保证通信过程中数据的完整性的描述； 3.应测试应用系统，可通	采用了密码技术保证通信过程中数据的完整性。	技术类

编号	检测项	检测说明	技术要求细化	检测方法及步骤	预期结果及判定	类别
				过获取通信双方的数据包，查看通信报文是否含有加密的验证码。		
4.3.9.1	应用安全/报文保密性/报文或会话加密	必测项	在通讯时采用安全通道或对报文中敏感信息进行加密。	1.应访谈相关人员，询问应用系统数据在通信过程中是否采取保密措施，具体措施有哪些； 2.应测试应用系统，通过查看通信双方数据包的内容，查看系统在通信过程中，安全通道或对报文敏感字段进行加密的功能是否有效。	在通讯时采用了安全通道或对报文中敏感信息进行加密。	技术类
4.3.10.1	应用安全/抗抵赖/原发和接收证据	必测项	1.应具有在请求的情况下为数据原发者或接收者提供数据原发证据的功能； 2.应具有在请求的情况下为数据原发者或接收者提供数据接收证据的功能。	1.应访谈安全员，询问系统是否具有抗抵赖的措施，具体措施有哪些； 2.查看系统是否提供在请求的情况下为数据原发者和接收者提供数据原发证据的功能；是否提供在请求的情况下为数据原发者和接收者提供数据接收证据的功能。	采用了技术措施保证数据原发者或接收者提供数据原发和数据接收证据的功能。	技术类
4.3.11.1	应用安全/编码安全/源代码审查	必测项	1.应对源代码进行安全性审查； 2.提供源代码审查证据。	1.应访谈安全员，是否针对源代码进行了安全性审查，采取了何种工具进行审查； 2.应检查源代码安全性审查报告； 3.应查看相关审查文档和证据，检查是否通过自动化工具实现了源代码安全审查。	1.实现了对源代码的安全性审查，并具有安全性审查报告； 2.采用恰当方法对源代码安全进行审查。	技术类
4.3.11.2	应用安全/编码安全/插件安全性审查	必测项	1.插件安全性审查方式； 2.提供审查证据。	1.应访谈安全员，是否针对插件进行了安全性审查； 2.应检查插件安全性审查报告。	实现了对插件的安全性审查，并具有安全性审查报告。	技术类
4.3.11.3	应用安全/编码安	必测项	1.应按照编码规范进行编码；	1.应访谈安全员，是否编制了编码安全规范；	具有编码规范，并严格按照编码规范执行。	技术

编号	检测项	检测说明	技术要求细化	检测方法及步骤	预期结果及判定	类别
	全/编码规范约束		2.应具有编码规范约束制度。	2.应查看相关记录和文档，验证是否按照规范执行。		类
4.3.11.4	应用安全/编码安全/源代码管理	必测项	1.应具备源代码管理制度，在每次源代码变更时，需填写变更备注信息； 2.应具备源代码管理记录。	1.应访谈安全员，是否编制了源代码管理制度； 2.应检查是否按照制度执行，并查看是否产生相关管理记录。	1.具有源代码管理制度； 2.具有源代码管理记录。	技术类
4.3.11.5	应用安全/编码安全/版本管理	必测项	应具有代码版本管理制度。	1.应访谈安全员，是否具有代码版本管理制度； 2.应检查代码版本管理的实现方式。	具有代码版本管理制度。	技术类
4.3.12.1	应用安全/电子认证应用/第三方电子认证机构证书	必测项	1.在对外业务(非内部业务)处理过程中，应使用经过认证的第三方电子认证证书； 2.在内部业务(仅涉及本机构内人员或设备的业务)处理过程中，可以使用自建证书(非第三方电子认证证书)； 3.在条件允许的情况下，建议对所有业务使用经过认证的第三方电子认证证书。	1.应访谈安全员，系统内是否使用了第三方电子认证证书，使用范围包括哪些业务； 2.应检查对外业务处理过程，是否使用了第三方电子认证证书，该证书是否经过认证； 3.应检查内部业务处理过程，是否使用了电子认证证书，证书来源是哪； 4.应检查其他业务处理过程，是否使用了第三方电子认证证书，证书来源是哪。	1.在对外业务（非内部业务）处理过程中，使用了经过认证的第三方电子认证证书； 2.在内部业务（仅涉及本机构内人员或设备的业务）处理过程中，使用了自建证书（非第三方电子认证证书）或第三方电子认证证书。	技术类
4.3.12.2	应用安全/电子认证应用/关键业务电子认证技术应用	必测项	1.关键业务应使用电子认证技术； 2.在条件允许的情况下，建议在所有业务均使用经过认证的第三方电子认证技术。	1.应访谈安全员，系统内关键业务有哪些，这些业务是否使用了电子认证技术； 2.应检查应用系统，查看关键业务使用电子认证技术的情况。	关键业务使用了电子认证技术。	技术类
4.3.12.3	应用安全/电子认证应用/电子签名有效性	必测项	1.对外业务和对内业务的情况； 2.对外业务是否采用第三方电子签名； 3.对内业务是否采用第	1.访谈应用系统管理员，了解目前支付系统对外的业务系统有哪些和对内的系统有哪些； 2.检查对外业务系统的设	1.应用系统管理员说明能够说明目前系统队伍的业务有哪些和对内业务有哪些； 2.在对外业务系统的	技术类

编号	检测项	检测说明	技术要求细化	检测方法及步骤	预期结果及判定	类别
			三方电子签名或者采用自建签名系统； 4.签名体系应有效运行。	计文档，查看是否采用第三方电子签名，并访谈应用系统管理员，查看与第三方电子签名提供商所签订的合同； 3.查看对内业务系统的设计文档，查看是否采用第三方电子签名或者自建的电子签名，如果采用第三方电子签名，查看与第三方电子签名提供商所签订的合同； 4.测试对外业务系统和对内业务系统的电子签名是否符合设计文档。	设计文档中明确写出了采用第三方的电子证书，并与第三方电子证书提供商的合同在有效期之内； 3.在对内业务系统的设计文档中写出了需要电子证书，如果采用第三方电子证书，与第三方电子证书提供商的合同在有效期之内； 4.根据设计文档，验证对外的业务系统是否有效采用了第三方证书，如果不采用第三方证书是否能够有效运行。对内的业务系统是否有效采用电子证书。	
4.3.12.4	应用安全/电子认证应用/服务器证书私钥保护	必测项	应对所持有的服务器证书私钥进行有效保护。	1.访谈应用系统管理员，了解支付系统有采用什么样的证书密钥系统，其私钥保存在哪些服务器上； 2.查看对私钥有哪些保护措施。	1.应用系统管理能够明确说出哪些服务器存放了证书私钥； 2.明确列出了对私钥的保护措施。	技术类
4.3.13.1	应用安全要求审查/终端安全/终端设备安全性要求	必测项	确认机顶盒和相关IC卡或遥控器等是否通过第三方中立测试机构安全检测。	1.访谈相关人员，询问机顶盒和相关IC卡或遥控器的生产厂家、型号等； 2.查看实际设备进行验证； 3.查看此类设备的第三方中立测试机构的安全检测报告。	此类设备应通过第三方中立测试机构的安全检测。	技术类

8.4 数据安全性测试

对支付业务设施的数据安全防护进行检测，主要考察数据的传输、存储、备份与恢复安全性。检测内容见表7。

表7　数据安全性测试

编号	检测项	检测说明	技术要求细化	检测方法及步骤	预期结果及判定	类别
4.4.1.1	数据安全/数据保护/客户身份信息保护	必测项	1.应具备数据保护的相关管理制度； 2.在管理制度中应对客户身份基本信息的定义； 3.应妥善对客户身份基本信息进行保存，并明确保存时间。	1.访谈相关管理员，是否制定了对数据保护的相关管理制度； 2.在所提供的数据保护的相关管理制度中，是否包括了对客户基本信息的定义，保存方式、保存时间等等； 3.在系统中验证通过管理制度中所定义的客户身份基本信息的保存方式和保存时间是否实现，并查看保存方式及保存时间，是否按照管理制度执行。	1.机构指定了相关数据保护的管理制度； 2.在数据保护的相关管理制度中对客户身份基本信息、保存方式和保存时间进行了定义； 3.在系统中实现了对客户身份基本信息的保护，时间和保存方式合理。	管理类
4.4.1.2	数据安全/数据保护/支付业务信息保护	必测项	1.应具备数据保护的相关管理制度； 2.在管理制度中应对支付业务信息的定义； 3.应妥善对支付业务信息进行保存，并明确保存时间。	1.访谈相关管理员，是否制定了对数据保护的相关管理制度； 2.在所提供的数据保护的相关管理制度中，是否包括了对支付业务信息的定义，保存方式、保存时间等等； 3.在系统中验证通过管理制度中所定义的支付业务信息的保存方式和保存时间是否实现，并查看保存方式及保存时间，是否按照管理制度执行。	1.机构指定了相关数据保护的管理制度； 2.在数据保护的相关管理制度中对支付业务信息、保存方式和保存时间进行了定义； 3.在系统中实现了对支付业务信息的保护，时间和保存方式合理。	管理类
4.4.1.3	数据安全/数据保护/会计档案信息保护	必测项	1.应制定了会计档案的相关管理制度； 2.对会计档案的保管期限应符合《会计档案管理办法》（财会字〔1998〕32号文印发）。	1.是否制定了会计档案的相关管理制度； 2.会计档案的保管期限是否符合《会计档案管理办法》（财会字〔1998〕32号文印发）。	1.制定了会计档案的相关管理制度； 2.对会计档案的保管期限符合《会计档案管理办法》（财会字〔1998〕32号文印发）。	管理类
4.4.2.1	数据安全/数据完整性/重要数据更改机制	必测项	1.应具有重要数据的更改管理制度； 2.应具有重要数据的更改流程； 3.应具有重要数据的更改记录。	1.询问系统管理对重要数据的更改是否有相关管理制度，在管理制度重视定义了相关的更改流程； 2.检测部分重要数据的更改记录。	1.制定了重要数据的更改管理制度； 2.具有重要数据的更改记录。	管理类
4.4.2.2	数据安全/数据完整性/数据备份	必测项	1.应具备数据备份相关制度； 2.应对数据备份进	1.询问数据管理员对数据备份记录是否有相关模板； 2.检查所有数据备份类型的备	1.在管理制度中能够提供数据备份的相关模板；	管理类

编号	检测项	检测说明	技术要求细化	检测方法及步骤	预期结果及判定	类别
	记录		行了记录。	份记录。	2.所有数据的备份都有相关记录。	
4.4.2.3	数据安全/数据完整性/保障传输过程中的数据完整性	必测项	1.应在数据传输过程中使用的专用通信协议或安全通信协议服务保证数据传输的完整性； 2.在数据传输中断或者接收到的数据经过篡改或者数据受损完整性验证失败，应采取数据恢复措施。	1.询问系统开发人员数据传输过程中使用何种专用通信协议或安全通信协议服务保证数据传输的完整性； 2.询问系统开发人员数据传输完成，通过何种手段验证接收到的数据的完整性； 3.询问数据传输中断或者接收的数据受到篡改，完整性校验失败时采用何种机制进行数据恢复； 4.通过软件模拟同类型/不同类型数据通过并发方式传输，验证接收到的各条数据完整。	1.系统数据传输过程中的协议或服务保证数据传输的完整性； 2.系统接收的数据，验证接收到的数据的完整性； 3.数据传输中断或者由于数据传输过程中遭到篡改导致数据受损时，进行数据恢复； 4.同类型/不同类型数据通过并发方式传输，接收到的各条数据均完整。	技术类
4.4.2.4	数据安全/数据完整性/备份数据定期恢复	必测项	1.应对系统数据备份方式、数据保存的格式进行要求； 2.应定期随机抽取备份数据进行解压、还原，检查其内容有效性。	1.询问系统开发人员数据备份采用何种方式，备份文件采用何种格式保存； 2.询问系统管理人员数据备份的周期、是否定期验证备份数据的有效性； 3.查看相关记录和文档。	1.按要求对系统进行记录和保存； 2.系统数据定期进行备份，并对备份数据进行有效性验证。	技术类
4.4.3.1	数据安全/交易数据以及客户数据的安全性/数据物理存储安全	必测项	1.应具备高可用性的数据物理存储环境； 2.系统的通信线路、网络设备和数据处理设备，提供业务应用都采用冗余设计并且能够实时无缝切换。	1.询问系统管理员系统备份策略，如是否每天进行完备份，备份是否介质场外存放； 2.系统的通信线路、网络、服务器、存储等设备以及系统应用程序是否采用冗余备份方式，能否实时无缝切换； 3.系统是否具有实时备份功能，如利用通信网络将数据实时备份至实时中心。	满足高可用性的最低指标要求。	管理类
4.4.3.2	数据安全/交易数据以及客户数据的安全性/客户身份认证信息存储安全	必测项	1.应不允许保存非必须的客户身份认证信息（如银行卡交易密码、指纹、银行卡磁道信息、CVN、CVN2等）； 2. 应对客户的其他	1.查看开发文档中的数据词典，验证是否在数据库中是否存在客户身份认证信息； 2.查看开发文档中的数据流部分，在对客户身份认证的过程中是否有保存信息； 3.按照开发文档中的在系统中	1.没有保存客户身份认证信息； 2.在对客户身份认证的过程中不保存非必须的客户身份认证信息； 3.通过抓取系统数据	技术类

编号	检测项	检测说明	技术要求细化	检测方法及步骤	预期结果及判定	类别
			敏感信息，如卡号、户名、开户手机、贷记卡有效期、电子邮箱等信息采取保护措施，防止未经授权擅自对个人信息进行查看、篡改、泄露和破坏。宜采用加密存储、部分屏蔽显示等技术。	对客户身份认证信息进行验证，查看系统是否对保存了客户身份认证信息。	分析系统不保存非必须的客户身份认证信息。	
4.4.3.3	数据安全/交易数据以及客户数据的安全性/终端信息采集设备硬加密措施或其它防伪手段	必测项	1.终端信息采集设备应采取硬加密措施； 2.如果使用终端信息采集设备则应采取硬加密措施，否则要使用其它手段达到防伪目的。	1.咨询系统开发人员和查看开发文档，是否采用了终端信息采集设备，如果采用了终端信息采集设备，查看系统与终端之间的数据交换和通讯的协议是否采取了加密措施。在系统中是否有对数据的解密模块； 2.如果没有采用加密措施，在开发文档中是否有采取其他的手段进行防伪； 3.通过数据包的分析，系统与终端采集设备之间的数据交换和通讯采取了加密措施。	终端信息采集设备采取了硬加密措施，如果没有采取加密措施，其防伪手段有效。	技术类
4.4.3.4	数据安全/交易数据以及客户数据的安全性/同一安全级别和可信赖的系统之间信息传输	必测项	应保证信息只能在同一安全保护级别、可信赖的系统之间传输。	1.询问系统开发方，系统是否具有安全级别的划分； 2.验证系统是否禁止数据从高安全保护级别向低安全保护级别传输； 3.验证相同安全保护级别之间数据是否可以互相传输。	1.系统具有安全级别的划分； 2.系统禁止数据从高安全保护级别向低安全保护级别传输； 3.相同安全保护级别之间数据可以互相传输。	技术类
4.4.3.5	数据安全/交易数据以及客户数据的安全性/加密传输	必测项	1.应能够识别系统管理数据、鉴别信息和重要业务数据； 2.应通过加密通讯协议对系统管理数据、鉴别信息和重要业务数据进行传输。	1.咨询系统开发人员和查看开发文档，目前系统有哪些系统管理数据、鉴别信息和重要业务数据。其系统对系统管理数据、鉴别信息和重要业务数据的分类是否全面； 2.访谈采用何种加密通讯协议对系统管理数据、鉴别信息和重要业务数据进行加密；	1.系统管理数据、鉴别信息和重要业务数据的分类全面； 2.采用了加密通讯协议对系统管理数据、鉴别信息和重要业务数据的加密。	技术类

编号	检测项	检测说明	技术要求细化	检测方法及步骤	预期结果及判定	类别
				3.通过抓包分析，在支付系统中验证对系统管理数据、鉴别信息和重要业务数据的加密是否有效。		
4.4.3.6	数据安全/交易数据以及客户数据的安全性/加密存储	必测项	1.应能够识别系统管理数据、鉴别信息和重要业务数据； 2.应对系统管理数据、鉴别信息和重要业务数据进行加密存储。	1.访谈系统开发人员和查看开发文档，目前系统有哪些系统管理数据、鉴别信息和重要业务数据； 2.访谈采用何种加密算法对系统管理数据、鉴别信息和重要业务数据进行存储； 3.通过对数据存储分析，在支付系统中验证对系统管理数据、鉴别信息和重要业务数据的加密是否有效。	1.系统管理数据、鉴别信息和重要业务数据的分类全面； 2.对系统管理数据、鉴别信息和重要业务数据的加密存储。	技术类
4.4.3.7	数据安全/交易数据以及客户数据的安全性/数据访问控制	必测项	1.应具备对重要数据访问控制的管理制度； 2.应具备重要数据访问控制的记录。	1.询问系统管理员是否存在对重要数据访问控制的管理制度； 2.查看重要数据访问控制的访问记录； 3.询问系统管理员对重要数据采取了哪些技术访问控制手段，并验证是否有效。	1.有重要数据的访问控制管理措施和相关记录； 2.采取了较全面的技术手段对重要数据进行控制。	技术类
4.4.3.8	数据安全/交易数据以及客户数据的安全性/在线的存储备份	必测项	1.支付系统应有实时在线的存储备份设备； 2.实时在线的存储备份设备应能够正常运行。	1.实地考察系统中是否有实时在线的存储备份设备； 2.由系统管理现场操作验证实时在线存储备份系统是否能够正常运行。	实时在线备份系统正常运行。	技术类
4.4.3.9	数据安全/交易数据以及客户数据的安全性/数据备份机制	必测项	1. 应制定数据的备份和恢复策略； 2.应采用合理备份数据的备份方式（如增量备份或全备份等）、备份频度（如每日或每周等）； 3.应采用合理的数据备份方式。	1.询问数据库管理员或者系统管理员，是否制定了数据备份的相关管理制度； 2.在数据备份管理制度中是否有对数据备份的对象、备份方式、备份频率、备份所采用的介质、存放地点、命名规则、保存周期、备份流程以及相关记录文档进行说明； 3.现场检查是否按照管理制度所规定的流程和内容进行备份。	1. 制定了相关的备份管理制度，而且内容全面； 2.备份制度执行情况良好。	管理类

编号	检测项	检测说明	技术要求细化	检测方法及步骤	预期结果及判定	类别
4.4.3.10	数据安全/交易数据以及客户数据的安全性/本地备份	必测项	1.应提供本地数据备份； 2.应具有同机房数据备份设施。	1.在机房内现场查看是否有本地备份的设备； 2.由现场管理人员操作验证设备是否正常运行。	在机房内提供了本地备份设备并能够有效运行。	技术类
4.4.3.11	数据安全/交易数据以及客户数据的安全性/异地备份	必测项	1.应提供异地备份的功能或者设备； 2.应具备异地备份的网络或者线路； 3.应能够成功进行异地备份。	1.现场查看是否有异地备份机房和备份设备，测试其备份线路和网络是否畅通； 2.按照备份的管理制度检查最近的异地备份是否符合要求。	1.提供了异地备份场地和设备； 2.异地备份设备能够有效的进行备份。	技术类
4.4.3.12	数据安全/交易数据以及客户数据的安全性/备份数据的恢复	必测项	1.应制定备份数据恢复操作手册； 2.备份数据恢复操作手册应对恢复的流程、内容、记录、对象等进行规定； 3.本地备份数据和异地备份数据应能够正常恢复。	1.询问数据备份管理员，是否制定了备份数据恢复操作手册，备份数据恢复操作手册是否定义了恢复的流程，对象、记录、内容等等； 2.现场查看本地备份数据和异地备份数据，按照备份数据恢复操作手册是否能够正常恢复； 3.现场查看备份数据恢复的操作记录是否完备。	1.制定了备份数据恢复操作手册，并且内容全面，符合机构的要求； 2.恢复操作记录完备； 3.恢复设备工作正常。	技术类
4.4.3.13	数据安全/交易数据以及客户数据的安全性/数据销毁制度和记录	必测项	应制定数据销毁制度应包括数据销毁范围、介质销毁方法、记录模板、监督机制等。	1.询问数据管理人员，是否制定了数据销毁管理制度； 2.数据销毁管理制度内容是否全面； 3.现场检查最近数据销毁记录。	数据销毁管理制度内容全面。并有相关的记录。	技术类
4.4.3.14	数据安全/交易数据以及客户数据的安全性/关键链路冗余设计	必测项	1.应保证通讯线路采用冗余； 2.应保证主要网络设备采用冗余； 3.应保证主要数据处理服务器采用冗余。	1.询问网络管理员，通讯线路、网络设备、主要数据处理服务器是否采用冗余； 2.核实网络拓扑图，对通讯线路、主要网络设备、主要数据处理服务器在网络拓扑图上有冗余体现； 3.现场机房核实通讯线路、网络设备、主要数据处理服务器采用了冗余。	通讯线路、主要网络设备和数据处理服务器采用硬件冗余。	技术类

8.5 运维安全性测试

对支付业务设施的运维安全进行检测，主要考察运维安全管理制度及运维安全执行情况。检测内容见表8。

表8　运维安全性测试

编号	检测项	检测说明	技术要求细化	检测方法及步骤	预期结果及判定	类别
4.5.1.1	运维安全/环境管理/机房基础设施定期维护	必测项	应指定专门的部门或人员定期对机房供配电、空调、温湿度控制等设施进行维护管理。	1.询问机房管理员，是否制定了机房的相关管理制度； 2.现场在机房考察是否有机房值班人员值守； 3.机房管理人员是否对机房内的电源供应设备、环境监控设备等有维护记录。	1.机房有专门的值班人员进行值守； 2.有对机房内的电源供应设备和环境监控设备的维护记录。	管理类
4.5.1.2	运维安全/环境管理/机房的出入管理制度化和文档化	必测项	应指定部门负责机房安全，并配备机房安全管理人员，对机房的出入、服务器的开机或关机等工作进行管理。	1.询问机房管理员，是否制定了机房的相关管理制度； 2.机房的出入是否有申请和审批流程，是否有相关的记录； 3.对出入机房的设备是否有记录； 4.对机房内的设备操作是否有监控或者记录。	1.制定了机房出入的申请和审批流程，并有相关记录； 2.对出入机房的设备有相关记录； 3.在机房内的设备操作有相关记录。	管理类
4.5.1.3	运维安全/环境管理/办公环境的保密性措施	必测项	1.应规范人员转岗、离岗过程； 2.外部人员访问受控区域前先应提出书面申请，批准后由专人全程陪同或监督，并登记备案； 3.应加强对办公环境的保密性管理，规范办公环境人员行为。工作人员调离办公室应立即交还该办公室钥匙、不在办公区接待来访人员、工作人员离开座位应确保终端计算机退出登录状态和桌面上没有包含敏感信息的纸档文件等。	1.是否制定了人员辞职和转岗的相关管理制度； 2.外部人员访问受控区域的制定了审批流程，是否有专人陪同； 3.是否制定了工作人员的工作规范文档。	1.制定了人员辞职和转岗的相关管理制度； 2.外部人员访问受控区域有审批流程，并有专门人陪同； 3.制定了工作人员的工作规范文档。	管理类
4.5.1.4	运维安全/环境管理/	必测项	1.人员进入机房应填写登记表；	1.询问机房管理人员，是否制定了机房管理制度；	1.制定了机房的管理制度；	管理

编号	检测项	检测说明	技术要求细化	检测方法及步骤	预期结果及判定	类别
	机房安全管理制度		2.进入机房的来访人员应经过申请和审批流程，并限制和监控其活动范围。	2.核查对机房内的设备带进、带出和设备的操作等有相关管理规定； 3.现场核查对机房内的设备有视频监控或者红外监控等的监控手段。	2.对机房的物理访问、设备的带进和带出有相关的管理制度和技术手段。	类
4.5.1.5	运维安全/环境管理/机房进出登记表	必测项	1.应具有人员进出入登记表； 2.应具有设备进出入登记表。	现场核查人员进出入登记表和设备进出入登记表是否记录完整。	对人员的进出和设备的进出都进行详细的记录。	管理类
4.5.2.1	运维安全/介质管理/介质的存放环境保护措施	必测项	1.应制定介质管理制度，规范对各类介质进行控制和保护以及介质的存放环境； 2.应由专人对介质进行管理； 3.应对介质的使用、维护进行登记。	1.询问管理人员是否制定了介质管理制度，规范对各类介质进行控制和保护以及介质的存放环境； 2.询问管理人员是否由专人对介质进行管理； 3.是否对介质的使用、维护进行登记。	1.制定了介质管理制度，规范对各类介质进行控制和保护以及介质的存放环境； 2.由专人对介质进行管理； 3.对介质的使用、维护进行登记。	管理类
4.5.2.2	运维安全/介质管理/介质的使用管理文档化	必测项	应建立介质安全管理制度，对介质的存放环境、使用、维护和销毁等方面作出规定。	1.询问介质管理人员是否应建立介质安全管理制度，对介质的存放环境、使用、维护和销毁等方面作出规定； 2.按照介质安全管理制度是否记录完整。	制定了比较全面的介质安全管理制度，并按照要求进行记录。	管理类
4.5.2.3	运维安全/介质管理/维修或销毁介质之前清除敏感数据	必测项	1.送出维修以及销毁等进行严格的管理，对送出维修或销毁的介质应首先清除介质中的敏感数据，对保密性较高的存储介质未经批准不得自行销毁； 2.设备确需送外单位维修时，应指定专门部门彻底清除所存的工作相关信息，必要时应与设备维修厂商签订保密协议，与密码设备配套使用的设备送修前应请生产设备的科研单位拆除与密码有	1.询问介质管理人员是否有介质送出的审批流程，在审批流程是否有对数据密级要求、清除方法进行说明； 2.现场检查审批流程的相关记录，并查看最近的维修记录； 3.询问介质管理人员是否对保密性较高的介质的销毁审批流程，是否有相关的记录。	1.制定了介质外出审批流程和维修记录； 2.制定了保密性较高的介质销毁审批流程和相关记录。	管理类

编号	检测项	检测说明	技术要求细化	检测方法及步骤	预期结果及判定	类别
			关的硬件，并彻底清除与密码有关的软件和信息，并派专人在场监督。			
4.5.2.4	运维安全/介质管理/介质管理记录	必测项	应对介质在物理传输过程中的人员选择、打包、交付等情况进行控制，对介质归档和查询等进行登记记录，并根据存档介质的目录清单定期盘点。	1.在介质安全管理制度中是否有对介质在物理传输过程中的人员选择、打包、交付等情况控制措施，并有相关的记录； 2.现场核查介质的归档查询是否有进行登记记录； 3.现场核查存档介质的清单，是否有定期盘点记录。	1.介质在物理传输过程中的人员选择、打包、交付等情况控制措施； 2.归档查询有进行登记； 3.有存档介质清单，并进行定期盘点，有盘点记录。	管理类
4.5.2.5	运维安全/介质管理/介质的分类与标识	必测项	1.重要介质中的数据和软件应采用加密存储； 2.应按照重要程度对介质进行分类和标识。	1.询问介质管理人员，对介质的分类和标识是否制定了相应的管理制度； 2.现场核查对介质的分类和标识是否按照管理制度执行，并有相关记录。	制定了相关的介质分类和标识的管理制度，相关记录完整。	管理类
4.5.3.1	运维安全/设备管理/设备管理的责任人员或部门	必测项	应对信息系统相关的各种设备（包括备份和冗余设备）、线路等指定专门的部门或人员进行管理。	访谈管理人员，是否指定专门的部门或人员对信息系统相关的各种设备（包括备份和冗余设备）、线路等进行管理。	管理人员说明指定了专门的部门或人员对信息系统相关的各种设备（包括备份和冗余设备）、线路等进行管理，管理部门/人员。	管理类
4.5.3.2	运维安全/设备管理/设施、设备定期维护	必测项	1.应对信息系统相关的各种设备（包括备份和冗余设备）、线路等指定专门的部门或人员定期进行维护管理； 2.应建立配套设施、软硬件维护方面的管理制度，对其维护进行有效的管理，包括明确维护人员的责任、涉外维修和服务的审批、维修过程的监督控制等。	1.访谈管理人员，是否指定专门的部门或人员对信息系统相关的各种设备（包括备份和冗余设备）、线路等定期进行维护管理； 2.检查是否建立配套设施、软硬件维护方面的管理制度，对其维护进行有效的管理，包括明确维护人员的责任、涉外维修和服务的审批、维修过程的监督控制等 。	1.管理人员说明指定了专门的部门或人员对信息系统相关的各种设备（包括备份和冗余设备）、线路等定期进行维护管理，指定的部门/人员、维护周期； 2.建立了配套设施、软硬件维护方面的管理制度，对其维护进行有效的管理，包括明确维护人员的责任、涉外维修和服务	管理类

编号	检测项	检测说明	技术要求细化	检测方法及步骤	预期结果及判定	类别
					的审批、维修过程的监督控制等。	
4.5.3.3	运维安全/设备管理/设备选型、采购、发放等的审批控制	必测项	1.应建立基于申报、审批和专人负责的设备安全管理制度，对信息系统的各种软硬件设备的选型、采购、发放和领用等过程进行规范化管理； 2.新购置的设备应经过测试，测试合格后方能投入使用。	1.检查基于申报、审批和专人负责的设备安全管理制度，是否明确信息系统的各种软硬件设备的选型、采购、发放和领用等过程的规范化管理； 2.检查新购置的设备测试记录，是否测试合格后方能投入使用。	1.建立了基于申报、审批和专人负责的设备安全管理制度，对信息系统的各种软硬件设备的选型、采购、发放和领用等过程进行规范化管理； 2.有新购置的设备测试记录，测试合格后方投入使用。	管理类
4.5.3.4	运维安全/设备管理/设备配置标准化	必测项	应建立标准化的设备配置文档。	访谈相关人员，是否建立标准化的设备配置文档，检查设备配置文档，是否与实际设备类型相符。	被访谈人员说明建立了标准化的设备配置文档，并与实际设备类型相符。	管理类
4.5.3.5	运维安全/设备管理/设备的操作规程	必测项	应对终端计算机、工作站、便携机、系统和网络等设备的操作和使用进行规范化管理，按操作规程实现主要设备（包括备份和冗余设备）的启动/停止、加电/断电等操作。	访谈相关人员，是否对终端计算机、工作站、便携机、系统和网络等设备的操作和使用进行规范化管理，按操作规程实现主要设备（包括备份和冗余设备）的启动/停止、加电/断电等操作。	被访谈人员说明对终端计算机、工作站、便携机、系统和网络等设备的操作和使用进行规范化管理，按操作规程实现主要设备（包括备份和冗余设备）的启动/停止、加电/断电等操作。	管理类
4.5.3.6	运维安全/设备管理/设备的操作日志	必测项	1.应具有完整的设备操作日志； 2.制定规范化的设备故障处理流程，建立详细的故障日志(包括故障发生的时间、范围、现象、处理结果和处理人员等内容)。	1.检查设备操作日志是否完善； 2.检查设备故障处理流程是否合理有效，检查故障日志，是否包含故障发生的时间、范围、现象、处理结果和处理人员等内容。	1.设备操作日志完善； 2.设备故障处理流程合理有效，检查故障日志包含故障发生的时间、范围、现象、处理结果和处理人员等内容。	管理类
4.5.3.7	运维安全/设备管理/设备使用管理文档	必测项	1.应做好设备登记工作，制定设备管理规范，落实设备使用者的安全保护责任； 2.应对终端计算机、工作站、便携机、系统和网络等设备的操作和	1.检查设备登记记录和设备管理规范，是否明确设备使用者的安全保护责任； 2.检查设备操作和使用相关记录，是否对终端计算机、工作站、便携机、系统和网络等设备的操作和使用进行	1.有设备登记记录和设备管理规范，明确设备使用者的安全保护责任； 2.有设备操作和使用相关记录，对终端计算机、工作站、便携	管理类

编号	检测项	检测说明	技术要求细化	检测方法及步骤	预期结果及判定	类别
			使用进行规范化管理。	规范化管理。	机、系统和网络等设备的操作和使用进行规范化管理。	
4.5.3.8	运维安全/设备管理/设备标识	必测项	应对设备进行分类和标识。	检查是否对设备进行分类和标识，且标识显而易见。	对设备进行分类和标识，标识显而易见。	管理类
4.5.4.1	运维安全/人员管理/人员录用	必测项	1.应指定或授权专门的部门或人员负责人员录用； 2.应严格规范人员录用过程，对被录用人的身份、背景、专业资格和资质等进行审查，对其所具有的技术技能进行考核； 3.应签署保密协议； 4.应从内部人员中选拔从事关键岗位的人员，并签署岗位安全协议。	1.访谈管理人员，是否指定/授权了专门的部门/人员负责人员录用； 2.访谈录用负责人员，是否严格规范人员录用过程，对被录用人的身份、背景、专业资格和资质等进行审查，对其所具有的技术技能进行考核并签署保密协议，检查录用人员考核记录和保密协议； 3.访谈录用负责人员，是否从内部人员中选拔从事关键岗位的人员，并签署岗位安全协议，检查岗位安全协议。	1.管理人员说明指定/授权了专门的部门/人员负责人员录用； 2.录用负责人员说明严格规范人员录用过程，对被录用人的身份、背景、专业资格和资质等进行审查，对其所具有的技术技能进行考核并签署保密协议。有录用人员考核记录和保密协议； 3.录用负责人员说明从内部人员中选拔从事关键岗位的人员，并签署岗位安全协议。有岗位安全协议。	管理类
4.5.4.2	运维安全/人员管理/人员转岗、离岗	必测项	1.应严格规范人员离岗过程，及时终止离岗员工的所有访问权限； 2.应取回各种身份证件、钥匙、徽章等以及机构提供的软硬件设备； 3.应办理严格的调离手续，关键岗位人员离岗须承诺调离后的保密义务后方可离开。	1.访谈录用负责人员，是否严格规范人员离岗过程，及时终止离岗员工的所有访问权限，取回各种身份证件、钥匙、徽章等以及机构提供的软硬件设备； 2.访谈录用负责人员，是否办理严格的调离手续，关键岗位人员离岗须承诺调离后的保密义务后方可离开。	1.录用负责人员说明严格规范人员离岗过程，及时终止离岗员工的所有访问权限，取回各种身份证件、钥匙、徽章等以及机构提供的软硬件设备； 2.录用负责人员说明办理严格的调离手续，关键岗位人员离岗须承诺调离后的保密义务后方可离开。	管理类
4.5.4.3	运维安全/人员管理/人员考核	必测项	1.应定期对各个岗位的人员进行安全技能及安全认知的考核；	1.访谈录用负责人员，是否定期对各个岗位的人员进行安全技能及安全认知的考	1.录用负责人员说明定期对各个岗位的人员进行安全技能及安	管理类

编号	检测项	检测说明	技术要求细化	检测方法及步骤	预期结果及判定	类别
			2.应对关键岗位的人员进行全面、严格的安全审查和技能考核； 3.应对考核结果进行记录并保存。	核，对关键岗位的人员进行全面、严格的安全审查和技能考核，并对考核结果进行记录并保存； 2.检查考核记录和安全审查记录。	全认知的考核，对关键岗位的人员进行全面、严格的安全审查和技能考核，并对考核结果进行记录并保存，并有考核周期； 2.有考核记录和安全审查记录。	
4.5.4.4	运维安全/人员管理/安全意识教育和培训	必测项	1.应对各类人员进行安全意识教育、岗位技能培训和相关安全技术培训； 2.应对安全责任和惩戒措施进行书面规定并告知相关人员，对违反违背安全策略和规定的人员进行惩戒； 3.应对定期安全教育和培训进行书面规定，针对不同岗位制定不同的培训计划，对信息安全基础知识、岗位操作规程等进行培训； 4.应对安全教育和培训的情况和结果进行记录并归档保存。	1.访谈相关人员，是否对各类人员进行安全意识教育、岗位技能培训和相关安全技术培训，对安全责任和惩戒措施进行书面规定并告知相关人员，对违反违背安全策略和规定的人员进行惩戒，是否对安全教育和培训的情况和结果进行记录并归档保存； 2.检查安全教育和培训的情况和结果记录； 3.检查关于安全教育和培训的书面规定，是否针对不同岗位制定不同的培训计划，对信息安全基础知识、岗位操作规程等进行培训。	1.被访谈人员说明对各类人员进行安全意识教育、岗位技能培训和相关安全技术培训，对安全责任和惩戒措施进行书面规定并告知相关人员，对违反违背安全策略和规定的人员进行惩戒，对安全教育和培训的情况和结果进行记录并归档保存； 2.有安全教育和培训的情况和结果记录； 3.关于安全教育和培训的书面规定针对不同岗位制定不同的培训计划，明确对信息安全基础知识、岗位操作规程等进行培训。	管理类
4.5.4.5	运维安全/人员管理/外部人员访问管理	必测项	1.应确保在外部人员访问受控区域前先提出书面申请，批准后由专人全程陪同或监督，并登记备案； 2.应对外部人员允许访问的区域、系统、设备、信息等内容应进行书面的规定，并按照规定执行。	1.访谈管理人员，在外部人员访问受控区域前是否先提出书面申请，批准后由专人全程陪同或监督，并登记备案，是否对外部人员允许访问的区域、系统、设备、信息等内容应进行书面的规定，并按照规定执行； 2.检查申请记录、登记备案记录、外部人员允许访问的区域、系统、设备、信息等	1.管理人员说明在外部人员访问受控区域前先提出书面申请，批准后由专人全程陪同或监督，并登记备案，对外部人员允许访问的区域、系统、设备、信息等内容应进行书面的规定，并按照规定执行； 2.有申请记录、登记	管理类

编号	检测项	检测说明	技术要求细化	检测方法及步骤	预期结果及判定	类别
				内容的书面规定。	备案记录、外部人员允许访问的区域、系统、设备、信息等内容的书面规定。	
4.5.4.6	运维安全/人员管理/职责分离	必测项	关键岗位人员应职责分离。	检查是否对关键岗位人员进行职责分离。	对关键岗位人员进行职责分离。	管理类
4.5.5.1	运维安全/监控管理/主要网络设备的各项指标监控情况	必测项	应对通信线路、网络设备的运行状况、网络流量、用户行为等进行监测和报警，形成记录并妥善保存。	检查通信线路、网络设备的运行状况、网络流量、用户行为等的监测工具、工具运行状况、监控记录、报警方式和报警记录等内容。	使用工具监控通信线路、网络设备的运行状况、网络流量、用户行为等，出现异常后按要求方式报警，监控工具运行良好，有监控记录和报警记录。	管理类
4.5.5.2	运维安全/监控管理/主要服务器的各项指标监控情况	必测项	应对主机的运行状况、用户行为等进行监测和报警，形成记录并妥善保存。	检查主机的运行状况、用户行为等的监测工具、工具运行状况、监控记录、报警方式和报警记录等内容。	使用工具监控主机的运行状况、用户行为等，出现异常后按要求方式报警，监控工具运行良好，有监控记录和报警记录。	管理类
4.5.5.3	运维安全/监控管理/应用运行各项指标监控情况	必测项	应对应用软件的运行状况进行监测和报警，形成记录并妥善保存。	检查应用软件运行状况的监测工具、工具运行状况、监控记录、报警方式和报警记录等内容。	使用工具监控应用软件的运行状况，出现异常后按要求方式报警，监控工具运行良好，有监控记录和报警记录。	管理类
4.5.5.4	运维安全/监控管理/异常处理机制	必测项	1.应组织相关人员定期对监测和报警记录进行分析、评审，发现可疑行为，形成分析报告，并采取必要的应对措施； 2.应按重要程度进行分级报警，并且重要报警要能以某种方式（短信、邮件等）主动通知相关人员及时处置； 3.此外，还应组织相关人员定期对监测和报	1.检查是否组织相关人员定期对监测和报警记录进行分析、评审，发现可疑行为，形成分析报告，并采取必要的应对措施； 2.检查是否按重要程度进行分级报警，并且重要报警要能以某种方式（短信、邮件等）主动通知相关人员及时处置。是否组织相关人员定期对监测和报警记录进行分析、评审，发现可疑行为，形成分析报告，采取必要措	1.组织人员定期对监测和报警记录进行分析、评审，发现可疑行为，形成分析报告，并采取必要的应对措施； 2.按重要程度进行分级报警，重要报警以某种方式主动通知相关人员及时处置。组织人员定期对监测和报警记录进行分析、评审，发现可疑行为，	管理类

编号	检测项	检测说明	技术要求细化	检测方法及步骤	预期结果及判定	类别
			警记录进行分析、评审，发现可疑行为，形成分析报告，采取必要措施。	施。	形成分析报告，采取必要措施。	
4.5.6.1	运维安全/变更管理/变更方案	必测项	应确认系统中要发生的变更，并制定变更方案。	检查是否确认系统中要发生的变更，并制定对应的变更方案。	确认系统中要发生的变更，并制定对应的变更方案。	管理类
4.5.6.2	运维安全/变更管理/变更制度化管理	必测项	应建立变更管理制度，系统发生变更前，向主管领导申请，变更申请和变更方案须经过评审、审批后方可实施变更，并在实施后将变更情况向相关人员通告。	检查变更管理制度，明确系统发生变更前，向主管领导申请，变更申请和变更方案须经过评审、审批后方可实施变更，并在实施后将变更情况向相关人员通告。	变更管理制度明确系统发生变更前，向主管领导申请，变更申请和变更方案须经过评审、审批后方可实施变更，并在实施后将变更情况向相关人员通告。	管理类
4.5.6.3	运维安全/变更管理/重要系统变更的批准	必测项	应建立变更控制的申报和审批文件化程序，对变更影响进行分析并文档化，变更内容中要有变更失败后的回退方案等，记录变更实施过程，并妥善保存所有文档和记录。	1.检查是否有变更控制的申报和审批文件化程序，是否明确对变更影响进行分析并文档化； 2.检查变更内容中是否包含变更失败后的回退方案等，检查变更过程中产生的文档和记录。	1.有变更控制的申报和审批文件化程序，对变更影响进行分析并文档化； 2.变更内容中包含变更失败后的回退方案等，有变更过程中产生的文档和记录。	管理类
4.5.6.4	运维安全/变更管理/重要系统变更的通知	必测项	重要系统变更前，应通过相关单位、部门和人员。	检查变更内容中是否包含变更前的通知的人员范围。	变更内容中包含变更前的通知人员的范围。	管理类
4.5.7.1	运维安全/安全事件处置/安全事件报告和处置	必测项	1.应制定安全事件报告和处置管理制度，明确安全事件的类型，规定安全事件的现场处理、事件报告和后期恢复的管理职责； 2.应制定安全事件报告和响应处理程序，确定事件的报告流程，响应和处置的范围、程度，以及处理方法等。	1.检查安全事件报告和处置管理制度，是否明确安全事件的类型，规定安全事件的现场处理、事件报告和后期恢复的管理职责； 2.检查安全事件报告和响应处理程序，是否明确事件的报告流程，响应和处置的范围、程度，以及处理方法等。	1.安全事件报告和处置管理制度明确了安全事件的类型，规定了安全事件的现场处理、事件报告和后期恢复的管理职责； 2.安全事件报告和响应处理程序明确了事件的报告流程，响应和处置的范围、程度，以及处理方法等。	管理类
4.5.7.2	运维安全/安全事件处	必测项	应根据国家相关管理部门对计算机安全事	检查安全事件报告相关管理制度，是否根据国家相关管	根据国家相关管理部门对计算机安全事件	管理

编号	检测项	检测说明	技术要求细化	检测方法及步骤	预期结果及判定	类别
	置/安全事件的分类和分级		件等级划分方法和安全事件对本系统产生的影响，对本系统计算机安全事件进行等级划分。	理部门对计算机安全事件等级划分方法和安全事件对本系统产生的影响，对本系统计算机安全事件进行等级划分。	等级划分方法和安全事件对本系统产生的影响，对本系统计算机安全事件进行等级划分。	类
4.5.7.3	运维安全/安全事件处置/安全事件记录和采取的措施	必测项	1.应在安全事件报告和响应处理过程中，分析和鉴定事件产生的原因，收集证据，记录处理过程，总结经验教训，制定防止再次发生的补救措施，过程形成的所有文件和记录均应妥善保存； 2.对造成系统中断和造成信息泄密的安全事件应采用不同的处理程序和报告程序。	1.检查安全事件记录，是否包含事件原因分析、处理方法、经验教训等内容； 2.检查安全事件报告和响应处理程序，是否对造成系统中断和造成信息泄密的安全事件采用不同的处理程序和报告程序。	1.安全事件记录包含事件原因分析、处理方法、经验教训等内容； 2.安全事件报告和响应处理程序对造成系统中断和造成信息泄密的安全事件采用不同的处理程序和报告程序。	管理类
4.5.8.1	运维安全/应急预案管理/制定不同事件的应急预案	必测项	1.应在统一的应急预案框架下制定不同事件的应急预案，应急预案框架应包括启动应急预案的条件、应急处理流程、系统恢复流程、事后教育和培训等内容； 2.从人力、设备、技术和财务等方面确保应急预案的执行有足够的资源保障； 3.应制定与其业务规模、复杂程度相适应的应急预案。	1.检查是否在统一的应急预案框架下制定不同事件的应急预案，应急预案框架包括启动应急预案的条件、应急处理流程、系统恢复流程、事后教育和培训等内容； 2.访谈相关人员，是否从人力、设备、技术和财务等方面确保应急预案的执行有足够的资源保障； 3.访谈相关人员，是否制定与其业务规模、复杂程度相适应的应急预案。	1.在统一的应急预案框架下制定不同事件的应急预案，应急预案框架包括启动应急预案的条件、应急处理流程、系统恢复流程、事后教育和培训等内容； 2.被访谈人员说明从人力、设备、技术和财务等方面确保应急预案的执行有足够的资源保障； 3.被访谈人员说明制定与其业务规模、复杂程度相适应的应急预案。	管理类
4.5.8.2	运维安全/应急预案管理/相关人员应急预案培训	必测项	应对系统相关的人员进行应急预案培训，应急预案的培训应至少每年举办一次。	检查应急预案培训计划，是否覆盖与系统相关的所有人员，且应急预案的培训至少每年举办一次。	制定应急预案培训计划，覆盖了与系统相关的所有人员，培训频率符合要求。	管理类

编号	检测项	检测说明	技术要求细化	检测方法及步骤	预期结果及判定	类别
4.5.8.3	运维安全/应急预案管理/定期演练	必测项	应制定演练计划，根据不同的应急恢复内容，确定演练的周期。对应急预案演练中暴露出的问题进行总结并及时整改。	检查演练计划，并明确是否根据不同的应急恢复内容，确定演练的周期。对应急预案演练中暴露出的问题是否进行总结并及时整改。	制定了演练计划，包含应急恢复内容、参与部门等，对应急预案演练中暴露出的问题进行总结并及时整改。	管理类

8.6 业务连续性测试

对支付业务设施的业务连续性进行检测，主要考察系统是否具备业务连续性管理并达到设计目标。检测内容见表9。

表9 业务连续性测试

编号	检测项	检测说明	技术要求细化	检测方法及步骤	预期结果及判定	类别
4.6.1.1	业务连续性/业务连续性需求分析/业务中断影响分析	必测项	应进行业务中断影响分析。	检查是否制定业务中断影响分析。	制定了支付业务的业务中断影响分析，对业务中断后可能产生的影响进行分析。	管理类
4.6.1.2	业务连续性/业务连续性需求分析/灾难恢复时间目标和恢复点目标	必测项	应具备灾难恢复时间目标和恢复点目标。	访谈相关人员，是否具备灾难恢复时间目标和恢复点目标。	按业务系统优先级对应用系统制定灾难恢复时间目标和恢复点目标，RPO小于等于规定时间，RTO小于等于规定时间。	管理类
4.6.2.1	业务连续性/业务连续性技术环境/备份机房	必测项	1.应定期进行完全数据备份，备份介质场外存放； 2.应配备灾难恢复所需数据处理设备；配备灾难恢复所需的通信线路； 3.应提供备份介质存放场地，提供备用数据处理系统和备用网络设备运行的场地； 4.应有计算机机房管理人员、数据备份技术支持人员和硬件、网络技术支持人员；	1.检查是否定期进行完全数据备份，备份介质场外存放； 2.检查是否配备灾难恢复所需数据处理设备；检查是否配备灾难恢复所需的通信线路； 3.检查是否提供备份介质存放场地，提供备用数据处理系统和备用网络设备运行的场地； 4.检查是否有计算机机房管理人员、数据备份技术支持人员和硬件、网络技术支持人员；	具有同城应用级备份机房，位于哪个市区哪条路。	管理类

编号	检测项	检测说明	技术要求细化	检测方法及步骤	预期结果及判定	类别
			5.应有介质存取、验证和转储管理制度；按介质特性对备份数据进行定期的有效性验证；有备用计算机机房运行管理制度；有硬件和网络运行管理制度；有电子传输数据备份系统运行管理制度。	5.检查是否有介质存取、验证和转储管理制度；检查是否按介质特性对备份数据进行定期的有效性验证；检查是否有备用计算机机房运行管理制度；检查是否有硬件和网络运行管理制度；检查是否有电子传输数据备份系统运行管理制度。		
4.6.2.2	业务连续性/业务连续性技术环境/网络双链路	必测项	应具备双链路。	检查主机房的互联网接入是否为不同运营商的两条链路。	主机房的互联网接入采用不同运营商。	管理类
4.6.2.3	业务连续性/业务连续性技术环境/网络设备和服务器备份	必测项	应具有同城应用级备份设施。	检查主机房的网络设备和服务器是否有同城备份措施。	主机房的网络设备和服务器实现同城备份。	管理类
4.6.2.4	业务连续性/业务连续性技术环境/高可靠的磁盘阵列	必测项	应使用高可靠的磁盘阵列。	1.访谈安全管理员是否使用了高可靠的磁盘阵列； 2.查看磁盘阵列设备。	采用服务器磁盘阵列方式组建主机房本地数据物理存储环境。	管理类
4.6.2.5	业务连续性/业务连续性技术环境/远程数据库备份	必测项	应具备远程备份数据库。	1.访谈安全管理员是否进行远程数据库备份； 2.查看备份记录； 3.检查备份策略，备份主机IP地址等。	提供异地灾备机房数据库服务器备份方式和备份记录。	管理类
4.6.3.1	业务连续性/业务连续性管理/业务连续性管理制度	必测项	1.应具备业务连续性管理制度； 2.业务连续性管理制度内容应完备，与实际执行应一致。	1.访谈安全管理员业务连续性管理制度内容； 2.查看业务连续性管理制度； 3.查看执行记录。	具备业务连续性管理制度，内容完备，实际工作中按照制度执行。	管理类
4.6.3.2	业务连续性/业务连续性管理/应急响应流程	必测项	应具备应急响应流程，应急响应流程合理。	1.访谈安全管理员是否具备应急响应流程； 2.查看应急响应流程相关文档。	应急响应流程有相关稳定规定和描述，合理。	管理类

编号	检测项	检测说明	技术要求细化	检测方法及步骤	预期结果及判定	类别
4.6.3.3	业务连续性/业务连续性管理/恢复预案	必测项	应具备不同场景（数据备份、应用级备份）恢复预案，内容完备、合理。	1.访谈安全管理员是否具备恢复预案； 2.查看恢复预案。	具备应用级恢复预案，内容完备、合理。	管理类
4.6.3.4	业务连续性/业务连续性管理/数据备份和恢复制度	必测项	应具备数据备份和恢复管理制度，内容完备、合理。	1.访谈安全管理员是否具备数据备份和恢复管理制度； 2.查看数据备份和恢复管理制度。	具备数据备份和恢复管理制度，内容是否完备、合理。	管理类
4.6.4.1	业务连续性/备份与恢复管理/备份数据范围和备份频率	必测项	应具备备份数据范围和备份频率清单。	1.访谈安全管理员是否具备备份数据范围和备份频率清单； 2.查看备份数据范围和备份频率清单。	具备备份数据范围和备份频率清单。	管理类
4.6.4.2	业务连续性/备份与恢复管理/备份和恢复手册	必测项	应具备数据备份和恢复手册，内容完备、与实际操作一致。	1.访谈安全管理员是否具备数据备份和恢复手册； 2.查看数据备份和恢复手册； 3.查看执行记录； 4.查看其数据备份策略能否满足业务连续性中灾难恢复点目标值。	1.具备数据备份和恢复手册，内容完备、一致； 2.数据备份策略可以满足业务连续性中灾难恢复点目标值。	管理类
4.6.4.3	业务连续性/备份与恢复管理/备份记录和定期恢复测试记录	必测项	应具备备份记录和定期恢复测试记录。	1.访谈安全管理员是否具备备份记录和定期恢复测试记录； 2.查看备份记录和定期恢复测试记录。	具备备份记录和定期恢复测试记录。	管理类
4.6.4.4	业务连续性/备份与恢复管理/定期数据备份恢复性测试	必测项	应定期进行备份数据的恢复性测试，并有记录。	1.访谈安全管理员是否定期数据备份恢复性测试； 2.查看记录。	定期进行备份数据的恢复性测试，有记录。	管理类
4.6.5.1	业务连续性/日常维护/每年业务连续性演练	必测项	应每年进行业务连续性演练，具备演练记录。	1.访谈安全管理员是否每年进行业务连续性演练； 2.查看记录。	每年进行业务连续性演练，具备演练记录。	管理类
4.6.5.2	业务连续性/日常维护/	必测项	应定期进行业务连续性培训并具有培训记	1.访谈安全管理员是否定期进行业务连续性培	定期进行业务连续性培训并具有培训记录。	管理

编号	检测项	检 测 说明	技术要求细化	检测方法及步骤	预期结果及判定	类别
	定期业务连续性培训		录。	训并具有培训记录； 2.查看记录。		类

9 文档审核

对支付业务设施的用户文档、开发文档、管理文档的完备性、一致性、正确性、规范性，以及是否符合行业标准，是否遵从更新控制和配置管理的要求等方面进行检测。检测内容见表10。

表10 文档审核

编号	检测项		检测说明	类别
5.1	用户文档	5.1.1 用户手册	必测项	管理类
		5.1.2 操作手册	必测项	管理类
5.2	开发文档	5.2.1 需求说明书	必测项	管理类
		5.2.2 需求分析文档	必测项	管理类
		5.2.3 总体设计方案	必测项	管理类
		5.2.4 数据库设计文档	必测项	管理类
		5.2.5 概要设计文档	必测项	管理类
		5.2.6 详细设计文档	必测项	管理类
		5.2.7 工程实施方案	必测项	管理类
5.3	管理文档	5.3.1 测试报告	必测项	管理类
		5.3.2 系统运维手册	必测项	管理类
		5.3.3 系统应急手册	必测项	管理类
		5.3.4 运维管理制度	必测项	管理类
		5.3.5 安全管理制度	必测项	管理类
		5.3.6 安全审计报告	必测项	管理类

10 外包附加测试

对于非金融机构将支付业务设施相关运维外包给第三方服务机构的情况，还应进行外包附加测试，检测内容见表11。

表11 外包附加测试

编号	检测项		检测说明	类别
6.1	外包服务的外包内容	6.1.1 外包程度及具体内容	必测项	管理类
6.2	安全保密协议	6.2.1 签署外包安全保密协议	必测项	管理类

编号	检测项		检测说明	类别
		6.2.2 保障托管数据的安全、可靠	必测项	管理类
		6.2.3 明确双方责任	必测项	管理类
6.3	风险评估	6.3.1 评估业务外包相关风险	必测项	管理类
		6.3.2 外包商的合同义务和要求	必测项	管理类
		6.3.3 控制和报告程序	必测项	管理类
		6.3.4 外包协议的持续评估	必测项	管理类
		6.3.5 符合监管要求和准则	必测项	管理类
		6.3.6 外包服务应急计划	必测项	管理类
6.4	外包商资质	6.4.1 外包商提供支付服务的经验和能力评估	必测项	管理类
		6.4.2 外包商硬件资源评估	必测项	管理类
		6.4.3 外包商的财务状况评估	必测项	管理类
		6.4.4 外包商的资金构成、人员构成以及主管部门的审批	必测项	管理类
		6.4.5 外包商的运维管理制度评估	必测项	管理类
		6.4.6 外包模式调查及风险评估	必测项	管理类
6.5	外包合同	6.5.1 明确规定有关各方的权利和义务	必测项	管理类
		6.5.2 明确外包商最低的服务水平	必测项	管理类
		6.5.3 规定保守信息资源机密	必测项	管理类
		6.5.4 规定争议解决办法	必测项	管理类
6.6	控制和监督	6.6.1 对外包业务的管理和监督	必测项	管理类
		6.6.2 定期评估外包商的财务状况	必测项	管理类
		6.6.3 定期审查合同条款的履行	必测项	管理类
6.7	外包交付	6.7.1 制定详细的系统交付清单	必测项	管理类
		6.7.2 技术人员的业务培训	必测项	管理类

附 录 A
（资料性附录）
检测过程风险分析

为保证检测实施的顺利进行，应在检测方案中分析支付业务设施在检测过程中出现的风险，并提出相应的应对措施，见表A.1。

表A.1 检测过程风险分析

风险编号	风险描述	风险发生可能性	风险对测试或项目的影响	责任人	规避方法
1	应用服务器或数据库服务器在测试中出现无法预料的未知错误，导致测试失败。	高	高	被检测方	对应用服务器、数据库服务器进行性能的预先评估，调整测试计划，预留调优时间直至延长测试时间。
2	被检测方技术支持人员不到位。	中	高	被检测方	充分的沟通与协调人力资源，保证检测活动的顺利进行。
3	测试环境受到干扰，比如数据库服务器或应用服务器被临时征用，不能专职为本测试服务。	低	高	被检测方	暂停测试，等待测试环境恢复正常，推迟测试计划。
4	测试数据准备不成功。	低	高	被检测方	由开发人员帮助解决。
5	性能测试方面的疲劳度不足，长时间运行情况不确定。	中	中	被检测方	保证测试进程的顺利进行，适当时候能延长测试周期。
6	在对服务器加压方面有欠缺。	低	中	被检测方	加深对系统的了解，尽量全面地覆盖系统业务功能点。
7	工具缺陷，测试工具和监控工具无法全部支持的所有 IT 系统的测试和监控。	中	高	被检测方	尽量在测试前能够准备充分，能提前使用系统以便对测试工具调试。
8	测试环境及条件制约，环境复杂多变，造成真正的测试加压时间缩短。	中	中	被检测方	保证测试环境的正常稳定运行。
9	被测系统与生产系统的不一致性，测试环境和生产环境的系统配置差别较大。	高	高	被检测方	尽量能够采用和生产环境配置性能相近的设备。

参 考 文 献

[1] GB/T 8567-2006 计算机软件文档编制规范
[2] GB/T 9385-2008 计算机软件需求规格说明规范
[3] GB/T 9386-2008 计算机软件测试文档编制规范
[4] GB/T 14394-2008 计算机软件可靠性和可维护性管理
[5] GB/T 15532-2008 计算机软件测试规范
[6] GB/T 16260-2006 软件工程 产品质量
[7] GB 17859-1999 计算机信息系统 安全保护等级划分准则
[8] GB/T 18336-2008 信息技术 安全技术 信息技术安全性评估准则
[9] GB/T 18905-2002 软件工程 产品评价
[10]GB/T 20271-2006 信息安全技术 信息系统通用安全技术要求
[11]GB/T 22080-2008 信息技术 安全技术 信息安全管理体系要求
[12]GB/T 22081-2008 信息技术 安全技术 信息安全管理实用规则
[13]GB/T 22239-2008 信息安全技术 信息系统安全等级保护基本要求
[14]GB/T 25000.51-2010 软件工程 软件产品质量要求与评价（SQuaRE） 商业现货（COTS）软件产品的质量要求和测试细则
[15]GB/T 27025-2008 检测和校准实验室能力的通用要求