ICS 03.060
A 11

JR

中 华 人 民 共 和 国 金 融 行 业 标 准

JR/T 0123.3—2018
代替 JR/T 0123.3—2014

非银行支付机构支付业务设施检测规范 第3部分：银行卡收单

Test specification of non-bank payment institutions payment service facilities—Part 3：Bank card acceptance

2018－10－29 发布　　2018－10－29 实施

中国人民银行　发布

目　　次

前　言

JR/T 0123《非银行支付机构支付业务设施检测规范》分为6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；

——第6部分：条码支付。

本部分为JR/T 0123的第3部分。

本部分按照GB/T 1.1—2009给出的规则起草。

本部分代替JR/T 0123.3—2014《非金融机构支付业务设施检测规范　第3部分：银行卡收单》，与JR/T 0123.3—2014相比主要变化如下：

——标准名称由《非金融机构支付业务设施检测规范　第3部分：银行卡收单》修改为《非银行支付机构支付业务设施检测规范　第3部分：银行卡收单》；

——增加了风险及反洗钱管理制度要求（见第6章）；

——增加了对自建机房的物理安全要求（见8.1）；

——增加了主机对象审计、应用操作审计的要求（见第8章）；

——修改了网络安全中对网络域安全隔离和限制、内容过滤、网络对象审计等的要求（见第8章，2014年版的第8章）；

——修改了主机安全中对访问控制范围等的要求（见第8章，2014年版的第8章）；

——修改了应用安全中对可信时间戳服务、登录访问安全策略、日志信息的要求（见第8章，2014年版的第8章）；

——增加了数据安全中对个人信息保护、数据使用的要求（见8.5）；

——增加了运维安全文档管理要求（见8.6）；

——删除了文档要求（见2014年版的第9章）；

——删除了外包附加要求（见2014年版的第10章）；

——增加了SM系列算法的使用要求（见第8章）。

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：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、银行卡检测中心、上海市信息安全测评认证中心、中金金融认证中心有限公司、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）、北京软件产品质量检测检验中心（国家应用软件产品质量监督检验中心）、中电科技（北京）有限公司、中国电子科技集团公司第十五研究所（信息产业信息安全测评中心）、支付宝（中国）网络技术有限公司、银联商务股份有限公司、财付通支付科技有限公司、网银在线（北京）科技有限公司。

本部分主要起草人：安荔荔、潘润红、邬向阳、聂丽琴、赵春华、高天游、王翠、王鹏飞、裴倩如、李红曼、焦莉纳、唐立军、牛跃华、林春、马鸣、刘欣、王妍娟、夏采莲、高祖康、陆嘉琪、王凯阳、赵亮、于泉、冯云、张益、宋铮、何韡、吴永强、马志斌。

本部分于2014年11月24日首次发布，本次为第一次修订。

引　言

JR/T 0123—2018基于JR/T 0122—2018《非银行支付机构支付业务设施技术要求》编制。检测目标是在系统版本确定的基础上，对非银行支付机构提供的支付业务设施的功能、风险监控、性能、安全性进行测试，客观、公正地评估设施是否符合中国人民银行对支付业务设施的技术标准要求，保障我国支付业务设施的安全稳定运行。

非银行支付机构支付业务设施检测规范
第3部分：银行卡收单

1 范围

本部分规定了非银行支付机构银行卡收单业务设施的功能、风险监控、性能、安全等方面的测试要求。

本部分适用于非银行支付机构银行卡收单业务设施的建设管理，以及第三方检测机构的检测工作。

注：支付业务设施包括支付业务处理系统、网络通信系统以及容纳上述系统的专用机房。

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 32905 信息安全技术 SM3密码杂凑算法

GB/T 32907 信息安全技术 SM4分组密码算法

GB/T 32918（所有部分） 信息安全技术 SM2椭圆曲线公钥密码算法

GM/T 0054—2018 信息系统密码应用基本要求

JR/T 0025.7—2018 中国金融集成电路（IC）卡规范 第7部分：借记贷记应用安全规范

JR/T 0122 非银行支付机构支付业务设施技术要求

中国人民银行.非银行支付机构网络支付业务管理办法（中国人民银行公告〔2015〕第43号），2016-07-01.

3 术语和定义

下列术语和定义适用于本文件。

3.1

非银行支付机构支付服务 non-bank payment institutions payment services

非银行支付机构在收付款人之间作为中介机构提供的下列部分或全部货币资金转移服务：

a) 网络支付；

b) 预付卡发行与受理；

c) 银行卡收单；

d) 中国人民银行确定的其他支付服务。

3.2

银行卡收单 bank card acceptance

收单机构与特约商户签订银行卡受理协议，在特约商户按约定受理银行卡并与持卡人达成交易后，为特约商户提供交易资金结算服务的行为。

3.3

特约商户 contracted merchant

向持卡人提供商品或服务，并接受使用银行卡完成资金结算的企事业单位、个体工商户或其他组织。

4 启动准则

启动测试工作应满足如下条件：

a) 非银行支付机构提交的支付服务业务系统被测版本与生产版本一致。

b) 非银行支付机构支付服务业务系统已完成内部测试。

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) 测试环境准备完毕，具体包括：

1) 测试环境与生产环境基本一致，其中安全性测试在生产环境下进行；

2) 支付服务业务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；

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，可满足测试需求。

5 功能测试

验证支付服务业务系统的业务功能是否能正确实现，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

序号	检测项		检测说明	类别
1	特约商户管理	商户信息登记管理	必测项	技术类
		商户交易状态管理	必测项	技术类
		商户信息查询	非必测项	技术类
		商户受理业务管理	必测项	技术类
		商户终端管理	必测项	技术类
2	终端机具信息管理	机具申领和报废控制	非必测项	管理类
		机具信息维护	非必测项	管理类
		机具信息查询	非必测项	管理类
3	密钥管理	密钥生成	非必测项	技术类
		密钥分发	非必测项	技术类
		密钥使用	非必测项	技术类

序号	检测项		检测说明	类别
		密钥存储	非必测项	技术类
		密钥更新	非必测项	技术类
		密钥销毁	非必测项	技术类
4	交易处理	联机消费	联机交易类必测项	技术类
		联机消费撤销	非必测项	技术类
		联机余额查询	非必测项	技术类
		退货	必测项	技术类
		指定账户圈存	非必测项	技术类
		非指定账户圈存	非必测项	技术类
		圈提	非必测项	技术类
		脱机消费	脱机交易类必测项	技术类
		脱机消费文件处理	脱机交易类必测项	技术类
		脱机余额查询	非必测项	技术类
		交易明细查询	必测项	技术类
		冲正交易	联机交易类必测项	技术类
		IC 卡参数下载	非必测项	技术类
		预授权	非必测项	技术类
		预授权撤销	非必测项	技术类
		预授权完成	非必测项	技术类
		预授权完成撤销	非必测项	技术类
		追加预授权	非必测项	技术类
5	资金结算	商户结算	必测项	技术类
		银行清算	必测项	技术类
6	对账处理	发送对账请求	必测项	管理类
		生成对账文件	必测项	技术类

序号	检测项		检测说明	类别
7	差错处理	单笔退款	必测项	技术类
		批量退款	非必测项	技术类
		差错交易查询	必测项	技术类
		对账差错处理	必测项	技术类
8	运营管理	统计报表	必测项	技术类
		运营人员权限管理	必测项	技术类

6 风险监控及反洗钱测试

验证支付服务业务系统是否具有账户风险、交易风险及反洗钱监控措施，并符合相关要求，测试内容见表2。

表 2 风险监控及反洗钱测试

序号	检测项		检测说明	类别
1	商户风险管理	商户资质审核	必测项	技术类
		商户签约	必测项	技术类
		商户日常风险管理	必测项	技术类
		合作的第三方机构的风险管理	必测项	技术类
		商户黑名单管理	必测项	技术类
2	交易风险管理监控	联机交易 ARQC/ARPC 验证	必测项	技术类
		联机报文 MAC 验证	必测项	技术类
		脱机交易 TAC 验证	必测项	技术类
		脱机报文 MAC 验证	必测项	技术类
		可疑交易处理	必测项	技术类
		卡片黑名单监控	必测项	技术类
3	风险及反洗钱管理制度	风控规则管理	必测项	管理类
		反洗钱管理制度和操作规程	必测项	管理类

序号	检测项		检测说明	类别
		岗位设置	必测项	管理类
		事件管理与处置	必测项	管理类
		风险报表	必测项	技术类
4	终端风险管理	终端使用生命周期管理	非必测项	管理类
		终端密钥和参数的安全管理	非必测项	管理类
		控制移动 POS 机的安装	非必测项	管理类
		终端安全检测报告和终端入网检测报告	非必测项	管理类
		密码键盘安全检测报告	非必测项	管理类
		终端监控管理	非必测项	管理类

7 性能测试

验证支付服务业务系统是否满足未来3年业务运行的性能需求。测试内容包括以下三个方面：

a) 验证系统是否支持业务的多用户并发操作；

b) 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的自恢复能力；

c) 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，选取的性能测试业务点见表3。

表 3 性能测试业务点

序号	检测项	检测说明	类别
1	消费	必测项	技术类
2	预授权	非必测项	技术类
3	日终批处理	必测项	技术类
4	圈存	非必测项	技术类
5	圈提	非必测项	技术类

8 安全性测试

8.1 物理安全性测试

验证自建机房的物理安全性是否符合JR/T 0122相关要求，测试内容见表4。

表 4　物理安全性测试

序号	检测项		检测说明	类别
1	物理位置选择	机房所在建筑物选择	必测项	技术类
		建筑物内机房位置选择	必测项	技术类
2	物理访问控制	机房设置电子门禁系统	必测项	技术类
		来访人员申请和审批	必测项	技术类
		对机房划分区域进行管理	必测项	技术类
3	防盗窃和防破坏	设备放置	必测项	技术类
		设备固定	必测项	技术类
		通信线缆铺设	必测项	技术类
		机房监控防入侵报警系统	必测项	技术类
4	防雷击	安装避雷装置	必测项	技术类
		安装防雷装置	必测项	技术类
		交流电源地线	必测项	技术类
5	防火	设置火灾自动消防系统	必测项	技术类
		机房应采用耐火的建筑材料	必测项	技术类
		采用区域隔离防火措施	必测项	技术类
6	防水和防潮	水管安装要求	必测项	技术类
		防雨水措施	必测项	技术类
		防水检测和报警	必测项	技术类
7	防静电	接地防静电措施	必测项	技术类
		采用防静电地板	必测项	技术类
		安装静电消除装置	必测项	技术类
8	温湿度控制		必测项	技术类
9	电力供应	供电线路防护设备配置	必测项	技术类

序号	检测项		检测说明	类别
		备用电力供应	必测项	技术类
		冗余或并行的电力电缆线路设置	必测项	技术类
		备用供电系统	必测项	技术类
10	电磁防护	防止电磁干扰	必测项	技术类
		电源线和通信线缆隔离铺设	必测项	技术类
		关键设备电磁屏蔽	必测项	技术类

8.2 网络安全性测试

验证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是否符合JR/T 0122相关要求，测试内容见表5。

表5 网络安全性测试

序号	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
1	网络安全/结构安全/网络冗余和备份	必测项	a) 应明确核心网络和边界网络设备承载能力； b) 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； c) 应明确网络带宽是否满足高峰时流量。	a) 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； b) 检查网络设计/验收文档，查看核心和边界网络设备能否满足基本业务需求，查看网络接入及核心网络的带宽能否满足业务高峰期的需要，以及是否存在带宽瓶颈等； c) 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。	a) 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； b) 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，能满足业务高峰期的需要； c) 核心网络设备均采用热备份的策略。	技术类

序号	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	网络安全/结构安全/网络安全路由	必测项	a) 应明确业务终端与业务服务器之间的访问路径； b) 应明确不同访问路径的路由控制措施。	a) 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； b) 查看在访问路径上是否采用具有安全路由技术的网络路由器或相关设备。	a) 业务终端与业务服务器之间的网络路由器配备了必要的路由访问控制设备； b) 路由访问控制设备具备安全访问功能（如采用静态路由或采用认证方式的动态路由）。	技术类
3	网络安全/结构安全/网络安全防火墙	必测项	a) 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； b) 相关访问控制策略应有效实现。	a) 访谈网络管理员，询问网络安全区域间划分情况； b) 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； c) 登录网络访问控制设备管理界面查看配置及状态。	a) 根据网络承载业务重要程度，对网络进行了安全域划分； b) 网络拓扑显示在网络边界处部署了网络访问控制设备； c) 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
4	网络安全/结构安全/网络拓扑结构	必测项	应绘制与当前运行情况相符的网络拓扑结构图。	采用现场抽查的方式，检查机房内的网络设备及实际链接线路与网络拓扑结构图是否一致。	机房内的网络设备及实际链接线路与网络拓扑结构图一致。	技术类
5	网络安全/结构安全/IP子网划分	必测项	a) 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，划分不同的网络区域； b) 应按照方便管理和控制的原则为各网络区域分配地址段。	a) 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； b) 查看IP子网划分情况，与收集的公司业务情况进行比较。	a) 公司建立了依据部门职能、重要性来划分安全等级的安全管理制度； b) 子网划分情况考虑了单位各部门的工作职能、重要性和所涉及信息的重要程度等因素，不同安全等级的机构未划分在同一个子网内，进行了必要隔离。	技术类
6	网络安全/网络访问控制/网络域安全隔离和	必测项	a) 应在网络边界和区域之间部署安全访问控制设备； b) 应启用网络设备	a) 访谈网络管理员，询问是否在网络边界和区域之间部署安全访问控制设备；	a) 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）； b) 上述安全设备已经启	技术类

序号	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
	限制		访问控制功能，根据访问控制策略设置访问控制规则。	b) 对安全访问控制设备进行检查。	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）。	
7	网络安全/网络访问控制/内容过滤	必测项	应在关键网络节点处对进出的信息内容进行过滤，实现对内容的访问控制。	a) 检查内容过滤设备（如防火墙等）的配置信息； b) 检查内容配置是否生效。	a) 内容过滤设备支持对应用层信息的过滤功能； b) 在内容过滤设备中设置了过滤规则，用户无法访问指定网络内容。	技术类
8	网络安全/网络访问控制/访问控制	必测项	a) 应对源地址、目的地址、源端口、目的端口和协议等进行检查，以允许/拒绝数据包进出； b) 网络设备和系统应有根据会话状态信息为数据流提供明确的允许/拒绝访问的能力，控制粒度为端口级； c) 应删除多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化。	a) 检查网络设备是否对源地址、目的地址、源端口、目的端口和协议等进行检查； b) 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； c) 检查是否删除了多余或无效的访问控制规则。	a) 网络设备对源地址、目的地址、源端口、目的端口和协议等进行检查； b) 网络设备提供会话控制功能，控制粒度为端口级； c) 删除了多余和无效的访问控制规则。	技术类
9	网络安全/网络访问控制/会话控制	必测项	a) 当会话处于非活跃状态，应具备超时退出机制； b) 会话结束后，应终止网络连接，释放资源。	查询网络设备（如交换机、防火墙等）的访问超时设置，使用预置用户访问网络设备登录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
10	网络安全/网络访问控制/远程访问	必测项	a) 应限制管理用户通过远程控制方式对服务器进行远程管理；	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。	a) 系统对远程访问有安全措施； b) 系统应禁止通过远程拨号方式访问主机	技术类

序号	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
	控制和记录		b) 如必须使用远程访问，应进行相关详细记录。		（如 Modem 拨号方式）； c) 如使用远程访问，有远程访问操作的详细记录。	
11	网络安全/网络安全审计/日志信息	必测项	a) 应对网络系统中的网络设备运行状况、网络流量、用户行为和重要安全事件等进行日志记录； b) 应确保日志记录的留存时间及存储空间容量符合法律法规的要求。	a) 检查网络及主机设备是否具备日志记录功能； b) 检查日志的保存时间是否满足相关法律法规的要求； c) 检查日志的保存时间及存储空间容量，是否满足相关法律法规的要求。	a) 网络及主机设备具备日志记录功能； b) 日志的保存时间满足相关法律法规的要求。	技术类
12	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。	a) 检查审计系统，查看系统的访问控制功能； b) 对比现有审计记录与系统维护记录，检查是否一致； c) 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。	a) 审计系统能提供必要的访问控制功能，并且提供 ACL 权限列表控制功能，或者审计系统能提供独立的管控环境； b) 审计记录与系统运行维护情况基本一致，未出现记录中断或明显跳跃情况； c) 低权限用户无法删除或初始化审计数据。	技术类
13	网络安全/网络安全审计/审计工具	必测项	a) 宜提供安全审计工具； b) 审计工具应提供日志规划功能、可进行分析形成审计报告； c) 网络审计工具提供自我数据保护功能。	a) 访谈网络管理员，询问是否配有网络审计工具； b) 检查网络安全审计工具状态和配置。	a) 具备安全审计工具； b) 审计服务应处于开启状态； c) 定义了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
14	网络安全/网络安全审计/	必测项	a) 应在网络边界、重要网络节点进行安全审计，审	a) 检查是否在网络边界、重要网络节点进行安全审计，检	a) 在网络边界、重要网络节点进行安全审计，审计范围应覆盖	技术类

序号	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
	网络对象操作审计		计范围应覆盖每个用户； b) 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； c) 应能对远程访问的用户行为、访问互联网的用户行为等单独进行行为审计和数据分析，并生成审计报表； d) 审计记录应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； e) 应确保审计记录的留存时间符合法律法规的要求； f) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等； g) 宜保护审计进程，避免受到未预期的中断。	查审计范围是否覆盖每个用户； b) 检查审计内容是否包括重要用户行为、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； c) 检查是否对远程访问的用户行为、访问互联网的用户行为等单独进行行为审计和数据分析，是否生成审计报表； d) 检查审计记录是否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； e) 检查审计记录的保存时间及存储空间容量，是否满足相关法律法规的要求； f) 检查是否对审计记录进行保护并定期备份。	每个用户； b) 审计系统的审计内容包括重要的用户行为、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； c) 系统对远程访问的用户行为、访问互联网的用户行为等单独进行行为审计和数据分析，具有审计报表； d) 审计记录包括了事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息； e) 应确保审计记录的留存时间及存储空间容量符合法律法规的要求； f) 系统对审计记录进行保护并定期备份。	
15	网络安全/边界完整性检查	必测项	a) 应保证跨越边界的访问和数据流通过边界防护设备提供的受控接口进行通信；	a) 访谈网络管理员，询问系统网络的外联种类有哪些（如互联网、合作伙伴企业网、上级部门	a) 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；	技术类

序号	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
			b) 应定期检查违反规定无线上网及其他违反网络安全策略的行为； c) 应能对非授权设备私自连接到内部网络的行为进行检查，并对其进行有效阻断； d) 应能对内部网络用户私自连接到外部网络的行为进行检查，并对其进行有效阻断； e) 应限制无线网络的使用，确保无线网络通过受控的边界防护设备接入内部网络。	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； b) 检查是否定期审查违反网络安全策略的上网行为； c) 访谈网络管理员，询问是否针对办公网和生产网设置了防私自接入的实时管控系统； d) 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； e) 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； f) 使用内网电脑插入移动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。	b) 定期检查违反规定无线上网及其他违反网络安全策略的行为，具有定期检查记录； c) 具有防外部设备私自接入内网的实时管控系统； d) 非授权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； e) 具有防内部设备私自连入外网的实时管控系统； f) 接入的电脑在插入移动上网卡后被管控系统发现后阻断（如实行内网接入认证、禁止多网卡接入等）。	
16	网络安全/网络入侵防范	必测项	a) 应在关键网络节点处检测、防止或限制从外部发起的网络攻击行为； b) 应在关键网络节点处检测和限制从内部发起的网络攻击行为； c) 应采取技术措施对网络行为进行分析，实现对网	a) 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攻击行为进行防范，如部署了入侵检测、流量清洗、应用防火墙等设备，询问采取什么方式进行网络入侵防范规则库升级；	a) 采用了网络入侵防范措施，如部署网络入侵防范设备等，并采取自动或手动方式对网络入侵防范规则库进行及时升级； b) 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	技术类

序号	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
			络攻击特别是新型网络攻击的检测和分析； d) 当检测到攻击行为时，记录攻击源IP、攻击类型、攻击目的、攻击时间，在发生严重入侵事件时应提供报警。	b) 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告警方式（如屏幕实时提示、Email告警、声音告警等）。	提示、Email告警、声音告警等）。	
17	网络安全/恶意代码防范/恶意代码防范措施	必测项	应具备网络防恶意代码防范措施。	a) 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么，询问防恶意代码产品有哪些主要功能； b) 检查在关键网络节点处是否有相应的防恶意代码措施。	a) 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； b) 在关键网络节点处有部署防病毒网关等产品。	技术类
18	网络安全/恶意代码防范/定时更新	必测项	a) 应具备恶意代码库更新策略（自动或定期手动更新）； b) 恶意代码库应为最新版本。	a) 访谈网络管理员，询问恶意代码库的更新策略； b) 检查防恶意代码产品，查看恶意代码库是否为最新版本。	a) 恶意代码库的更新策略为自动或定期手动更新； b) 防恶意代码产品的恶意代码库为最新版本。	技术类
19	网络安全/网络设备防护/设备登录设置	必测项	a) 应具备身份鉴别措施，不允许管理员共用账户； b) 应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和网络登录连接超时自动退出等措施； c) 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	a) 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，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； b) 登录网络设备，查看设置的用户是否有相同用户名； c) 访谈网络管理员，	a) 网络设备对登录用户进行了身份鉴别； b) 网络设备上设置的用户不存在相同的用户名； c) 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网络登录连接超时自动退出等措施； d) 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	技术类

序号	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
			来进行身份鉴别，且其中一种鉴别技术至少应使用动态口令、密码技术或生物技术来实现。	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网络登录连接超时自动退出等措施）； d) 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； e) 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。	数，网络登录连接超时时间，超时后自动退出； e) 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登录。	
20	网络安全/网络设备防护/设备登录口令安全性	必测项	a) 应具有身份鉴别信息防冒用措施； b) 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）。	a) 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）； b) 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。	a) 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； b) 2.使用双因素认证，符合本要求。	技术类
21	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。	a) 访谈网络管理员，询问网络设备的源地址是否进行了限制； b) 检查网络设备上的安全设置，查看是	网络设备中限制了源地址。	技术类

序号	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
				否对网络设备的源地址进行限制。		
22	网络安全/网络设备防护/远程管理安全	必测项	a) 网络设备远程管理应具备防窃听措施； b) 应启用网络设备远程管理防窃听措施。	a) 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； b) 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。	a) 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； b) 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
23	网络安全/网络设备防护/设备用户设置	必测项	a) 网络设备用户的标识应唯一，及时删除或停用多余的、过期的账户，避免共享账户的存在； b) 应重命名或删除默认账户，修改默认账户的默认口令。	a) 检查网络设备用户列表，查看是否有多余或过期用户，访谈网络管理员，询问是否存在共用账户； b) 检查网络设备用户列表，查看是否存在使用默认口令且未修改名称的默认账户。	a) 当前网络设备所有用户均为在用账户，无多余或过期用户，不同管理员使用不同账户； b) 网络设备中不存在使用默认口令且未修改名称的默认账户。	技术类
24	网络安全/网络设备防护/权限分离	必测项	网络设备应进行特权用户权限分离。	a) 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分离； b) 检查网络设备是否实现设备特权用户的权限分离（如每个管理员账户是否仅分配完成其任务的最小权限）； c) 检查网络设备的安全设置，验证设备特权用户的权限分	a) 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； b) 网络设备目前有不同的特权用户； c) 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

序号	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
				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）。		
25	网络安全/网络设备防护/最小化服务	必测项	a) 网络设备应实现设备的最小服务配置； b) 应对配置文件进行定期离线备份。	a) 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； b) 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（如查看离线备份记录是否定期备份）。	a) 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； b) 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
26	网络安全/网络安全管理/定期补丁安装	必测项	a) 软件版本升级前，应对重要文件进行备份； b) 应及时更新重要安全补丁。	a) 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（如账户数据、配置数据等）进行备份； b) 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）。	a) 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（如账户数据、配置数据等）进行备份； b) 及时更新重要安全补丁。	技术类
27	网络安全/网络安全管理/漏洞扫描	必测项	a) 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； b) 应对扫描发现的漏洞进行及时处	a) 访谈网络管理员，询问是否对网络设备进行过漏洞扫描（如多久一次），对扫描出的漏洞是否及时修补，使用的	a) 至少半年对网络设备进行漏洞扫描，对扫描出的漏洞进行及时修补，使用的扫描工具符合要求； b) 网络漏洞扫描报告内	技术类

序号	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
			理。	扫描工具是什么； b) 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。	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。	

8.3 主机安全性测试

验证主机安全防护能力是否符合JR/T 0122相关要求，测试内容见表6。

表 6 主机安全性测试

序号	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
1	主机安全/身份鉴别/系统与应用管理员用户设置	必测项	a) 应具备身份鉴别措施，不允许管理员共用账户； b) 主机设备不允许使用默认口令； c) 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，且其中一种鉴别技术至少应使用动态口令、密码技术或生物技术来实现。	a) 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采取何种措施实现，询问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）； b) 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UID等）； c) 测试服务器操作系统和数据库系统，当进入系统时，是否需要先进行标识（如建立账号等），没有进行标识的用户不应进入系统； d) 测试重要服务器操作	a) 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； b) 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； c) 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； d) 不能添加一个已存在的用户标识； e) 使用一种身份鉴别技术不能登录服务器操作系统和数据库系统，使用规定的组合身份鉴别技术方可登录服务器操作系统和数据库系统。	技术类

序号	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），查看是否会成功； e) 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。		
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	a) 身份鉴别信息防冒用措施； b) 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）。	a) 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； b) 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。	a) 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； b) 使用双因素认证。	技术类
3	主机安全/身份鉴别/登录策略	必测项	主机设备应提供登录失败处理功能，应采取结束会话、限制非法登录次数和登录连接超时自动退出等措施。	a) 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）； b) 检查主机设备上的安全设置，查看其是否对登录失败采取相应的措施，查看其是否设置非法登录次数，查看是否设置登录连接超时时间。	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登录连接超时自动退出等。	技术类
4	主机安全/访问控制/访问控制范围	必测项	a) 主机设备应启用访问控制功能，依据安全策略控制用户对资源访问；	a) 访谈主机管理员，询问其访问控制策略内容； b) 访谈主机管理员，询问主机设备是否实现	a) 主机设备启用访问控制功能，依据安全策略控制用户对资源的访问； b) 主机设备已实现特权	技术类

序号	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
			b) 主机设备应根据管理用户的角色分配权限，实现管理用户权限分离，仅授予管理用户所需最小权限； c) 应实现不同特权用户的权限分离； d) 应能建立一条安全的信息传输路径，对设备进行管理。	设备特权用户的权限分离； c) 检查主机设备是否实现设备特权用户的权限分离（如每个管理员账户是否仅分配完成其任务的最小权限）； d) 检查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）； e) 检查主机设备远程管理时是否使用了安全的信息传输路径。	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； c) 主机设备目前有不同的特权用户； d) 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； e) 远程管理设备时使用安全通道。	
5	主机安全/访问控制/主机信任关系	必测项	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，应避免不必要的主机信任关系。	a) 访谈主机管理员，询问主机是否启用了信任关系； b) 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表中； c) 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) 未启用非必要的主机信任关系； b) 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； c) 可信任主机间的主机A可以不用输入登录密码登录到它的可信任主机B。	技术类
6	主机安全/访问控制/默认过期账户	必测项	a) 应及时删除共用账户、过期账户、默认账户等； b) 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。	a) 访谈主机管理员，询问是否已及时删除多余的、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； b) 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存在过期的账号	a) 操作系统和数据库系统中及时删除了多余的、过期的账户，不存在过期账户、无用账户、共享账户等，修改了默认账户及口令； b) 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	技术类

序号	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
				和无用的账号等；查看设置的用户是否有相同用户名； c) 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等）；以未授权用户身份/角色访问客体，验证是否能进行访问。	用；以未授权用户身份/角色访问客体，不能进行访问。	
7	主机安全/安全审计/日志信息	必测项	a) 应对用户行为、系统资源的异常使用和重要系统命令的使用等进行日志记录； b) 应确保日志记录的留存时间符合法律法规的要求。	a) 访谈主机管理员，询问主机系统是否具备日志记录功能； b) 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； c) 检查日志的保存时间及存储空间容量，是否满足相关法律法规的要求。	a) 主机系统针对用户行为、系统资源的异常使用和重要系统命令的使用等进行日志记录，记录信息应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； b) 日志的保存时间及存储空间容量，是否满足相关法律法规的要求。	技术类
8	主机安全/安全审计/日志权限和保护	必测项	a) 应具有日志记录的存储和保护的措施； b) 应保护日志记录，避免受到未预期的删除、修改或覆盖等。	a) 访谈主机管理员，询问日志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）； b) 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、修改或覆盖日志记录； c) 测试安全审计的保护情况与要求是否一致。	a) 日志记录存储在日志服务器上，并已启用日志守护进程 syslo-gd 等； b) 用户删除、修改或覆盖日志记录失败； c) 未授权用户不能终止日志记录功能或修改其配置。	技术类

序号	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
9	主机安全/安全审计/审计工具	必测项	宜具备日志审计工具，提供对日志记录数据进行统计、查询、分析及生成审计报表的功能。	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。	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
10	主机安全/安全审计/主机对象审计	必测项	a) 审计范围应覆盖到服务器和重要客户端上的每个用户； b) 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； c) 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； d) 应确保审计记录的留存时间符合法律法规的要求； e) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等； f) 宜保护审计进程，避免受到未预期的中断。	a) 访谈主机管理员，询问主机系统是否开启了安全审计功能； b) 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； c) 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，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等； d) 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（如末端标识符等）、事件的结果等内容； e) 检查操作系统和数据库系统，在系统上以	a) 主机系统针对用户行为、系统资源的异常使用和重要系统命令的使用等进行日志记录； b) 审计范围已经覆盖到每个操作系统用户和数据库用户； c) 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、删除系统表等）、系统资源的异常使用、重要系统命令的使用等； d) 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（如末端标识符等）、事件的结果等内容； e) 安全审计记录中含有用户鉴别失败的记录； f) 系统对审计记录进行	技术类

序号	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
				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），检查安全审计的记录情况与要求是否一致； f) 检查审计日志的保存时间及存储空间容量，是否满足相关法律法规的要求。	保护并定期备份； g) 审计记录的留存时间符合法律法规的要求。	
11	主机安全/系统保护/系统备份	必测项	a) 应具有系统备份或系统重要文件备份； b) 应对备份方式、备份周期、备份介质进行要求； c) 备份应真实有效。	a) 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； b) 检查是否具有规定备份方式（如热备、冷备等）、备份周期文档； c) 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。	a) 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； b) 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； c) 备份真实有效。	技术类
12	主机安全/系统保护/磁盘空间安全	必测项	a) 应具备磁盘监控措施； b) 应对主机磁盘空间进行合理规划，确保磁盘空间使用安全。	a) 访谈主机管理员，询问是否对主机磁盘空间进行监控； b) 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。	a) 对主机磁盘空间进行监控，并提供记录； b) 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
13	主机安全/系统保护/主机安全加固	必测项	a) 应具有主机加固策略； b) 应进行过主机加固，并具备相应记录。	a) 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； b) 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人、审	a) 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； b) 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、加固策略等。	技术类

序号	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
				核人、操作时间、加固策略等。		
14	主机安全/入侵防范/入侵防范记录	必测项	a) 宜采取入侵防范措施； b) 宜能检测到对重要服务器进行入侵的行为，能记录入侵的源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； c) 宜能对系统程序、应用程序和重要配置文件/参数进行可信执行验证，并在检测到完整性受到破坏后采取恢复的措施。	a) 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； b) 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； c) 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）； d) 检查入侵攻击检测日志； e) 检查采用何种报警方式； f) 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。	a) 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等方面； b) 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； c) 在网络边界处部署了IDS或IPS系统，或UTM启用了入侵检测或保护功能； d) 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，则该项要求为不符合； e) 有入侵攻击相关日志记录； f) 在发生严重事件时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； g) 在检测到重要程序完整性受到破坏后采取一定的恢复措施，如通过定期备份的文件进行恢复。	技术类
15	主机安全/入侵防	必测项	a) 应关闭不必要的服务；	a) 访谈系统管理员，询问是否定期对系统中	a) 定期对系统中的服务和端口进行梳理，并	技术

序号	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
	范/关闭服务和端口		b) 应关闭不必要的端口。	的服务和端口进行梳理，并关闭不必要的服务和端口； b) 查看系统中已经启动的服务，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； c) 输入 netstat -an 查看系统端口开放情况； d) 采用端口扫描工具，查看是否存在不必要的服务或端口。	关闭不必要的服务和端口； b) 通过查看和扫描，系统中未发现不必要的服务和端口开启。	类
16	主机安全/入侵防范/最小安装原则	必测项	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。	a) 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。 b) 查看系统中已经启动的服务，一些不必要的服务是否已启动，输入 netstat -an 查看系统是否有不必要端口开启。 c) 针对 Windows 操作系统，查看系统默认共享的开启情况： 1) 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； 2) 依次展开[开始]	a) 系统安装的组件和应用程序遵循了最小安装的原则。 b) 系统中不必要的服务没有启动，不必要的端口没有打开。 c) 针对 Windows 操作系统，非域环境中，关闭默认共享，即： 1) “共享名”列为空，无 C$、D$、IPC$ 等默认共享； 2) HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\restrictanonymous 值不为“0”（0 表示共	技术类

序号	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
				->[运行]，在文本框中输入regedit点确定，查看HKEY_LOCAL_日志信息HINE\SYSTEM\CurrentControlSet\Co-ntrol\Lsa\res-trictanonymous值是否为“0”(0表示共享开启)。	享开启)。	
17	主机安全/恶意代码防范/防范软件安装部署	必测项	a) 应安装防恶意代码软件； b) 防恶意代码软件的部署应覆盖所有生产设备。	a) 查看系统中是否部署了防恶意代码软件； b) 访谈系统管理员，询问防恶意代码软件覆盖范围如何； c) 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。	a) 安装了防恶意代码软件； b) 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
18	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。	a) 查看系统中是否部署了防恶意代码软件； b) 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； c) 查看防恶意代码软件版本是否是最新版本，最新版本更新日期是否超过1个星期。	a) 安装了防恶意代码软件； b) 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
19	主机安全/恶意代码防范/防范软件统一管理	必测项	宜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。	防恶意代码统一管理，统一升级。	技术类
20	主机安全/连接控制	必测项	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。	a) 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	a) 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。 b) 采用了以下一种或几种措施对终端接入的	技术类

序号	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
				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。 b) 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： 1) 查看主机防火墙或系统有无限制登录地址； 2) 针对 Windows 操作系统，查看“TCP/IP 筛选”中是否对端口进行了限制； 3) 网络层面访问控制规则限制情况。	方式、网络地址范围进行了限制： 1) 通过主机防火墙的配置对登录地址进行限制； 2) 针对 Windows 操作系统，在“TCP/IP 筛选”中对端口做了限制； 3) 在网络层面通过设置访问控制规则进行限制； c) 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。	
21	主机安全/主机安全管理/漏洞扫描	必测项	a) 应至少半年对主机设备进行一次漏洞扫描，并提供扫描记录； b) 应对扫描发现的漏洞进行及时处理。	a) 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； b) 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； c) 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； d) 检查漏洞修复记录表	a) 至少半年对主机设备进行漏洞扫描，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； b) 主机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。	管理类

序号	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
				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。		
22	主机安全/主机安全管理/系统补丁	必测项	a) 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更新系统补丁； b) 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。	a) 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、安装流程等； b) 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； c) 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； d) 查看系统中系统补丁的安装情况及安装时间。	a) 具有系统补丁安装或升级策略文档，规定了补丁安装周期、安装流程等； b) 定期对系统安装补丁程序，在安装前，进行测试并备份重要文件； c) 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； d) 系统中安装较新系统补丁（参考技术检查结果）。	管理类
23	主机安全/主机安全管理/系统操作管理	必测项	a) 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； b) 应具有详细操作日志； c) 应定期对系统运行日志和审计数据进行分析； d) 应具有审计分析报告。	a) 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； b) 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）； c) 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； d) 检查是否有定期对系统运行日志和审计数据的分析报告，查看报告是否能记录账户	a) 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； b) 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； c) 定期对系统运行日志和审计数据进行分析； d) 具有定期的日志分析报告，能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	管理类

序号	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。	的失败尝试、系统错误等非正常事件。	

8.4 应用安全性测试

验证应用系统对非法访问及操作的控制能力是否符合JR/T 0122相关要求，测试内容见表7。

表7 应用安全性测试

序号	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
1	应用安全/身份鉴别/系统与普通用户设置	必测项	a) 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； b) 内部管理应用宜采用两种或两种以上的身份鉴别方式； c) 应提供系统管理员和普通用户的设置功能。	a) 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)； b) 查看内部管理系统是否采用多种身份鉴别技术； c) 验证身份鉴别模块是否有效，身份鉴别是否正确。	a) 系统提供登录模块对用户进行身份标识和鉴别； b) 内部管理系统采用两种或两种以上的身份鉴别技术(如用户/口令、数字证书、动态令牌等)； c) 系统身份鉴别模块有效，且身份鉴别结果正确。	技术类
2	应用安全/身份鉴别/登录口令安全性	必测项	a) 业务系统、管理系统应有口令长度及复杂度要求，登录口令长度应至少8位，复杂度要求应至少包含数字、字母、特殊字符中的任意两种； b) 业务系统、管理系统如提供密码初始化功能，应	a) 查看系统是否有口令长度、复杂度要求； b) 如系统提供密码初始化功能的，首次登录后查看是否要求用户修改密码； c) 查看系统是否提示用户定期修改口令； d) 查看系统是否限制系统管理用户的口令有效期； e) 查看是否采用即时加密等措施保护用户输入的鉴别信息；	a) 系统对用户口令有复杂度要求，登录口令长度应至少8位，复杂度要求应至少包含数字、字母、特殊字符中任意两种混合； b) 如系统提供密码初始化功能，用户第一次登	技术类

序号	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
			强制要求用户对初始化密码进行修改； c) 宜提示用户定期修改口令； d) 宜限制系统管理用户的口令有效期； e) 应对输入的登录口令进行安全保护，防范被窃取（如系统为内部使用，不对互联网用户提供服务，该项不适用）； f) 短信验证方式不应作为用户登录的唯一验证方式。	f) 如果允许保存身份鉴别信息，查看是否采取加密措施； g) 通过截包工具进行截包测试，查看鉴别信息是否加密传输； h) 查看系统登录时的验证方式是否唯一，如唯一不应以短信验证码为登录的验证方式。	录系统时系统强制要求用户修改初始密码； c) 系统提示用户定期修改口令； d) 系统限制系统管理用户的口令有效期； e) 支付密码等鉴别信息采用即时加密等措施防止被窃取； f) 加密保存身份鉴别信息； g) 通过截包分析，用户口令以密文方式在网络中传输； h) 不以短信验证码作为用户登录的唯一验证方式。	
3	应用安全/身份鉴别/支付密码安全性	非必测项	a) 业务系统应采用独立的支付密码进行支付； b) 应具有健全的密码重置机制； c) 应严格限制使用初始支付密码并提示客户及时修改，建立支付密码复杂度系统校验机制，避免支付密码过于简单或与客户个人信息（如出生日期、证件号码、手机号码等）相似度过高； d) 客户输入支付密	a) 查看系统是否使用独立的支付密码； b) 查看系统是否具有健全的密码重置机制； c) 查看系统是否严格限制了使用初始支付密码并提示客户及时修改，是否建立了支付密码复杂度系统校验机制，避免支付密码过于简单或与客户个人信息（如出生日期、证件号码、手机号码等）相似度过高； d) 查看对输入的支付密码或 PIN 码是否进行安全保护； e) 查看输入支付密码时，客户端是否明文显示；	a) 系统在进行支付时需要输入支付密码才能进行支付（小额免密支付除外）； b) 具有健全的密码重置机制； c) 系统严格限制使用初始支付密码并提示客户及时修改，建立支付密码复杂度系统校验机制，避免支付密码过于简单或与客户个人信息（如出生日	技术类

序号	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
			码时，客户端不应明文显示； e) 应在重置支付密码等关键操作时提供多种身份验证方式保障支付安全，并以短信、邮件等方式告知用户。	f) 查看在重置支付密码等关键操作时是否提供了多种身份验证方式保障支付安全，并以短信、邮件等方式告知用户。	期、证件号码、手机号码等）相似度过高； d) 系统采用即时加密等措施对输入的支付密码或 PIN 码进行安全保护； e) 客户端输入支付密码时，不明文显示； f) 在重置支付密码等关键操作时提供了多种身份验证方式保障支付安全，并以短信、邮件等方式告知用户。	
4	应用安全/身份鉴别/支付安全策略	必测项	a) 支付前应按照《非银行支付机构网络支付业务管理办法》对用户身份进行鉴别； b) 使用数字证书、电子签名作为身份鉴别要素的，应优先使用 SM 系列算法，并符合 GM/T 0054—2018 的相关规定，具体算法见 GB/T 32905、GB/T 32907、GB/T 32918（下同）； c) 应采用技术手段对私钥信息进行保护； d) 用户身份鉴别信	a) 查看系统采用的身份鉴别方式是否达到交易的安全级别； b) 查看数字证书、电子签名作为身份鉴别要素的，是否优先使用 SM 系列算法； c) 查看客户端对私钥信息进行保护的技术手段； d) 查看是否具有鉴别信息重置或其他技术措施保证系统安全。	a) 系统采用的身份鉴别技术达到交易的安全级别； b) 查看数字证书、电子签名作为身份鉴别要素的，优先使用 SM 系列算法； c) 客户端采用了有效的技术手段对私钥信息进行保护； d) 具有鉴别信息重置或人工找回等其他措施。	技术类

序号	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
			息丢失或失效时，应采用鉴别信息重置或其他技术措施保证系统安全。			
5	应用安全/身份鉴别/非法访问控制策略	必测项	a) 业务系统、管理系统应提供登录失败处理功能； b) 应采取结束会话、限制非法登录次数或登录连接超时自动退出等措施，并根据安全策略配置参数； c) 业务系统、管理系统应对非法访问进行警示和记录。	a) 查看系统是否提供多次登录失败处理功能，是否采取结束会话、限制非法登录次数或登录连接超时自动退出等措施，并根据安全策略配置参数； b) 查看登录错误提示是否过于详细（如错误明确提示用户名错误、密码错误等）； c) 查看系统是否对登录成功、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）。	a) 系统提供了多次登录失败处理功能； b) 系统通过结束会话、限制非法登录次数或登录连接超时自动退出等措施进行处理，并根据安全策略配置了参数； c) 系统用户名/口令错误时，系统进行了模糊提示； d) 系统对用户登录成功、失败进行了日志记录，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
6	应用安全/身份鉴别/身份标识唯一性	必测项	应提供用户身份标识唯一性检查功能，保证应用系统中不存在重复用户身份标识。	查看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）。	提供了用户身份标识唯一性检查功能。	技术类
7	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。	a) 如该系统为B/S模式，可通过下列步骤进行测试： 1) 登录系统，并复制某功能模块URL； 2) 正常退出后，通过	a) 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	技术类

序号	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
				浏览器访问该URL，查看是否可以访问并继续进行操作； 3) 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继续进行操作。 b) 如该系统为C/S模式，模拟正常、非正常退出系统，查看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。	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； b) 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。	
8	应用安全/WEB页面安全/登录防穷举	必测项	a) 业务系统应提供登录防穷举的措施，如图片验证码等； b) 登录失败后图形验证码应能自动更换； c) 图形验证码应具备一定的复杂度，防止能轻易地被自动化工具识别； d) 如系统为内部使用，不对互联网用户提供服务，该项不适用； e) 若有其他安全登录措施，如客户端扫码登录等，可视为满足该项要求。	a) 查看是否提供图形验证码等机制防范对用户名、口令穷举攻击； b) 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； c) 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。	a) 系统使用图形验证码等技术防范登录穷举； b) 图形验证码在登录失败后自动更换； c) 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
9	应用安全/WEB页面	必测项	业务系统、管理系统应无SQL注入、Path注入	通过Web扫描软件及手工测试，查看系统是否存在SQL注	通过Web扫描软件及手工测试，未发现系	技术

序号	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/网站页面注入防范		和LDAP注入等漏洞。	入、Path注入和LDAP注入等漏洞。	统存在SQL注入、Path注入和LDAP注入等漏洞。	类
10	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
11	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
12	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（如系统为内部使用，不对互联网用户提供服务，该项不适用）。	a) 检查网站是否存在黑客挂马情况； b) 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。	a) 通过检测，未发现系统存在黑客挂马情况； b) 通过检测，未发现网站存在被黑客挂马的风险。	技术类
13	应用安全/WEB页面安全/网站页面防篡改措施	必测项	宜采取网站页面防篡改措施（如系统为内部使用，不对互联网用户提供服务，该项不适用）。	a) 访谈系统管理员，询问是否采取了网站页面防篡改措； b) 查看系统是否使用了网页防篡改系统。	a) 采取了网站页面防篡改措施； b) 系统使用了网页防篡改系统防止黑客挂马。	技术类
14	应用安全/WEB页面安全/网站页面防钓鱼	必测项	a) 网站页面宜支持用户设置预留防伪信息； b) 防伪信息应能正确显示； c) 如系统为内部使用，不对互联网用户提供服务，该项不适用。	a) 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； b) 查看是否具有预留防伪信息功能，并尝试对其进行配置； c) 查看用户登录后是否能正确显示预留的防伪信息。	a) 网站支持用户设置预留防伪信息； b) 防伪信息能正确显示。	技术类
15	应用安全/WEB页面安全/漏洞扫描	必测项	a) 应至少半年对应用系统进行一次漏洞扫描，并提供扫描记录；	a) 访谈系统管理员，询问扫描方式、扫描频率等； b) 查看漏洞扫描报告是否无误。	a) 至少半年对应用系统进行了漏洞扫描，并会对扫描出的漏	技术类

序号	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
			b) 应对发现的WEB应用、中间件等安全漏洞及时进行修补。		洞进行了及时修补，使用的扫描工具符合要求； b) 应用系统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。	
16	应用安全/访问控制/访问权限设置	必测项	a) 应提供访问控制功能，依据安全策略控制用户对文件、数据库表等客体的访问； b) 应由授权主体配置访问控制策略，并严格限制默认账户的访问权限； c) 应授予不同用户为完成各自承担任务所需的最小权限，并在它们之间形成互相制约的关系； d) 应及时删除或停用多余的、过期的账户，避免共享账户的存在。	a) 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哪些，访问控制的粒度如何； b) 查看应用系统的访问控制粒度是否达到主体为用户级、客体为文件、数据库表级，查看其是否由授权账户设置其他账户访问系统和数据的权限，是否限制默认账户的访问权限； c) 查看应用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，特权账户的权限是否分离，权限之间是否相互制约； d) 测试应用系统，可通过以不同权限的账户登录系统，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； e) 测试应用系统，可通过以默认账户登录系统，并进行一些合法和非法操作，	a) 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； b) 访问控制措施由授权主体设置，并限制了默认账户的访问权限； c) 各账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； d) 系统不存在多余的、过期的账户，无共享账户的存在。	技术类

序号	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
				验证系统是否严格限制了默认账户的访问权限； f) 验证是否能限制低权限账户登录后通过URL直接跳转到高权限账户的操作。		
17	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。	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
18	应用安全/访问控制/业务操作日志	必测项	应提供业务操作日志。	a) 访谈安全审计员，系统是否具备业务操作日志； b) 查看应用系统是否记录了业务操作日志； c) 测试应用系统，可通过业务操作产生相关审计日志，并查看记录是否正确。	系统具有对所有业务操作进行日志记录的功能。	技术类
19	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。关键数据包括敏感数据、重要业务数据、系统管理数据等。	a) 访谈系统管理员，询问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； b) 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
20	应用安全/安全审计/日志信息	必测项	a) 应具备安全审计功能； b) 应对业务系统和管理系统的重要用户行为、支付标记化行为、系统资源的异常使用和重要系统命令的使用等进行日志记录。	a) 访谈安全审计员，询问应用系统是否有安全审计功能； b) 查看应用系统审计记录信息是否包括重要用户行为、支付标记化行为、系统资源的异常使用和重要系统命令的使用等内容。	a) 系统具备安全审计功能； b) 审计记录信息包括了重要用户行为、支付标记化行为、系统资源的异常使用和重要系统命令的使用等内容。	技术类
21	应用安全/安全审	必测项	a) 应对日志记录进行保护，避免受	a) 访谈安全审计员，询问对日志的保护措施有哪些；	a) 无法单独中断日志进程；	技术

序号	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
	计/日志权限和保护		到未预期的删除、修改或覆盖等； b) 宜保证无法单独中断日志进程。	b) 通过非审计员的其他账户试图中断日志进程，验证日志进程是否受到保护； c) 验证是否无法非授权删除、修改或覆盖日志记录。	b) 提供了日志记录保护措施，无法删除、修改或覆盖日志记录； c) 日志数据进行了备份。	类
22	应用安全/安全审计/审计工具	必测项	宜具备日志审计工具，提供对日志记录数据进行统计、查询、分析及生成审计报表的功能。	a) 访谈系统管理员，询问是否配有系统审计工具； b) 检查系统安全审计工具状态和配置； c) 查看审计工具是否能提供对日志记录数据进行统计、查询、分析及生成审计报表的功能。	a) 具备安全审计工具； b) 审计服务处于开启状态； c) 审计工具能提供对日志记录数据进行统计、查询、分析及生成审计报表的功能。	技术类
23	应用安全/安全审计/应用操作审计	必测项	a) 应提供覆盖到应用系统每个用户的安全审计功能； b) 审计内容应包括用户重要行为和异常行为等系统内重要的安全相关事件； c) 审计记录应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； d) 宜保护审计进程，避免受到未预期的中断。	a) 查看应用系统当前审计范围是否覆盖到每个用户； b) 查看应用系统审计策略是否覆盖系统内重要的安全相关事件，如用户标识与鉴别、访问控制操作记录、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； c) 查看审计记录是否至少包括了事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息； d) 查看应用系统是否采取措施保护审计进程。	a) 审计范围覆盖到每个用户； b) 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、访问控制操作记录、用户重要行为和异常行为等； c) 审计记录包括了事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息； d) 采取了措施保护审计进程，避免受到未预期的中断。	技术类
24	应用安全/剩余信	必测项	应对无用的过期信息、文档进行完整删除。	测试应用系统，用某用户登录系统并进行操作后，在该用户	a) 能对无用、过期信息和文档进	技术

序号	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
	息保护			退出后用另一用户登录，试图操作（如读取、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，以确保系统内的文件、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整清除。	行完整删除； b) 采取了技术手段对剩余信息进行保护。	类
25	应用安全/资源控制/连接控制	必测项	a) 宜能根据业务需求，对系统的最大并发会话连接数进行限制； b) 宜能对一个时间段内可能的并发会话连接数进行限制。	a) 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； b) 查看应用系统是否有最大并发会话连接数的限制。	a) 实现了最大并发会话连接数限制； b) 对一段时间内的可能并发会话连接数进行了限制。	技术类
26	应用安全/资源控制/会话控制	必测项	a) 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，另一方应能自动结束会话； b) 应能对单个账户的多重并发会话进行限制； c) 会话标识应唯一、随机、不可猜测； d) 会话过程中应维持登录认证状态，防止信息未经授权访问； e) 应用审计日志宜记录暴力破解会话令牌的事件。	a) 查看应用系统是否限制了单个账户的多重并发会话； b) 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，验证系统是否能正确地限制单个账户的多重并发会话数； c) 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，查看另一方是否能自动结束会话； d) 验证会话标识是否唯一、随机、不可猜测； e) 查看会话过程中是否维持了登录认证状态，防止信息未经授权访问； f) 查看应用审计日志是否记录了暴力破解会话令牌的事件。	a) 会话超时会自动结束会话； b) 限制了单个用户的多重并发会话； c) 会话标识唯一、随机、不可猜测； d) 会话过程中维持了登录认证状态，防止了信息未经授权访问； e) 应用审计日志记录了暴力破解会话令牌的事件。	技术类

序号	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
27	应用安全/资源控制/进程资源分配	必测项	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。	查看应用系统是否能根据安全策略设定主体的服务优先级，并根据优先级分配系统资源。	提供了服务优先级设定功能，并在安装后根据安全策略设定了访问用户或请求进程的优先级，根据优先级分配了系统资源。	技术类
28	应用安全/应用容错/数据有效性校验	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及长度符合系统设定要求。	a) 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； b) 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； c) 可通过对人机接口输入不同长度、格式的数据，查看应用系统的反应，验证系统人机接口有效性检验功能是否正确。。	对通过人机接口输入或通过通信接口输入的数据格式及长度进行了严格限制。	技术类
29	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，保证系统能进行恢复。	查看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
30	应用安全/抗抵赖/时间同步机制	必测项	系统时间应由系统范围内唯一确定的时钟产生，本地时间宜从国家权威时间源采时，保证时间的同一性。	a) 访谈管理员，询问系统是否有时间同步机制； b) 抽查系统服务器验证时间是否同步，是否从国家权威时间源采时。	系统采取了时间同步机制，服务器时间与国家权威时间源相同。	技术类
31	应用安全/编码安全/源代码审查	必测项	a) 应对源代码进行安全性审查； b) 应能提供源代码审查证据。	a) 访谈安全员，询问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； b) 查看源代码安全性审查报告； c) 查看相关审查文档和证据，查看是否通过自动化工具实现了源代码安全	a) 实现了对源代码的安全性审查，并具有安全性审查报告； b) 采用了恰当的方法对源代码安全进行审查。	技术类

序号	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
				审查。		
32	应用安全/编码安全/插件安全性审查	非必测项	a) 应对插件进行安全性审查； b) 应能提供插件审查报告。	a) 访谈安全员，询问是否针对插件进行了安全性审查； b) 查看插件安全性审查报告无误。	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
33	应用安全/编码安全/编码规范约束	非必测项	a) 应具有编码规范约束制度； b) 应按照编码规范进行编码。	a) 访谈安全员，询问是否编制了编码安全规范； b) 查看相关记录和文档，验证是否按照规范执行。	具有编码规范，并严格按照编码规范执行。	技术类
34	应用安全/编码安全/源代码管理	必测项	a) 应具备源代码管理制度； b) 应具备源代码管理记录，在每次源代码变更时，需填写变更备注信息。	a) 访谈安全员，询问是否编制了源代码管理制度； b) 查看是否按照制度执行，是否产生相关管理记录。	a) 具有源代码管理制度； b) 具有源代码管理记录。	技术类
35	应用安全/电子认证应用/数字证书	必测项	a) 在外部业务处理过程中，应使用第三方电子认证服务生成的数字证书或经国家有关管理部门许可的电子认证服务生成的数字证书； b) 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，可使用自建的电子认证服务生成的数字证书； c) 电子认证应优先使用SM系列算法。	a) 访谈安全员，询问外部业务处理过程中，是否使用第三方电子认证服务生成的数字证书或经国家有关管理部门许可的电子认证服务生成的数字证书； b) 访谈安全员，询问在内部业务（仅涉及本机构内人员或设备的业务）处理过程中，是否使用了数字证书； c) 访谈安全员，询问电子认证是否优先使用SM系列算法的。	a) 在外部业务处理过程中，使用了第三方电子认证服务生成的数字证书或经国家有关管理部门许可的电子认证服务生成的数字证书； b) 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，使用了数字证书； c) 优先使用了SM系列算法的电子认证服务生成的数字证书。	技术类
36	应用安全/电子认	必测项	a) 在外部关键业务处理过程中（包	a) 访谈应用系统管理员，询问外部关键业务（如支	a) 外部关键业务处理（如支付、	技术

序号	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
	证应用/电子认证		含但不限于支付、转账等），应使用经过国家有关管理部门许可的电子认证服务； b) 电子认证应优先使用 SM 系列算法。	付、转账等）处理过程中是否采用经过国家有关管理部门许可的电子认证服务； b) 访谈应用系统管理员，询问电子认证是否优先使用 SM 系列算法。	转账等）过程中采用了经过国家有关管理部门许可的电子认证服务； b) 电子认证服务优先使用了 SM 系列算法。	类
37	应用安全/电子认证应用/电子认证证书私钥保护	必测项	应对所持有的电子认证证书私钥进行有效保护。	a) 访谈应用系统管理员，询问支付系统采用了何种电子认证证书密钥系统，其私钥保存在哪些服务器上； b) 查看对私钥有哪些保护措施。	a) 电子认证证书私钥存放在服务器上； b) 采取有效措施对私钥进行了保护（如严格控制访问权限、加密等）。	技术类
38	应用安全要求审查/脱机数据认证/密钥和证书	脱机交易类必测项	应符合 JR/T 0025.7—2018 中 5.2 的规定，生成符合业务要求的密钥和证书。	a) 访谈开发人员，询问是否按照 JR/T 0025.7—2018 中 5.2 的规定生成密钥和证书； b) 查看卡片认证证书。	a) 密钥和证书的生成按照 JR/T 0025.7 — 2018 中 5.2 的的规定执行； b) 具有卡片认证证书。	管理类
39	应用安全要求审查/脱机数据认证/数据认证	脱机交易类必测项	应采用静态数据认证、动态数据认证或复合动态数据认证的方式。	访谈开发人员，询问脱机交易采用何种数据认证方式；	脱机交易采用静态数据认证、动态数据认证或复合动态数据认证的方式。	管理类
40	应用安全要求审查/安全报文/报文格式	必测项	报文格式应符合 JR/T 0025.7 — 2018 中 7.2 的规定。	查看报文格式是否符合 JR/T 0025.7—2018 中 7.2 的规定。	报文格式符合 JR/T 0025.7—2018 中 7.2 的规定。	管理类
41	应用安全要求审查/安全报文/报文完整性验证	必测项	应对报文完整性进行验证。	a) 查看开发文档中的报文完整性校验方式； b) 验证报文完整性校验的正确性。	a) 报文经过完整性校验； b) 报文完整性校验正确。	管理类

序号	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
42	应用安全要求审查/安全报文/报文私密性	必测项	应保证报文私密性。	a) 查看开发文档中的报文格式要求和报文加密方式； b) 查看报文是否对敏感信息进行加密。	a) 报文格式符合要求； b) 报文中对敏感信息进行加密。	管理类
43	应用安全要求审查/安全报文/密钥管理	必测项	应对密钥进行安全管理。	查看密钥管理制度中是否对密钥管理进行规定。	密钥管理制度中包括对密钥的管理要求（如密钥生成、使用、销毁等）。	管理类
44	应用安全要求审查/终端安全/终端数据安全性要求	必测项	应符合JR/T 0025.7—2018中9.1的规定。	查看金融行业检测机构出具的终端安全检测报告。	终端安全检测报告中说明终端数据安全性符合JR/T 0025.7—2018中9.1的规定。	管理类
45	应用安全要求审查/终端安全/终端设备安全性要求	必测项	应符合国家相关标准，并提供金融行业检测机构出具的安全检测报告。	查看金融行业检测机构出具的终端安全检测报告。	具有金融行业检测机构出具的终端安全检测报告。	管理类
46	应用安全要求审查/终端安全/终端密钥管理要求	必测项	应符合国家相关标准，并提供金融行业检测机构出具的安全检测报告。	查看金融行业检测机构出具的终端安全检测报告，终端密钥管理是否符合国家相关标准。	具有金融行业检测机构出具的终端安全检测报告，终端密钥管理符合国家相关标准。	管理类

8.5 数据安全性测试

验证数据安全防护能力是否符合JR/T 0122相关要求，测试内容见表8。

表8 数据安全性测试

序号	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
1	数据安全/数据保护/敏感信息安全管理制度	必测项	a) 应具备支付敏感信息保护的相关管理制度； b) 在管理制度中应明确支付敏感信	a) 访谈相关管理员，询问是否制定了对支付敏感信息保护的相关管理制度； b) 在所提供的相关管理	a) 机构制定了相关支付敏感信息保护的管理制度； b) 在相关管理制度中规定了支付敏	管理类

序号	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
			息定义； c) 在制度中应明确规定严禁留存非本机构的支付敏感信息（包括银行卡磁道或芯片信息、卡片验证码、卡片有效期、银行卡密码、网络支付交易密码等），确有必要留存的应取得客户本人及账户管理机构的授权。	制度中，是否包括了支付敏感信息的定义、保存方式、保存时间等； c) 在系统中验证是否留存非本机构的支付敏感信息，确有必要留存的应取得客户本人及账户管理机构的授权。	感信息的定义、保存方式、保存时间等； c) 在系统未留存非本机构的支付敏感信息，确有必要留存的应取得客户本人及账户管理机构的授权。	
2	数据安全/数据保护/敏感信息安全审计	必测项	每年应至少开展两次支付敏感信息安全的内部审计，并形成报告存档备查。	检查审计报告。	每年至少开展了两次支付敏感信息安全的内部审计。	技术类
3	数据安全/数据完整性/重要数据更改机制	必测项	a) 应具有重要数据的更改管理制度； b) 应具有重要数据的更改流程； c) 应具有重要数据的更改记录。	a) 访谈系统管理员，询问对重要数据的更改是否有相关管理制度，在管理制度中是否定义了相关的更改流程； b) 检测部分重要数据的更改记录。	a) 制定了重要数据的更改管理制度； b) 具有重要数据的更改记录。	管理类
4	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	a) 应在数据传输过程中使用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； b) 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时，应采取数据恢复措施； c) 完整性校验应优	a) 访谈系统开发人员，询问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； b) 访谈系统开发人员，询问数据传输通过何种手段验证接收到的数据的完整性； c) 访谈系统开发人员，询问当数据传输中断或者接收的数据受到	a) 系统数据传输过程中使用的通讯协议或安全通讯协议服务能保证数据传输的完整性； b) 系统能验证接收到的数据的完整性； c) 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，	技术类

序号	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
			先使用SM系列算法。	篡改导致完整性校验失败时，采用何种机制进行数据恢复； d) 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性； e) 查看完整性校验是否优先使用了SM系列算法。	系统能进行数据恢复； d) 系统接收到的通过并发方式传输的同类型/不同类型数据均完整； e) 完整性校验优先使用SM系列算法，并符合GM/T 0054—2018的相关规定。	
5	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	a) 应具备高可用性的数据物理存储环境； b) 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实时无缝切换。	a) 访谈系统管理员，询问系统备份策略（如是否每天进行备份，备份介质是否场外存放）； b) 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； c) 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
6	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	a) 应不允许保存非必需的客户身份认证信息（银行卡磁道信息或芯片信息、卡片验证码、卡片有效期、银行卡交易密码、指纹、CVN、CVN2、非本机构的网络支付交易密码等）； b) 应对客户的其他敏感信息（如口令、身份证号、卡	a) 查看开发文档中的数据词典，验证数据库中是否存在非必需客户身份认证信息； b) 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非必需信息； c) 按照开发文档，在系统中对客户身份认证信息进行验证，查看系统是否保存了非必需的客户身份认证信	a) 在对客户身份认证的过程中不保存非必需的客户身份认证信息； b) 通过抓取系统数据分析系统不保存非必需的客户身份认证信息； c) 数据库对客户的其他敏感信息进行了加密存储； d) 系统对客户的其他敏感信息进行了屏蔽处理；	技术类

序号	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
			号、手机号、经授权的贷记卡有效期、电子邮箱、身份证影印件等）采取加密等保护措施，显示时应进行屏蔽处理，防止未经授权擅自对个人信息进行查看、篡改和泄露； c) 数据加密应优先使用SM系列算法。	息； d) 查看数据库是否对客户的其他敏感信息进行了加密存储； e) 查看系统是否对客户的其他敏感信息进行了屏蔽显示； f) 查看是否优先使用SM系列算法进行数据加密。	e) 优先使用了SM系列算法进行数据加密。	
7	数据安全/交易数据以及客户数据的安全性/个人信息保护	必测项	a) 应仅采集和保存业务必需的用户个人信息； b) 应仅允许授权的访问和使用用户个人信息； c) 应在修改个人信息等关键操作时提供多种身份验证方式保障个人信息安全，并以短信、邮件等方式告知用户。	a) 检查是否具有个人信息保护制度； b) 检查是否采集和保存了业务非必需的用户个人信息； c) 检查是否仅允许授权的访问和使用用户个人信息； d) 查看系统是否在修改个人信息等关键操作时提供多种身份验证方式保障。	a) 具有完善的个人信息保护制度，对个人信息的采集、存储、使用、传输等进行了规定； b) 仅采集和保存业务必需的用户个人信息； c) 仅允许授权的访问和使用用户个人信息； d) 在修改个人信息等关键操作时提供多种身份验证方式保障。	管理类
8	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。	a) 访谈系统开发方，询问系统是否具有安全级别的划分； b) 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； c) 验证相同安全保护级别之间数据是否可以互相传输。	a) 系统具有安全级别的划分； b) 系统禁止数据从高安全保护级别向低安全保护级别传输； c) 相同安全保护级别之间数据可以互相传输。	技术类
9	数据安全/交易数据以及客户	必测项	a) 应能识别系统管理数据、鉴别信息和重要业务数据；	a) 访谈系统开发人员，询问目前系统有哪些系统管理数据、鉴别	a) 系统管理数据、鉴别信息和重要业务数据的分类全	技术类

序号	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
	数据的安全性/加密传输		b) 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； c) 数据加密传输应优先采用SM系列算法。	信息和重要业务数据，其对系统管理数据、鉴别信息和重要业务数据的分类是否全面； b) 访谈系统开发人员，询问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； c) 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； d) 查看数据加密传输是否优先采用SM系列算法。	面； b) 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进行加密； c) 数据加密传输优先采用SM系列算法。	
10	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	a) 应能识别系统管理数据、鉴别信息和重要业务数据； b) 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； c) 数据加密存储应优先采用SM系列算法。	a) 访谈系统开发人员，询问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； b) 访谈系统开发人员，询问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； c) 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； d) 查看数据加密存储是否优先采用SM系列算法。	a) 系统管理数据、鉴别信息和重要业务数据的分类全面； b) 对系统管理数据、鉴别信息和重要业务数据的加密存储； c) 数据加密存储优先采用SM系列算法。	技术类

序号	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
11	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	a) 应采取对重要数据访问控制的管理制度； b) 应具备重要数据访问控制的记录。	a) 访谈系统管理员，询问是否采取对重要数据访问控制的管理制度； b) 查看重要数据访问控制的访问记录； c) 访谈系统管理员，询问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。	a) 有重要数据的访问控制管理措施和相关记录； b) 采取了较全面的技术手段对重要数据进行控制。	技术类
12	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	a) 支付系统应有实时在线的存储备份设备； b) 实时在线的存储备份设备应能正常运行。	a) 实地考察系统中是否有实时在线的存储备份设备； b) 由系统管理员现场操作验证实时在线存储备份系统是否能正常运行。	实时在线备份系统正常运行。	技术类
13	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	a) 应根据数据的重要性和数据对系统运行的影响，制定数据的备份和恢复策略； b) 应明确备份数据合理的备份范围、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）、存储介质、保存期、放置场所、文件命名规则、介质替换频率和数据传输方法等； c) 应采用合理的数据备份方式； d) 应具有数据备份记录。	a) 访谈数据库管理员或者系统管理员，询问是否根据数据的重要性和数据对系统运行的影响，制定了数据备份的相关管理制度； b) 在数据备份管理制度中是否对备份范围、备份方式、备份频度、存储介质、保存期、放置场所、文件命名规则、介质替换频率和数据传输方法等进行说明； c) 检查是否按照管理制度所规定的流程和内容进行备份； d) 检查数据备份记录是否完整。	a) 根据数据的重要性和数据对系统运行的影响，制定了相关的备份管理制度，而且内容全面； b) 备份制度执行情况良好，具有备份记录。	管理类
14	数据安全/交易数据以及客户	必测项	a) 应提供本地数据备份； b) 应具备机房数据	a) 在机房内现场查看是否有本地备份的设备；	在机房内提供了本地备份设备并能有效运行。	技术类

序号	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
	数据的安全性/本地备份		备份设施； c) 对于采用异地多中心多活等方式的大型机构不适用。	b) 由现场管理人员操作验证设备是否正常运行。		
15	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	a) 应提供异地备份的功能或者设备； b) 应具有异地备份的网络或者线路； c) 应能成功进行异地备份。	a) 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； b) 按照备份的管理制度检查最近的异地备份是否符合要求。	a) 提供了异地备份场地和设备； b) 异地备份设备能有效的进行备份。	技术类
16	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	a) 应制定备份数据恢复操作手册； b) 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； c) 应对系统数据备份方式、数据保存的格式进行要求； d) 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； e) 本地备份数据和异地备份数据应能正常恢复； f) 应进行定期数据备份恢复性测试并记录。	a) 访谈数据备份管理员，询问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； b) 访谈系统开发人员，询问数据备份采用何种方式，备份文件采用何种格式保存； c) 访谈系统管理人员，询问数据备份的周期、是否定期验证备份数据的有效性； d) 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正常恢复； e) 现场查看备份数据恢复的操作记录是否完备。	a) 制定了备份数据恢复操作手册，并且内容全面，符合要求； b) 系统数据定期进行备份，并对备份数据进行有效性验证； c) 恢复操作记录完备； d) 恢复设备工作正常。	技术类
17	数据安全/交易数据以及客户数据的安全性/数据	必测项	a) 应制定数据销毁制度，内容应包括数据销毁范围、介质销毁方法、记录模板、监督机制	a) 访谈数据管理人员，询问是否制定了数据销毁管理制度； b) 数据销毁管理制度内容是否全面；	数据销毁管理制度内容全面，并有相关的记录。	管理类

序号	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
	销毁		等； b) 应具有数据销毁记录。	c) 检查最近数据销毁记录。		
18	数据安全/交易数据以及客户数据的安全性/数据使用	必测项	a) 开发环境和测试环境应与实际运行环境物理分离； b) 开发环境不应使用生产数据，测试环境使用的生产数据应进行脱敏处理。	a) 检查开发环境、测试环境是否与生产环境物理分离； b) 检查开发环境是否使用了生产环境数据； c) 如测试环境使用了生产环境数据，检查是否对数据进行了脱敏处理。	a) 开发和测试环境与实际运行环境物理分离； b) 开发环境未使用生产数据； c) 测试环境如果使用了生产数据，使用前由安全管理员对数据进行了脱敏处理。	技术类

8.6 运维安全性测试

验证运维安全管理制度及运维安全执行情况是否符合JR/T 0122相关要求，测试内容见表9。

表9 运维安全性测试

序号	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
1	运维安全/环境管理/机房基础设施定期维护	必测项	a) 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； b) 应对机房的温度、湿度、防火、防盗、供电、线路、整洁等进行规范化管理。	a) 访谈机房管理员，询问是否制定了机房的相关管理制度； b) 现场在机房考察是否有机房值班人员值守； c) 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。	a) 制定了机房的相关管理制度 b) 机房有专门的值班人员进行值守； c) 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
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	应制定机房出入管理制度，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。	a) 访谈机房管理员，询问是否制定了机房出入管理制度； b) 检查机房进出是否有申请和审批流程，是否有相关的记录。	a) 制定了机房的出入管理制度； b) 制定了机房出入的申请和审批流程，并有相关记录。	管理类
3	运维安全/环境管理/办公环境的保密性措施	必测项	a) 应规范人员转岗、离岗过程； b) 外部人员访问受控区域前应先提出书	a) 访谈管理人员，询问是否制定了人员辞职和转岗的相关管理制度；	a) 制定了人员辞职和转岗的相关管理制度； b) 外部人员访问受	管理类

序号	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
			面申请，批准后由专人全程陪同或监督，并登记备案； c) 应加强对办公环境的保密性管理，规范办公环境中的人员行为； d) 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质文件等。	b) 外部人员访问受控区域是否制定了审批流程，是否有专人陪同； c) 是否制定了工作人员的工作规范文档。	控区域有审批流程，并有专人陪同； c) 制定了工作人员的工作规范文档。	
4	运维安全/环境管理/机房安全管理制度	必测项	a) 人员进入机房应填写登记表； b) 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。	a) 访谈机房管理人员，询问是否制定了机房管理制度； b) 查看是否有关于机房内的设备带进、带出和操作等的管理规定； c) 查看对机房内的设备是否有视频监控或者红外监控等监控手段； d) 检查对机房内的设备操作是否有监控或者记录。	a) 制定了机房的管理制度； b) 具有对机房内设备操作的相关记录。	管理类
5	运维安全/环境管理/机房进出登记表	必测项	a) 应具有人员进出登记表； b) 应具有设备进出登记表。	检查人员进出登记表和设备进出登记表是否记录完整。	对人员和设备的进出都进行了详细的记录。	管理类
6	运维安全/介质管理/介质的存放环境保护措施	必测项	a) 应制定介质管理制度，规范对各类介质的使用控制、保护以及存放环境的要求； b) 应由专人对介质进行管理；	a) 访谈管理人员，询问是否制定了介质管理制度，是否对各类介质的使用控制、保护以及存放环境作出了要求；	a) 制定了介质管理制度，规范了各类介质的使用控制、保护以及存放环境的要求； b) 由专人对介质进	管理类

序号	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
			c) 应对介质的使用、维护进行登记。	b) 访谈管理人员，询问是否由专人对介质进行管理； c) 访谈管理人员，询问是否对介质的使用、维护进行登记。	行管理； c) 对介质的使用、维护进行登记。	
7	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。	a) 访谈管理人员，询问是否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； b) 查看介质安全管理记录是否完整。	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
8	运维安全/介质管理/介质的维修或销毁	必测项	a) 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； b) 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。	a) 访谈管理人员，询问是否有介质送出的审批流程，在审批流程中是否有对数据密级要求、清除方法进行说明； b) 检查审批流程的相关记录，并查看最近的维修记录； c) 访谈管理人员，询问是否具有对保密性较高介质的销毁审批流程，是否有相关的记录。	a) 制定了介质外出审批流程和维修记录； b) 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
9	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	a) 查看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	a) 介质在物理传输过程中对人员选择、打包、交付等情况有控制措	管理类

序号	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，并根据存档介质的目录清单定期盘点。	包、交付等情况的控制措施，并有相关的记录； b) 检查是否具有介质的归档和查询记录； c) 检查存档介质的清单，是否有定期盘点记录。	施； b) 对归档查询等操作进行了登记； c) 有存档介质清单，并进行定期盘点，有盘点记录。	
10	运维安全/介质管理/介质的分类与标识	必测项	a) 重要介质中的数据和软件应采用加密存储； b) 应按照重要程度对介质进行分类和标识。	a) 访谈管理人员，询问对介质的分类和标识是否制定了相应的管理制度； b) 检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
11	运维安全/设备管理/设备管理的责任部门或人员	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，询问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。	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。	管理类
12	运维安全/设备管理/设施、设备定期维护	必测项	a) 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； b) 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。	a) 访谈管理人员，询问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； b) 检查是否建立配套设施、软硬件维护方面的管理制度，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。	a) 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； b) 建立了配套设施、软硬件维护方面的管理制度，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。	管理类
13	运维安全/设备管理/设备管理制	必测项	a) 应建立基于申报、审批和专人负责的设备管理制度，对信息	a) 检查是否建立基于申报、审批和专人负责的设备管理制度，	a) 建立了基于申报、审批和专人负责的设备管理	管理类

序号	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
	度		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； b) 新购置的设备应经过测试，测试合格后方能投入使用。	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； b) 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。	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了规范化管理； b) 有新购置设备的测试记录，测试合格后投入使用。	
14	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，询问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。	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
15	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，询问是否对终端计算机、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，按操作规程实现设备（包括备份和冗余设备）的启动/停止、加电/断电等操作。	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了规范化管理，按操作规程执行设备（包括备份和冗余设备）的启动/停止、加电/断电等操作。	管理类
16	运维安全/设备管理/设备的操作日志	必测项	a) 应具有完整的设备操作日志； b) 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)。	a) 检查设备操作日志是否完善； b) 检查设备故障处理流程是否合理有效，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。	a) 设备操作日志完善； b) 设备故障处理流程合理有效，故障日志中包含了故障发生的时间、范围、现象、处理结果和处理人员等内容。	管理类
17	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
18	运维安全/人员管理/人员录用	必测项	a) 应指定或授权专门的部门或人员负责人员录用； b) 应严格规范人员录用过程，对被录用人	a) 访谈管理人员，询问是否指定或授权了专门的部门和人员负责人员录用； b) 访谈录用负责人员，	a) 指定或授权了专门的部门和人员负责人员录用； b) 严格规范了人员录用过程，对被	管理类

序号	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； c) 应签署保密协议； d) 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。	询问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； c) 检查录用人员考核记录和保密协议； d) 访谈录用负责人员，询问是否从内部人员中选拔从事关键岗位的人员，是否签署岗位安全协议，查看岗位安全协议内容。	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； c) 有录用人员考核记录和保密协议； d) 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。	
19	运维安全/人员管理/安全管理岗位设置	必测项	a) 应成立指导和管理信息安全工作的委员会或领导小组，其最高领导由单位主管领导委任或授权； b) 应设立信息安全管理工作的职能部门，设立安全主管、安全管理各个方面的负责人岗位，并定义各负责人的职责； c) 应设立网络管理员、主机管理员、数据库管理员、安全管理员等岗位，并定义部门及各个工作岗位的职责。	a) 访谈安全负责人，询问是否成立了指导和管理信息安全工作的委员会或领导小组； b) 访谈安全负责人，询问是否设立了信息安全管理工作的职能部门，是否设立了安全主管、安全管理各个方面的负责人岗位，并访谈各个岗位负责人； c) 检查是否设立了网络管理员、主机管理员、数据库管理员、安全管理员等岗位； d) 检查是否定义各部门及各个工作岗位的职责。	a) 成立了指导和管理信息安全工作的委员会或领导小组； b) 设立了信息安全管理工作的职能部门，设立了安全主管、安全管理各个方面的负责人岗位，并定义各负责人的职责； c) 设立了网络管理员、主机管理员、数据库管理员、安全管理员等岗位； d) 定义了各部门及各个工作岗位的职责。	管理类
20	运维安全/人员管理/安全管理人	必测项	a) 应配备一定数量的网络管理员、主机管理员、数据库管理	a) 检查是否配备了一定数量的网络管理员、主机管理员、数	a) 配备了专职的网络管理员、主机管理员、数据库	管理类

序号	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
	员配备		员、安全管理员等； b) 应配备专职的安全管理人员，不可兼任； c) 应划分各管理员角色，明确各个角色的权限、责任和风险，权限设定应遵循最小授权原则。	据库管理员、安全管理员等，至少满足AB角要求； b) 检查是否有专职安全管理员； c) 检查是否划分各管理员角色，是否明确了各个角色的权限、责任和风险； d) 检查权限设定是否遵循最小授权原则。	管理员、安全管理员等，至少满足AB角要求； b) 有专职的安全管理员； c) 划分了各个角色权限和职责，权限设定遵循最小授权原则。	
21	运维安全/人员管理/人员转岗、离岗	必测项	a) 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； b) 应取回各种身份证件、钥匙、徽章等物品以及机构提供的软硬件设备； c) 应办理严格的调离手续，关键岗位人员离岗应承诺调离后的保密义务后方可离开。	a) 访谈录用负责人员，询问是否严格规范人员离岗过程，是否及时终止离岗员工的所有访问权限； b) 查看是否取回转岗、离岗员工各种身份证件、钥匙、徽章等物品以及机构提供的软硬件设备等； c) 查看关键岗位人员的调离手续是否符合制度要求，关键岗位人员离岗是否在承诺调离后的保密义务后方可离开。	a) 严格规范了人员离岗过程，制度文件中有明确的规定，并及时终止离岗员工的所有访问权限； b) 取回转岗、离岗员工各种身份证件、钥匙、徽章等物品以及机构提供的软硬件设备； c) 关键岗位人员的调离手续符合制度要求，具有严格的调离手续，关键岗位人员在承诺调离后的保密义务后方离岗。	管理类
22	运维安全/人员管理/人员考核	必测项	a) 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； b) 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； c) 应对考核结果进行	a) 访谈录用负责人员，询问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核，是否定期对关键岗位的人员进行全面、严格的安全审查和技能考核； b) 检查考核记录和安	a) 定期对各个岗位的人员进行安全技能及安全认知的考核，定期对关键岗位的人员进行全面、严格的安全审查和技能考核； b) 对考核结果进行	管理类

序号	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
			记录并保存。	全审查记录。	记录并保存。	
23	运维安全/人员管理/安全意识教育和培训	必测项	a) 应对各类人员进行安全意识教育，对信息安全基础知识、岗位操作规程、岗位技能和相关安全技术等进行培训； b) 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； c) 应对定期开展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； d) 应对安全教育、培训的情况和结果进行记录并归档保存。	a) 访谈相关人员，询问是否对各类人员进行安全意识教育，对信息安全基础知识、岗位操作规程、岗位技能和相关安全技术等进行培训； b) 访谈相关人员，询问是否对安全责任和惩戒措施进行书面规定并告知相关人员，是否对违反违背安全策略和规定的人员进行惩戒； c) 检查是否对定期开展安全教育和培训进行了书面规定，是否针对不同岗位制定不同的培训计划； d) 检查是否对安全教育、培训的情况和结果进行记录并归档保存。	a) 对各类人员进行了安全意识教育，对信息安全基础知识、岗位操作规程、岗位技能和相关安全技术等进行了培训； b) 对安全责任和惩戒措施进行了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了惩戒； c) 对定期开展安全教育和培训进行了书面规定，针对不同岗位制定了不同的培训计划； d) 对安全教育、培训的情况和结果进行了记录并归档保存。	管理类
24	运维安全/人员管理/外部人员访问管理	必测项	a) 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； b) 应对外部人员允许访问的区域、系统、设备、信息等内容进行书面的规定，并按照规定执行。	a) 访谈管理人员，询问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、信息等内容进行书面的规定，并按照规定执行； b) 检查申请记录、登记备案记录、外部人员	a) 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； b) 有申请记录、登	管理类

序号	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
				允许访问的区域、系统、设备、信息等内容的书面规定。	记备案记录、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。	
25	运维安全/人员管理/职责分离	必测项	a) 关键岗位人员应职责分离； b) 应明确规定敏感信息管理的相关岗位和人员管理责任，分离不相容岗位并控制信息操作权限，规定敏感信息操作流程和规范。	a) 检查是否对关键岗位人员进行职责分离； b) 检查敏感信息管理制度； c) 检查敏感信息管理的相关岗位和人员管理责任。	a) 对关键岗位人员进行职责分离； b) 具有敏感信息操作流程和规范； c) 规定了敏感信息管理的相关岗位和人员管理责任。	管理类
26	运维安全/文档管理/文档编写要求	必测项	文档描述应与实际系统相符合。	检查文档描述是否与实际系统相符合。	文档描述与实际系统相符合。	管理类
27	运维安全/文档管理/文档版本控制	必测项	文档应进行版本控制管理与编号管理。	检查文档是否进行了版本控制管理与编号管理。	文档进行了版本控制管理与编号管理。	管理类
28	运维安全/文档管理/文档格式要求	必测项	文档格式应统一规范，易于浏览。	检查文档格式是否统一规范，易于浏览。	文档格式统一规范，易于浏览。	管理类
29	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。	检查是否有通信线路、网络设备的运行状况、网络流量、用户行为等的监测工具，查看工具运行状况、监控记录、报警方式和报警记录等内容。	使用了工具监控通信线路、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
30	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	a) 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； b) 运行状况应包括监视服务器的CPU、硬盘、内存、网络等资	a) 检查是否对主机的运行状况、用户行为等进行监测，查看监测工具的运行状况、监控记录、报警方式和报警记录等内容； b) 查看主机监控软件，	a) 使用了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	管理类

序号	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
			源的使用情况； c) 应能对系统的服务水平降低到预先规定的最小值进行检测和报警。	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； c) 检查主机，查看是否有服务水平最小值的设定，当服务水平降低到预先设定的最小值时，是否能报警。	和报警记录； b) 如果采用人工监控方式，每日至少三次查看系统资源使用状况并记录； c) 集中监控平台的监控范围覆盖所有的重要服务器，且监控内容包括了服务器的CPU、硬盘、内存、网络等资源； d) 能对降低到预设最小值时进行检查和报警。	
31	运维安全/监控管理/应用运行各项指标监控情况	必测项	a) 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； b) 应能对系统的服务水平降低到预先规定的最小值进行监测和报警。	a) 检查是否有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； b) 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，系统是否能报警。	a) 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； b) 对服务水平进行了配置； c) 能对降低到预设最小值时进行监测和报警。	管理类
32	运维安全/监控管理/异常处理机制	必测项	a) 应按重要程度进行分级报警，并且重要报警应能以某种方式（如短信、邮件等）主动通知相关人员及时处置； b) 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，采取必要	a) 检查是否按重要程度进行分级报警，重要报警是否能以某种方式（如短信、邮件等）主动通知相关人员及时处置； b) 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	a) 按重要程度进行了分级报警，重要报警以某种方式主动通知相关人员及时处置； b) 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，采取必要的应对	管理类

序号	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
			的应对措施。	必要的应对措施。	措施。	
33	运维安全/变更管理/变更制度化管理	必测项	a) 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应经过评审、审批、测试后方可实施变更，并在实施后将变更情况向相关人员通告； b) 变更方案应有变更失败后的回退方案等。	a) 检查变更管理制度是否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应经过评审、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； b) 检测变更方案是否具有变更失败后的回退方案。	a) 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在经过评审、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； b) 变更方案具有变更失败后的回退方案等。	管理类
34	运维安全/变更管理/变更实施	必测项	应记录变更实施过程，并妥善保存所有文档和记录。	检查变更过程中产生的文档和记录。	a) 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； b) 变更内容中包含了变更失败后的回退方案等，具有完整的变更过程文档和记录。	管理类
35	运维安全/安全事件处置/安全事件识别、报警和分析	必测项	a) 应使用必要的手段对服务器资源进行监控； b) 监控的范围应包括网络设备、重要的服务器，且监控内容覆盖服务器CPU、硬盘、内存、网络等资源； c) 网络设备和服务器资源的分配应能满足其业务需求； d) 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。	a) 访谈系统管理员，询问采用何种方式监控系统资源使用情况（如人工监控、第三方主机监控软件等）； b) 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网络设备和服务器，监控的内容是否包括服务器的CPU、硬盘、内存、网络等资源； c) 访谈系统管理员，询	a) 如果采用人工监控方式，每日至少三次查看系统资源使用状况并记录； b) 集中监控平台的监控范围覆盖了所有的重要网络设备和服务器，且监控内容包括服务器的CPU、硬盘、内存、网络等资源； c) 如果服务器不是多业务竞争使用	管理类

序号	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
				问系统资源控制的管理措施，询问服务器是否为专用服务器； d) 如果使用专用服务器，查看系统资源的实时利用率是不是不高（如CPU使用率等），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； e) 访谈系统管理员，询问有无采用第三方主机监控程序，并查看是否有报警功能。	硬件资源且实时利用率不是很高，则该项要求为不适用，如果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，则该项要求为符合，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； d) 针对系统服务水平报警，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。	
36	运维安全/安全事件处置/安全事件报告和处置	必测项	a) 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； b) 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	a) 检查安全事件报告和处置管理制度中，是否明确安全事件的类型，是否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； b) 检查安全事件报告和响应处理程序中，是否明确事件的报告流程，是否明确响	a) 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； b) 安全事件报告和响应处理程序明确了事件的报告	管理类

序号	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
			围、程度，以及处理方法等。	应和处置的范围、程度，以及处理方法等。	流程，响应和处置的范围、程度，以及处理方法等。	
37	运维安全/安全事件处置/安全事件的分类和分级	必测项	应根据国家相关管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。	检查安全事件相关管理制度中是否对系统计算机安全事件进行等级划分，等级划分是否考虑了国家相关管理部门对计算机安全事件等级划分方法的要求，以及安全事件对系统产生的影响。	安全事件相关管理制度中，根据国家相关管理部门对计算机安全事件等级划分方法和安全事件对系统产生的影响，对系统计算机安全事件进行了等级划分。	管理类
38	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	a) 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； b) 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。	a) 检查安全事件记录中，是否包含事件原因分析、处理方法、经验教训等内容； b) 检查安全事件报告和响应处理程序中，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。	a) 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； b) 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
39	运维安全/内部审计管理/内部审计制度	必测项	a) 应制定信息系统安全内部审计制度，规定审计职责、审计内容、审计周期、审计问题处理机制； b) 应明确规定敏感信息的内部监督机制、安全事件处置机制和安全审计机制，严禁从业人员非法存储、窃取、泄露、买卖支付敏感信息。	a) 检查信息系统安全内部审计制度； b) 检查敏感信息的内部监督机制、安全事件处置机制和安全审计机制。	a) 具有完善的系统安全内部审计制度； b) 具有完善的敏感信息的内部监督机制、安全事件处置机制和安全审计机制。	管理类

序号	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
40	运维安全/内部审计管理/内部审计	必测项	a) 按制度开展内部审计工作，记录审计内容； b) 通报审计结果，总结问题，制定整改计划，并进行记录； c) 每年宜至少进行一次全面系统的第三方安全审计，并作出相应评价报告。	检查内部审计记录。	定期按照要求开展内部审计。	管理类

8.7 业务连续性测试

验证系统是否具备业务连续性管理制度，设计目标符合JR/T 0122相关要求，测试内容见表10。

表10 业务连续性测试

序号	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
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
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	a) 应具备灾难恢复时间目标和恢复点目标； b) 系统应支持RPO和RTO的设置。	访谈相关人员，询问是否具备灾难恢复时间目标和恢复点目标。	a) 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； b) 系统支持RPO和RTO的设置。	管理类

序号	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	业务连续性/业务连续性技术环境/备份机房	必测项	a) 应具有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及基础设施（包括但不限于网络设备、主机设备等）； b) 应具有数据备份系统和核心业务处理系统； c) 应具有专业技术支持及运行维护管理能力。	a) 检查是否具有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及基础设施； b) 检查备份机房是否具有数据备份系统和核心业务处理系统； c) 检查备份机房是否具有专业技术支持及运行维护管理能力。	a) 备份机房与主机房不在同一个建筑物内，距离大于 10 公里； b) 备份机房具有进行数据处理和支持关键业务功能运作的基础设施； c) 备份机房具有数据备份系统和核心业务处理系统； d) 备份机房具有专业技术支持及运行维护管理能力。	管理类
4	业务连续性/业务连续性技术环境/关键链路冗余设计	必测项	a) 应保证通讯线路采用冗余； b) 应保证主要网络设备采用冗余； c) 应保证主要数据处理服务器采用冗余； d) 主机房的互联网接入应具备双链路。	a) 访谈网络管理员，询问通讯线路、网络设备、主要数据处理服务器是否采用冗余； b) 检查通讯线路、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； c) 检查主机房的通讯线路、主要网络设备、主要数据处理服务器是否采用了冗余方式； d) 检查主机房的互联网接入是否为不同运营商的两条链路。	a) 通讯线路、主要网络设备和数据处理服务器采用了硬件冗余方式； b) 主机房的互联网接入采用了不同运营商提供的双链路。	管理类
5	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。	a) 访谈安全管理员，询问是否使用了高可靠的磁盘阵列； b) 查看磁盘阵列设备。	采用了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

序号	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
6	业务连续性/业务连续性管理/业务连续性管理制度	必测项	a) 应具备业务连续性管理制度； b) 业务连续性管理制度内容应完备，与实际执行应一致。	a) 访谈安全管理员，询问业务连续性管理制度内容； b) 查看业务连续性管理制度； c) 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
7	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。	a) 访谈安全管理员，询问是否具备应急响应流程； b) 查看应急响应流程相关文档。	具有应急响应流程，流程规范合理。	管理类
8	业务连续性/业务连续性管理/应急恢复预案	必测项	a) 应在统一的应急预案框架下制定不同事件的应急预案； b) 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； c) 应具备不同场景的恢复预案（如数据恢复、应用级恢复等），内容完备、合理。	a) 访谈安全管理员，询问是否具备应急预案； b) 查看应急预案框架是否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； c) 查看应急预案是否覆盖不同场景（如数据恢复、应用级恢复等），内容是否完备、合理。	a) 具备了应急预案； b) 应急预案框架全面； c) 应急预案覆盖了不同场景，内容完备、合理。	管理类
9	业务连续性/日常维护/定期演练	必测项	a) 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，至少每年一次； b) 应每年进行业务连续性演练，包括主备机房的切换演练，演练需提供记录； c) 应对演练中暴露出的问题进行总结并及时整改。	a) 检查演练计划； b) 查看演练记录； c) 检查演练问题整改记录。	a) 具有演练计划，定期进行应急演练； b) 每年进行业务连续性演练，包括主备机房切换演练，具有演练记录； c) 具有演练后的总结报告或记录。	管理类

序号	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
10	业务连续性/日常维护/定期培训	必测项	应定期进行应急预案和业务连续性培训并具有培训记录，应至少每年举办一次培训。	a) 访谈安全管理员，询问是否至少每年举办一次应急预案和业务连续性培训，并具有培训记录； b) 查看记录完整性。	至少每年举办一次应急预案和业务连续性培训，并具有完整的培训记录。	管理类

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 12406—2008 表示货币和资金的代码
[5] GB/T 22080—2016 信息技术 安全技术 信息安全管理体系 要求
[6] GB/T 22081—2016 信息技术 安全技术 信息安全控制实践指南
[7] GB/T 22239—2008 信息安全技术 信息系统安全等级保护基本要求
[8] GB/T 27065—2015 合格评定 产品、过程和服务认证机构要求
[9] JR/T 0149—2016 中国金融移动支付 支付标记化技术规范