ICS 35.240.40
CCS A 11

JR

中华人民共和国金融行业标准

JR/T 0281—2024

银行业软件测试环境管理规范

Banking software test environment management specification

2024－01－15 发布　　2024－01－15 实施

中国人民银行　发布

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由中信银行股份有限公司提出。

本文件由全国金融标准化技术委员会（SAC/TC 180）归口。

本文件起草单位：中信银行股份有限公司、北京金安信息技术有限责任公司、北京国家金融科技认证中心有限公司、中国工商银行股份有限公司、中国农业银行股份有限公司、招商银行股份有限公司、中国光大银行股份有限公司、北京农村商业银行股份有限公司。

本文件主要起草人：冷炜、李昭文、高蕊、闫鑫、章岩、陈让宽、张雪、倪又明、冯晓文、周鑫、赵世航、范建峰、胡小丽、屈小凯。

引　言

近年来，随着客户体验升级、管理水平的提升，为适应业务发展的需要，银行业金融机构开展了新一轮大规模业务流程再造和应用系统升级，其中软件测试作为保证系统稳定、产品质量和提升用户满意度的重要措施，越来越受到银行业金融机构的重视。软件测试环境作为软件测试的基础保障，贯穿整个测试过程，对项目进度、质量、资源投入等方面均起到至关重要的作用。为提升软件测试环境管理的规范性，从整体上保障软件测试质量，持续激发测试环境管理创新意识，特编制本文件。

银行业软件测试环境管理规范

1 范围

本文件规定了银行业软件测试环境管理（以下简称测试环境管理）的测试环境规划、测试环境准备、测试环境监控及巡检、测试环境事件及问题管理、测试环境变更管理、测试环境备份与恢复、测试环境配置管理、测试环境安全管理、测试环境资源管理及测试环境释放管理的要求。

本文件适用于指导测试环境运行维护人员（以下简称运维人员）、项目管理人员、软件设计人员、软件开发人员、软件测试人员及其他相关人员开展测试环境管理相关工作。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；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。

JR/T 0171—2020 个人金融信息保护技术规范

3 术语和定义

下列术语和定义适用于本文件。

3.1

监控工具 monitoring tool

采集监控对象的具体指标所采用的手段和方法。

注：监控工具通常包括专业监控软件、标准监控工具、自行开发的监控程序及脚本等。

3.2

配置管理 configuration management

应用技术和管理方法，识别和记录配置项及其功能特征、物理特征、控制特征的变更，记录和报告变更的处理状态和执行状态，以及验证其是否符合特定需求的过程。

3.3

去标识化 de-identification

通过对个人信息的技术处理，使其在不借助额外信息的情况下，无法识别或者关联个人信息主体的过程。

[来源：GB/T 35273—2020，3.15]

4 总则

4.1 目标

测试环境管理的目标是通过显性化、指标化、可测量化等各种手段，保证测试环境运行的稳定性、安全性和可控性，提高银行业应用系统的测试质量，提升测试工作效率，建立系统化的测试环境管理体系。

4.2 原则

测试环境管理的过程应遵循以下原则。

a）计划性原则：应提前制定计划，并在实施过程中严格按照计划开展测试环境管理工作。

b）安全性原则：树立风险防范意识，将安全措施落实到测试环境管理的各个环节。

c）实用性原则：遵循高效益、低成本、易操作的原则。

d）系统性原则：对测试环境管理中涉及的资源和活动进行系统性管理，明确测试环境生命周期不同阶段的职责和权限。

e）可用性原则：测试环境管理应保证不同类型测试工作的顺利开展。

f）可追溯性原则：测试环境管理中涉及的管理对象应具备统一的标识，管理行为应具备规范的记录，为测试环境管理过程的持续改进提供依据。

4.3 测试环境管理范围

测试环境管理范围涉及测试环境全生命周期的各阶段，包括测试环境规划、测试环境准备、测试环境监控及巡检、测试环境事件及问题管理、测试环境变更管理、测试环境备份与恢复、测试环境配置管理、测试环境安全管理、测试环境资源管理以及测试环境释放管理。

4.4 组织与职能

4.4.1 组织机构设立

应结合具体情况设立测试环境管理过程中相关的组织机构，明确各组织机构的职能和人员角色的职责。

4.4.2 组织机构的职能

测试环境管理过程中相关的组织机构应主要具备以下职能。

a）测试环境管理制度建设职能：制定测试环境管理制度及规范，对测试环境管理人员、使用人员及操作人员的行为进行约束和指导，保障测试环境的安全、可靠和稳定运行。

b）测试环境规划职能：依据测试工作的任务目标，完成测试环境资源评估、测试环境使用原则的制定等工作，保障测试环境准备工作的顺利开展。

c）测试环境准备职能：完成测试环境需求采集、需求分析、资源分配、软硬件环境准备、测试数据准备等工作，发现并识别测试环境准备过程中存在的风险及隐患，保障搭建完成的测试环境能够正常开展测试工作。

d）测试环境运维职能：依据测试环境运维制度，建立完善的管理策略、监控测试环境运行状态、识别风险及安全事件、处理测试环境运行过程中出现的异常情况，保障测试环境的稳定运行。

4.4.3 人员角色及职责

在设立人员角色时，应遵循最小权限原则和权限互斥原则，并依据测试环境管理流程及规范设立所需角色，主要包括以下角色类型。

a）决策类角色：依据现有实际情况及未来目标，负责对测试环境管理工作进行战略规划，并对测试环境建设、运维及使用过程中的重大事项进行审议、决策。

b）测试环境管理类角色：负责测试环境整体规划及流程管控，建立测试环境管理的相关规范及制度，合理调配人员及资源，对重要事件进行分析、决策，保证测试环境管理中各项工作的顺利进行。

c）测试环境实施类角色：依据实施方案、实施计划及实施手册等文档，负责测试环境生命周期中各项工作的具体实施。测试环境实施类角色的操作行为应严格遵守相关管理规范及安全制度的要求。

d）测试环境使用类角色：依据测试环境使用规范及相关规章制度，严格遵守访问控制要求，合理使用测试环境。

5 测试环境规划

5.1 测试环境规划管理对象和目的

5.1.1 测试环境规划管理对象

测试环境规划管理的对象为测试环境规划活动。测试环境规划活动是为建立测试环境而进行的整体性的、具有长远意义的策划工作，包括评估测试环境所需资源、制定测试环境建设整体原则、制定测试环境使用原则等。

5.1.2 测试环境规划管理目的

通过测试环境规划，使测试环境资源能够支撑应用系统建设的各测试阶段，并使测试环境资源得到充分的利用。

5.2 测试环境规划原则

测试环境规划应遵循以下原则。

a）前瞻性原则：测试环境应不仅满足近期测试需求，还应满足可以预见的未来测试需求。

b）充分性原则：测试环境应满足各阶段、各种类型的测试需求并至少包括 1 套独立的、完整的主测环境。

c）合理性原则：基于对测试环境使用需求的充分评估以及实际使用情况的定期评估，应随时调整测试环境资源，对闲置率较高的资源进行重新分配，减少资源浪费。

d）安全性原则：充分考虑数据安全策略、网络安全策略、用户访问安全策略、应用软件安全策略等安全要求，避免泄露敏感数据，保障测试环境不被非法入侵、不受外部攻击、不被人为破坏。

e）一致性原则：测试环境的操作系统、数据库、中间件等基础软件版本、参数配置以及网络结构宜与生产环境保持一致。

5.3 测试环境资源需求评估

测试环境资源需求评估应随测试环境的使用定期进行。

测试环境资源需求评估应充分考虑近期及远期测试环境资源需求，主要包括以下评估内容。

a）项目建设周期及上线频率。

b）项目涉及的应用系统。

c）近期及远期重点项目规划。

d）本单位及监管单位对应用系统的安全要求。

e）基础软件（操作系统、数据库、中间件等）的服务保障周期及升级计划。

5.4 测试环境规划制定

应制定完整的、统一的测试环境规划方案。测试环境规划应包括测试环境建设方案、测试环境建设计划、测试环境资源预算、测试环境使用调度基本策略等内容。

6 测试环境准备

6.1 测试环境准备的对象及目的

6.1.1 测试环境准备的对象

测试环境准备的对象包括硬件、基础软件、应用软件、网络以及测试数据。

6.1.2 测试环境准备的目的

测试环境准备的目的是规范测试环境需求采集、需求分析、需求确认、数据准备、测试环境搭建等工作过程，保障测试环境准备过程的质量与效率。

6.2 测试环境需求管理

6.2.1 测试环境需求要素

测试环境需求包括现有测试环境的需求以及新建测试环境的需求。

现有测试环境需求主要包括以下要素。

a）测试环境用途：主要描述测试环境的使用者和具体用途。

b）基础数据需求：执行测试所需测试数据的具体需求。
c）应用软件需求：包括测试所需的应用软件及其版本要求和配置信息。
d）使用时间需求：使用测试环境的起止时间。
e）存量数据需求：存量数据相关说明。

新建测试环境需求除包括与现有测试环境需求同样的要素外，还应包括以下要素。

a）硬件需求：包括系统架构、硬件类型、硬件数量、配置需求等。
b）基础软件需求：包括操作系统、数据库、中间件等基础软件及其版本的需求。
c）网络环境需求：包括相关系统访问策略、外联需求等。

6.2.2 测试环境需求分析原则

应建立对测试环境需求的有效分析评估机制，需求分析应遵循以下原则。

a）分析测试环境需求应涵盖各要素以及与生产环境的差异等。
b）分析现有测试环境使用情况，现有测试环境不能满足需求时可补充资源或新建测试环境。
c）按重要性与紧急程度为测试环境需求分配优先级。
d）进行测试环境安全性分析，包括相应网络访问控制、权限控制的安全性分析等。
e）制定测试环境需求确认策略，根据测试环境需求确认策略决定是否组织各相关方对测试环境需求进行评审。

6.3 测试环境基础数据准备

测试环境基础数据准备是开展测试工作前的重要环节之一。根据测试数据来源不同，相应的测试数据准备工作如下。

a）测试数据来源于生产数据时，应制定生产数据脱敏或去标识化方案和测试数据导入方案，评审方案并进行测试验证。
b）测试数据来源于其他测试环境数据时，应根据测试数据需求制定测试数据导入方案，并进行测试验证。
c）测试数据来源于模拟数据时，应根据测试数据需求提前准备生成测试数据的脚本或工具，并进行测试验证。
d）测试数据来源于外部数据时，应与测试数据提供方共同确定测试数据提供方式和导入方案，并进行测试验证。

6.4 测试环境搭建

测试环境搭建包括制定测试环境搭建方案与计划、实施测试环境搭建以及测试环境验证工作。

测试环境搭建方案与计划的制定应参照测试环境需求，当测试环境需求发生变更时，应首先评估影响范围，然后对方案和计划进行调整。

测试环境搭建实施过程包括以下内容。

a）硬件安装和配置。
b）基础软件的安装和配置。
c）初始应用系统版本的部署。
d）测试数据的创建。
e）测试环境配置信息的更新。

测试环境搭建完成后，应进行测试环境验证。验证完毕后更新测试环境配置信息，整理并留存测试环境搭建和测试环境验证过程中的记录。

7 测试环境监控及巡检

7.1 测试环境监控及巡检的对象和目的

7.1.1 测试环境监控及巡检的对象

测试环境监控及巡检的对象包括应用系统、服务器、存储设备、数据库、网络设备、网络线路、应用程序服务端口等。

7.1.2 测试环境监控及巡检的目的

测试环境监控的目的是实时了解各层面的运行状态，及时发现测试环境的故障问题。
测试环境巡检的目的是有效识别风险隐患，提前发现和解决日常运维中的故障隐患。

7.2 测试环境监控及巡检的范围

测试环境监控及巡检包括基础设施监控及巡检、应用监控及巡检，具体包括以下内容。

a）基础设施监控及巡检的范围主要包括以下内容。
——硬件设备：服务器、存储设备、网络设备等相关硬件的状态、负载。
——系统软件：各类操作系统、数据库、中间件、虚拟化软件等其他相关系统支撑软件的状态、性能。
——网络状态：网络线路、重要端口等的状态、负载。
——机房环境：温湿度、通风、消防、不间断电源（UPS）等状态。

b）应用监控及巡检的范围主要包括以下内容。
——应用状态：应用相关进程、端口、服务等是否可用。
——应用性能：交易响应时间是否存在异常。
——应用配置：应用相关配置参数、应用间关联关系等。
——应用日志：应用程序错误日志文件和交易日志。

7.3 测试环境监控的原则

测试环境监控应遵循以下原则。

a）及时性原则：测试环境监控活动应定期开展，保证可以及时发现测试环境问题。
b）有效性原则：测试环境监控策略可参考生产环境的监控策略、测试环境的使用目的、应用系统的运行特点等制定，并定期对监控策略进行评估及改进，以保证监控策略的有效性。
c）可度量性原则：测试环境监控可通过特定指标度量测试环境状态。指标可包括但不限于系统可用性指标，系统连通性指标，系统运行性能指标，测试环境、生产环境比对指标。
d）低影响性原则：测试环境监控活动应减少对监控对象的影响，监控工具宜部署在独立的文件系统或路径下，且监控工具不宜占用过多系统资源。
e）记录完整性原则：监控日志记录及监控报警记录应集中存放，并可根据系统特点定期清理。

7.4 测试环境巡检原则

测试环境巡检应遵循以下原则。

a）有效性原则：测试环境巡检策略应结合生产环境巡检策略、巡检对象特性、监控结果分析报告等因素制定。
b）及时性原则：测试环境巡检应定期实施，遇到需重点保障的系统或时期可提高巡检频率。
c）记录完整性原则：测试环境巡检应保留巡检记录，报错巡检项应得到有效的跟踪处理，对有影响或重大隐患的软硬件故障应及时上报。

8 测试环境事件及问题管理

8.1 测试环境事件及问题管理对象和目的

8.1.1 测试环境事件及问题管理对象

测试环境事件管理的对象包括测试环境运行过程中导致服务中断或服务可用性下降的现象以及与测试环境相关的支持服务请求。测试环境问题管理的对象包括导致服务中断或服务可用性下降的根本原因及可能导致测试环境故障的隐患。

8.1.2 测试环境事件及问题管理的目的

测试环境事件管理的目的包括尽可能降低测试环境事件对测试环境服务的影响，确保测试环境服务快速恢复正常，提升测试环境可用率，提供最佳的测试环境服务。测试环境问题管理的目的包括建立问题发现、解决、持续改进的常态化机制，防止服务中断或服务可用性下降以及其他风险事件的重复发生。

8.2 测试环境事件处理机制

8.2.1 测试环境事件提出

测试环境事件处理机制应建立明确、畅通的测试环境事件提出渠道，相关人员发现测试环境事件时应及时提出。

对于导致服务可用性下降的测试环境事件，提出的信息应主要包括以下内容。

a）事件发生时间。

b）事件现象。

c）事件所在的测试环境。

d）事件所影响的测试任务。

e）提出人员。

f）事件影响的系统范围。

对于支持服务请求类的测试环境事件，提出的信息应主要包括以下内容。

a）服务支持需求内容。

b）目标环境或应用说明。

c）紧急程度。

d）期望完成时间。

8.2.2 测试环境事件处理过程记录

应对测试环境事件的处理过程进行记录，支持事件查询、问题分析和事后审计。应根据测试环境事件的处理结果，及时更新知识库，提高同类事件的处置效率。

对于导致服务可用性下降的测试环境事件，记录的信息主要包括以下内容。

a）事件发生时间。

b）事件解决时间。

c）事件影响范围。

d）事件描述。

e）事件处理过程。

f）事件级别。

g）事件来源。

对于支持服务请求类的测试环境事件，记录的信息主要包括以下内容。

a）服务请求提出时间。

b）服务请求完成时间。

c）服务请求描述。

d）服务请求结果。

e）服务请求处理过程。

f）服务请求来源。

8.3 测试环境问题处理机制

8.3.1 测试环境问题发现

测试环境问题发现的来源主要包括事件转化、运维自查、管理层或监管层的专项检查。

8.3.2 测试环境问题记录

应对测试环境问题处理过程进行记录，主要包括以下记录内容。

a）与测试环境事件的关联关系。

b）测试环境问题原始记录信息。

c）测试环境问题分析情况和原因记录。

d）测试环境问题解决方案记录。

e）测试环境问题总结。

f）整改计划和实施情况信息。

9 测试环境变更管理

9.1 测试环境变更管理对象和目的

9.1.1 测试环境变更管理对象

测试环境变更管理对象包括发生在测试环境设备、网络、基础软件、应用软件等配置及测试数据的变更过程。

9.1.2 测试环境变更管理目的

测试环境变更管理的目的是确保测试环境的变更遵循标准的方法、程序和规则，并能快捷有效地进行变更，降低因测试环境变更导致的测试服务中断所造成的影响。测试环境变更管理过程应具备明确的记录，便于变更的追溯和跟踪。

9.2 测试环境变更分类和分级

测试环境变更宜按照紧急程度进行分类，通常包括以下类别。

a）标准变更：变更实施风险较低，对测试环境影响较小，且可以通过标准程序及流程处理的测试环境变更，可通过预授权机制简化变更流程。

b）紧急变更：为修复重大测试故障、安全漏洞、生产问题等需要立即在测试环境中实施的变更，可通过快速应急流程进行紧急变更的审批及授权。

c）例行变更：有一定周期性的测试环境变更。

测试环境变更应根据对测试环境服务的影响程度进行分级管理，不同级别的变更应制定相应的评审机制，对测试环境服务水平及可用性有影响的变更，应按照对测试环境影响最小原则提前规划软件版本变更时间。

9.3 测试环境变更请求

测试环境变更请求要素应包括测试环境变更内容、应急回退方案、测试服务影响说明、期望完成时间等，以支撑测试环境变更的决策、执行、回退、跟踪审计等活动。

9.4 测试环境变更评审

对测试环境服务水平及可用性有重大影响或涉及安全策略的测试环境变更应建立变更评审机制。参与评审的人员包括变更所涉及的领域专家以及变更影响的相关人员，涉及安全策略的测试环境变更评审还应要求具有安全职责的岗位人员参与。紧急变更应建立事后评审回顾机制，以确保测试环境变更实施过程的正确性和完整性。

9.5 测试环境变更实施

在测试环境变更实施过程中，应及时通知测试环境变更相关人员配合。

如变更失败或变更验证不通过，在不具备继续变更的条件时，应详细记录现场信息、及时终止变更，对已实施的变更按照应急回退方案进行回退并及时报告失败原因。

9.6 测试环境变更验证

测试环境变更管理应建立测试环境变更实施完成后的验证确认机制。在变更实施完成后的一定时间内，对测试环境变更实施结果进行验证及确认，应对验证不通过的变更实施过程记录进行分析和检查。

10 测试环境备份与恢复

10.1 测试环境备份与恢复对象和目的

10.1.1 测试环境备份与恢复对象

测试环境备份与恢复对象包括但不限于基础软件、应用软件、数据、日志及相应配置参数。

10.1.2 测试环境备份与恢复目的

测试环境备份与恢复的目的是通过对测试环境的定期备份以及有效的恢复手段保障测试环境的可用性。

10.2 测试环境备份的原则与策略

测试环境备份应遵循以下原则。

a）合理性原则：确保备份对象包括恢复环境所需的全部内容。

b）关联性原则：备份开始前应明确备份对象涉及的关联内容，确保备份工作的一致性。

c）计划性原则：应制定测试环境备份计划，减少备份工作对环境使用带来的影响。

d）可靠性原则：确保备份数据在需要进行恢复时可用。

e）安全性原则：确保备份数据存储介质的安全性。

测试环境备份的策略主要包括全量备份、增量备份和差分备份。测试环境管理人员应提供备份所需的软硬件资源，其中备份内容宜存储于安全介质上。备份操作过程中应有日志记录，应对备份完成情况进行验证确认。

10.3 测试环境备份的检查

根据已制定的测试环境备份计划开展备份工作，对已完成备份的内容进行检查，确保备份的有效性。

10.4 测试环境恢复的原则

测试环境恢复应遵循以下原则。

a）合理性原则：针对所需恢复的状态，将全部所需的内容进行完整恢复。

b）关联性原则：结合备份涉及的关联系统，将必要的关联内容一并进行恢复。

c）安全性原则：测试环境恢复工作应具备安全性，例如涉及敏感数据恢复时，确保将敏感数据进行数据脱敏或去标识化，避免出现安全问题。

d）可追溯性原则：测试环境恢复工作应具备可追溯性，测试环境恢复工作具备提出申请、需求评审、恢复执行、恢复验证等过程记录。

10.5 测试环境恢复的验证

测试环境恢复的验证应结合测试环境恢复需求以及备份时采用的策略开展，确保恢复工作有序准确地进行，恢复完成后由执行方、需求提出方分别验证确认。

11 测试环境配置管理

11.1 测试环境配置管理对象和目的

11.1.1 测试环境配置管理对象

测试环境配置管理对象是测试环境所涉及的纳入配置管理范畴的配置项集合，包括硬件、软件、文档、人员信息和其他配置项。

11.1.2 测试环境配置管理目的

测试环境配置管理的目的是规范配置管理活动，保证配置项的更改受控，保障测试环境配置管理的准确性、完整性、时效性和可追溯性，并准确、全面、及时地反映测试环境中各配置项的整体视图，为测试环境管理和技术活动提供坚实的支撑信息和支持依据。

11.2 测试环境配置信息管理

测试环境配置信息管理是对测试环境各配置项进行标识、组织和控制的技术活动。

各单位应建立和维护测试环境配置信息管理流程，制定测试环境配置信息管理计划，建立相应的配置信息识别准则，确定配置项的主要特征，为配置项建立唯一的标识规范，新增配置项时需考虑同时建立与其他配置项之间的关联关系。

测试环境配置信息变更的触发原因包括但不限于硬件改造、版本升级、系统扩容。各单位应建立测试环境配置变更管控机制，明确对测试环境配置项变更请求、评估、审核、实施、确认等环节的具体要求。

对测试环境配置信息的操作应作记录留痕处理，并定期验证配置信息是否符合测试环境管理要求及测试活动开展需求。

11.3 测试环境软件版本基线管理

测试环境软件版本基线管理主要包括测试环境基础软件版本基线管理和测试环境应用软件版本基线管理。

测试环境基础软件版本基线应定期与生产环境基础软件版本基线进行比对，确保测试环境与生产环境基础软件版本基线一致。对于版本不一致的情况，测试环境管理人员应及时评估版本不一致的风险并做出说明。

测试环境应用软件版本基线应及时更新，确保待测应用软件版本基线及关联应用软件版本基线与生产环境应用软件版本基线一致。

11.4 测试环境配置管理风险管控

测试环境配置管理过程中应对各类风险进行防范，包括配置管理权限分配不当、配置基准评审不足、配置信息记录缺失、新增配置基准检查不足、配置变更操作准确性控制不足和配置清单维护不及时等。

各单位应明确配置检查记录的标准，定期开展测试环境配置检查工作，审核测试环境配置信息状态，及时发现各类不完整或者异常的配置信息，进行配置信息的维护。各单位可采用的措施包括但不限于权限分配、配置备份、配置信息新增及更改过程记录、配置信息变更过程审核、配置状态报告维护方案和配置评审会等。

12 测试环境安全管理

12.1 测试环境安全管理对象和目的

12.1.1 测试环境安全管理对象

测试环境安全管理对象是测试环境管理过程中所涉及的主机安全、数据安全、通信网络及区域边界安全。

12.1.2 测试环境安全管理目的

测试环境安全管理的目的是对主机安全、数据安全、通信网络及区域边界安全在测试环境全生命周期内各环节进行管控，保障测试工作安全有序进行。

12.2 测试环境主机安全

12.2.1 访问控制管理

测试环境访问控制管理应遵从权限最小化原则，为不同账户授予完成任务所需的最小权限，不同账户间形成相互制约的关系。访问权限可分为高级、中级、低级并按需分配给用户。

应制定测试环境访问权限申请流程，测试环境运维人员可采取默认授权的方式简化流程，提高访问权限授权的效率。授权许可其他人员访问时，应具备审批授权记录，并限定访问时限。授权结束后，应及时回收访问权限。对存在异常的访问权限，应及时反馈纠正，无法纠正的，应做注销处理。测试环境访问账户创建及权限分配应与生产环境或设计文档保持一致。测试环境访问账户口令应定期更新，避免采用弱口令。

12.2.2 身份鉴别管理

身份鉴别管理具体包括以下内容。

a）应使用关键系统的静态口令对登录操作系统和数据库的用户进行身份鉴别，关键系统的静态口令应具备一定复杂度并定期更换。

b）应确保操作系统和数据库的用户名具有唯一性。

c）应具备登录失败处理措施。

d）应对与主机系统相连的服务器或终端设备进行身份鉴别，当通过互联网对服务器进行远程管理时，应采取防窃听措施。

12.2.3 恶意代码防范

测试环境管理人员应在测试环境安装防恶意代码软件，对于依赖病毒库进行恶意代码查杀的软件，应及时更新防恶意代码软件版本和病毒库；对于非依赖于病毒库进行恶意代码查杀的软件，应保证防恶意代码软件特征库的有效性与实时性。恶意代码防范工作应实行统一管理，确保对网络内计算机病毒感染情况进行统一监控。

12.2.4 软件合规管理

测试环境不应安装与测试工作无关的软件、存在恶意代码的软件和未经授权的软件。

测试环境安装的软件要保证合规、可用，可建立合规软件清单，确定测试环境可安装的软件范围，对于不属于清单范围内的软件，安装应有审批授权记录。

12.3 测试数据安全

12.3.1 敏感数据脱敏或去标识化

12.3.1.1 敏感数据脱敏或去标识化范围界定

敏感数据主要是指具有较高机密性和完整性保护要求的信息，一旦泄露可能对用户或机构造成损失，敏感数据范围的界定应符合JR/T 0171—2020中的规定。在使用生产数据进行测试时，应对敏感数据进行脱敏处理或去标识化处理，应结合自身应用系统架构选择脱敏或去标识化的数据范围，在实施脱敏或去标识化后，确保无敏感信息外泄安全风险。

结合应用系统特征，敏感数据主要包括以下内容。

a）客户类敏感信息：客户类敏感信息主要包括客户基本信息、客户交易信息和客户鉴别信息，内容如下。

——客户基本信息：以电子或者其他方式记录的，能够单独或者与其他信息结合识别特定客户身份的各种信息，例如客户姓名、证件号码、联系方式、住址、电子邮件、银行账户信息、财产状况等，证件号码应覆盖所有的证件类型，包括但不限于身份证、护照、军官证、居留证，联系方式应覆盖所有类型的号码，包括但不限于办公号码、住宅号码。

——客户交易信息：客户在各种银行业务活动中形成的能够单独或者与其他信息结合识别特定客户身份的交易记录、行为轨迹等。

——客户鉴别信息：客户留存在银行系统中并用于登录系统、执行交易等相关操作进行访问控制的信息。

b）系统类敏感信息：应用系统运行相关的关键配置信息。

c）其他类敏感信息：本单位内部财务信息等。

12.3.1.2 敏感数据脱敏或去标识化原则

生产数据在进入测试环境前，需对敏感字段信息进行脱敏或去标识化处理，脱敏或去标识化后的数据要有相应检查机制。

境外机构使用的测试数据包括生产敏感信息，数据脱敏或去标识化的范围及规则需要满足境外当地的监管要求。如因国家有关管理部门明确要求需要在测试环境使用未脱敏或未去标识化的生产数据时，应在使用期间严格控制敏感信息的使用范围和用户权限。

生产数据敏感信息脱敏或去标识化方法需要基于以下原则。

a）数据脱敏或去标识化的方法和工具具备可实施性。

b）数据脱敏或去标识化的方法的强度，即脱敏或去标识化运算不可逆程度。综合考虑测试实际需求和脱敏或去标识化效率等因素，使用强度适宜的脱敏或去标识化方法，强度应与脱敏或去标识化字段的敏感程度相匹配。对于高敏感字段，使用高强度的脱敏或去标识化方法。

c）数据脱敏或去标识化工作原则上在生产环境或与生产环境同等安全级别的环境下进行。

d）数据脱敏或去标识化后保证原有系统之间的一致性，避免影响系统功能的可用性。

e）数据脱敏或去标识化算法及密钥等关键参照信息由具备安全职责岗位的人员进行管理，严格控制访问范围。

f）数据脱敏或去标识化密钥需定期进行更换，应每年至少更换 1 次。

g）如不能实施数据脱敏或去标识化，需要在测试环境使用未脱敏或未去标识化的生产数据时，应在使用期间提供与生产环境相当的安全防护级别。

12.3.1.3 敏感数据脱敏或去标识化验证

完成生产数据脱敏或去标识化后，应严格按照数据脱敏或去标识化验证方案进行检查，确保结果的准确性和完整性。

12.3.2 测试数据访问控制原则

应控制测试数据的访问范围，需要使用生产敏感数据时，应按照最小授权原则，严格控制访问含有敏感信息数据的用户权限和客户端地址范围，同时应对数据的使用记录进行留痕。

测试数据访问控制应遵循以下原则。

a）向外单位提供数据时，应对其中的敏感数据实施脱敏或去标识化处理（国家有关管理部门要求不能实施数据脱敏或去标识化处理的除外）后提供，应以合作范围为限确保提供最小化内容，严禁提供超出合作范围的数据。

b）应严格控制敏感信息在测试环境中的存储区域，禁止在个人终端（含办公终端和测试终端）中存放敏感信息。

c）对需利用公共渠道（例如邮箱、内部信息系统等）进行传输的敏感数据，应对其采取加密处理或使用符合安全管理要求的方式进行传输，以确保含有敏感信息的数据的安全性。涉及密钥类的敏感数据应使用安全渠道进行传输。

d）针对数据脱敏或去标识化方案和验证方案、数据脱敏或去标识化工具和结果检查工具的操作手册等相关文档在制作和传递过程中应进行加密处理，并使用安全渠道进行传输，按照最小授权的原则控制发布范围。

e）需要向境外提供脱敏或去标识化的生产数据时，应对生产数据出境进行安全评估，并遵循个人信息出境的流程及相关要求。

12.3.3 敏感数据清理原则

如因国家有关管理部门明确要求不能实施数据脱敏或去标识化处理的敏感数据，应在测试环境使用完成后，采取不可逆的方式及时清理。

12.4 测试环境网络安全

12.4.1 测试环境网络安全配置原则

12.4.1.1 测试环境网络安全服务配置原则

测试环境网络需具备抗攻击能力，通过部署入侵检测系统、入侵防护系统、防火墙、攻击防护设备及配套的管理流程共同实现，防攻击系统需要能及时检测到攻击行为，并通过手工或自动的方式阻断攻击行为。

为保证测试环境网络的安全性，宜配置的网络安全服务包括以下内容。

a）部署防病毒系统，建立病毒监控体系，及时发现并防止病毒对整个网络系统的危害。

b）建立辖内统一的网络时间协议（NTP）服务，用以统一整个测试环境网络设备的时间，以便精确确定故障问题时间。

c）建立日志服务体系，包括收集防火墙日志和网络设备日志，并建立相应的日志审计机制，便于对故障问题及安全事件进行分析。

d）部署非法外联检测系统，防止本单位用户同时连接内部内联网（Intranet）和互联网（Internet），避免发生直接互连的风险。

e）部署漏洞扫描系统，定期检测及发现所维护服务器的各种传输控制协议（TCP）端口的分配、提供的服务、软件版本，以及这些服务和软件的安全漏洞，防范攻击行为。

12.4.1.2 测试环境网络设备安全配置原则

测试环境网络设备应配置访问控制列表，配置合法登录声明。测试环境网络设备的型号原则上应和生产环境保持一致，路由器、交换机应启用密码加密功能。

12.4.2 测试环境网络规划原则

12.4.2.1 测试环境内联网规划原则

测试环境内联网规划应遵循以下原则。

a）内联网根据安全管理的需要划分为核心区、隔离区、接入区等安全区域，各安全区域间根据各自的风险分别部署防火墙、入侵检测等安全系统，建立专用的网管区域。

b）对于高风险网络出口，应采用异构防火墙结构，即接入层防火墙与应用层防火墙采用不同品牌设备。

c）除因测试需要需对网络架构进行重大调整外，测试环境内联网和生产环境网络应尽量保持网络结构的对等。

d）内联网无线网络接入用户应授权到个人，并使用加密方式对通信信道进行加密。

12.4.2.2 测试环境外联网规划原则

测试环境外联网网络规划应遵循以下原则。

a）外联网与企业合作单位网络进行连接时，需接入防火墙，并设立相应的安全策略，确保所有企业合作单位的网络通讯均经过防火墙，并且只允许合法访问到达外联网。

b）在外联网部署入侵防御系统，对从企业合作单位进入的数据流量进行安全威胁检测。

c）企业合作单位服务器只允许访问外联网的服务器，再由外联网服务器访问内联网服务器。

d）需通过路由过滤或者包过滤的方式进行控制，保证每个企业合作单位只能访问允许的网段，不能访问其他企业合作单位的网段。

e）针对测试环境虚拟专用网络（VPN），在互联网接入路由器、VPN 路由器等设备的相应接口配置相关防病毒、高风险端口访问控制列表。将 VPN 路由器的流量纳入入侵防御系统的日常监控中。

12.4.2.3 测试环境网络隔离控制原则

测试环境网络规划时需遵循二网隔离原则，将测试环境网络同生产环境网络进行隔离，并在客户端、测试服务器端、生产服务器端的交换机或防火墙等网络设备上分别实施访问控制。严格控制通过生产环境网段直接访问测试环境服务器及数据，严格控制测试环境网络和生产环境网络的互访互通。

12.4.3 测试环境网络安全等级划分原则

测试环境网络安全等级划分应按照应用系统中服务器功能和重要性的不同，实施不同层次的安全防护，以提高重要资源的安全防护水平。

对应用系统实施网络分层防护，有效地增加重要应用系统的安全防护纵深。

12.4.4 防火墙策略管理安全配置原则

防火墙策略管理安全配置应遵循以下原则。

a）各区域防火墙负责对本区域内部业务应用的访问控制，防火墙默认应设置为双向禁止的访问策略，访问策略需根据业务访问需求逐项开通。

b）防火墙策略要求精确到源互联网协议地址、目标互联网协议地址和目标端口号。对于开放端口范围过大的情况应经过本单位具备安全职责的岗位审批。

c）针对文件传输协议（FTP）、远程终端协议（TELNET）、简单邮件传输协议（SMTP）、网上基本输入输出系统（NETBIOS）、远程访问等高风险端口，应增加具备安全职责的岗位审批流程，并严格控制源地址范围和开放周期。

d）Internet 应接入防火墙，禁止对 Internet 全部打开访问链接策略。

e）对于没有防火墙保护的网络层级边界，通过路由器、交换机访问控制列表实现网络区域之间的访问控制，配置防病毒访问控制列表，防止病毒数据在网络中的传播。

13 测试环境资源管理

13.1 测试环境资源管理对象和目的

13.1.1 测试环境资源管理对象

测试环境资源管理对象包括测试环境中计算机及其外围配套设备（例如密码键盘、磁条读写器、打印及扫描设备、影像仪等）、数据通信及网络安全设备、机房环境设施、银行自助服务设备（例如自助回单打印机、发卡机、智能终端、产品领取机等）、移动设备（例如手机、平板电脑等）、专用机具（例如制卡机、封装机等）等设备。

13.1.2 测试环境资源管理目的

测试环境资源管理的目的是通过合理评估和资源需求的规划，有效利用资源，充分发挥测试环境资源的实际效益。

13.2 测试环境资源规划

测试环境资源规划时，应根据现有同类资源的使用及库存情况，综合考虑及评估新增资源需求和现有资源的更新需求，以及现有资源的使用状况，且结合本单位的资源调配计划，合理制定测试环境资源更新计划。

测试环境资源更新和购置工作计划应遵循的原则如下。

a）匹配性原则：资源的选择应同应用需求相匹配。优先选择成熟的设备，避免盲目追求新型号、高配置，造成资源浪费。

b）稳定性原则：对于关键资源的选择，应参考生产环境资源型号及配置，将稳定性作为第一原则，避免盲目追求新技术或使用未经过市场检验的新型设备。

c）安全性原则：在充分发挥现有资源使用效益的情况下，避免资源超期服役所带来的故障隐患和安全隐患。关键环节资源超出设计使用寿命时，原则上应及时进行更换。

13.3 测试环境计算机设备的安装与交付

测试环境计算机设备的安装与交付应遵循以下原则。

a）设备安装前，应对设备运行环境进行检查，确保供电、制冷、监控等设施能够满足运行要求。

b）设备安装过程中，应严格按照相关设备的安装要求、操作规范、网络准入要求执行。

c）设备安装完成后，应对设备运行情况进行验收确认。

13.4 测试环境资源维护

测试环境资源的维护工作主要包括日常监控、巡检、保养、健康检查、维护修理、扩容升级、停机管理等。

应定期对运行关键应用的资源的使用情况进行评估，评估内容包括但不限于日常及业务高峰时计算机设备的硬件和软件运行情况、中央处理器（CPU）、内存、存储资源使用率、微码版本等，应及时更新计算机设备驱动。

在进行设备维修、更换前，应通过消磁等方式销毁存储介质。应建立关键测试设备故障处理应急预案，明确设备发生故障时的应急处理流程。

13.5 测试环境资源回收

对于闲置或使用效率持续低下的资源应予以合理调整，对于不再使用的资源应及时进行回收。回收后的资源应根据测试环境资源规划及使用场景进行再分配或报废处理。

应针对回收的资源进行全面检查，并更新配置管理信息。

如测试环境计算机设备符合以下条件之一的，可申请进行设备回收技术评估。

a）设备达到使用期限要求。

b）设备因损坏无法维修。

c）设备维修成本过高。

d）设备无继续使用场景。

对于确认报废的测试环境计算机设备，必须符合国家电子类设备处置的相关法律法规，确保相关存储信息安全备份，在交付报废处置前完成消磁或物理粉碎处理。

密钥类设备报废时，密钥管理部门应作为第三方进行现场监督，核对设备序列号与登记序列号是否一致，并确保密钥被完全清除、密钥存储设备已进行物理破坏。

14 测试环境释放管理

14.1 测试环境释放管理对象和目的

14.1.1 测试环境释放管理对象

测试环境释放管理对象是测试环境资源的使用权。

14.1.2 测试环境释放管理目的

测试环境释放管理的目的是高效利用测试环境资源，实现资源环境最大化的使用和共享，节约测试环境运维的成本。

14.2 测试环境释放原则

测试环境释放应遵循以下原则。

a）未使用的环境资源应及时主动释放，包括已下线生产系统的测试环境、测试需求任务完结的测试环境等。

b）及时收回已释放的测试资源的使用权，并更新相关配置信息。

c）释放后的测试环境资源可不提供应用层面的运维活动。

d）释放后的测试环境可根据环境使用需求进行再分配。

15 证实方法

查看测试环境管理工作相关的台账、操作记录等是否按照本文件要求留存和管理，以及测试环境管理相关制度中的相关项是否与本文件中的要求一致。

参 考 文 献

[1] GB/T 9386—2008 计算机软件测试文档编制规范
[2] GB/T 22239—2019 信息安全技术 网络安全等级保护基本要求
[3] GB/T 35273—2020 信息安全技术 个人信息安全规范
[4] GB/T 37964—2019 信息安全技术 个人信息去标识化指南
[5] JR/T 0101—2013 银行业软件测试文档规范
[6] ISO/IEC/IEEE 29119-1:2022 软件和系统工程 软件测试 第1部分：一般概念（Software and systems engineering—Software testing—Part 1:General concepts）