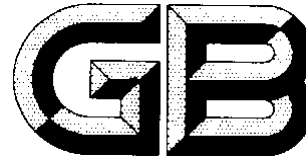


ICS

点击此处添加中国标准文献分类号



# 中华人民共和国国家标准

GB/T XXXXX—XXXX

## 信息安全技术 办公信息系统安全可靠测试规范

Information security technology - Security and reliable testing specification for office information systems

点击此处添加与国际标准一致性程度的标识

(征求意见稿)

XXXX - XX - XX 发布

XXXX - XX - XX

中华人民共和国国家质量监督检验检疫总局  
中国国家标准化管理委员会 发布

# 目 次

前言 .....	II
1 范围 .....	1
2 引用文件 .....	1
3 术语和缩略语 .....	1
4 环境测试 .....	3
5 基础硬件产品测试 .....	4
6 软件产品测试 .....	5
7 网络设施测试 .....	19
8 应用系统测试 .....	21
附录 A（资料性附录） .....	26
参考文献 .....	27

## 前 言

本标准按照GB/T 1.1-2009给出的规则起草。

本标准由全国信息安全标准化技术委员会（SAC/TC 260）提出并归口。

本标准主要起草单位：中国电子技术标准化研究院、软件与集成电路促进中心、工业和信息化部电子第五研究所、深圳赛西信息技术有限公司、北京赛西科技发展有限公司、西安电子科技大学、北京工业大学

本标准主要起草人：姚相振、刘贤刚、范科峰、高林、杨建军、唐一鸿、孙康健、刘龙庚、刘帅、李云婷、裴庆祺、杨震

# 办公信息系统安全可靠测试规范

## 1 范围

本标准规定了办公信息系统安全可靠的测试规范，包括环境测试规范、硬件测试规范、软件测试规范、网络设施测试规范以及应用系统测试规范。

本标准适用于指导党政部门的办公信息系统建设，包括系统设计、产品采购、系统集成等。

## 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 2887-2011 《计算机场地通用规范》
- GB 18030-2005 《信息交换用汉字编码字符集基本集的扩充》
- GB/T 28821-2012 《信息技术 关系数据管理系统技术要求》
- GB/T 26856-2011 《信息技术 中文办公软件基础要求及符合性测试规范》
- GB/T 20916-2007 《信息技术 中文办公软件文档格式规范》
- GB/T 18019-1999 《信息技术 包过滤防火墙安全技术要求》
- GB/T 26269-2010 《网络入侵检测系统技术要求》
- GB/T 28454-2012 《信息技术 安全技术 入侵检测系统的选择、部署和操作》
- GB/T 21052-2007 《信息安全技术 信息系统物理安全技术要求》
- GB/T 20272 《信息安全技术 操作系统安全技术要求》
- GB/T 20273 《信息安全技术 数据库管理系统安全技术要求》
- GB/T 21026-2007 《信息技术 中文办公软件应用编程接口规范》
- GB/T 9704-2012 《党政机关公文格式》
- GB/T 21050-2007 《信息安全技术 网络交换机安全技术要求》
- GB/T 18018-2007 《信息安全技术 路由器安全技术要求》
- GB/T 20281-2006 《信息安全技术 防火墙技术要求和测试评价方法》
- GB/T 20275-2006 《信息安全技术 入侵检测系统技术要求和测试评价方法》
- GB/T 20270-2006 《信息安全技术 网络基础安全技术要求》

## 3 术语和定义

下列术语和定义适用于本文件。

### 3.1

**信息系统 information system**

信息系统由计算机及其相关的配套部件、设备和设施构成，按照一定的应用目的和规则对信息进行采集、加工、存储、传输、检索等的人机系统。

## 3.2

**信息系统物理安全 physical security for information system**

为了保证信息系统安全可靠运行，确保信息系统在对信息进行采集、处理、传输、存储过程中，不致受到人为或自然因素的危害，而使信息丢失、泄露或破坏，对计算机设备、设施（包括机房建筑、供电、空调等）、环境人员、系统等采取适当的安全措施。

## 3.3

**服务器 server**

服务器是信息系统的主要组成部分，是信息系统中为客户端计算机提供特定应用服务的计算机系统，由硬件系统（如处理器、存储设备、网络连接设备等）和软件系统（如操作系统、数据库管理系统、应用系统等）组成。

## 3.4

**操作系统安全 security of operating system**

操作系统所存储、传输和处理的信息的保密性、完整性和可用性的表征。

## 3.5

**操作系统安全技术 security technology of operating system**

实现各种类型的操作系统安全需要的所有安全技术。

## 3.6

**数据库系统 database system**

储存、管理、处理和维持数据的软件系统，主要由数据库、数据库管理系统和数据库管理员组成。

## 3.7

**数据库管理系统 database management system**

用于建立、使用和维护数据库的软件。

## 3.8

**数据库管理系统安全 security of database management system**

数据库管理系统所存储、传输和处理的信息的保密性、完整性和可用性的表征。

## 3.9

**数据库管理系统安全技术 security technology of database management system**

实现各种类型的数据库管理系统安全需要的所有安全技术。

## 3.10

**中文办公软件 Chinese office software**

用于中文办公处理的一套完整的计算机应用程序和相关文档，主要包括文字处理、电子表格和演示文稿3个应用软件。

## 3.11

**路由器 router**

路由器是主要的网络节点设备，工作在网络层，通过路由选择算法决定流经数据的存储转发，并具备访问控制和安全扩展功能。

## 3.12

**防火墙 firewall**

一个或一组在不同安全策略的网络或安全域之间实施访问控制的系统。

## 3.13

**入侵检测系统 intrusion detection system**

用于监测信息系统中可能存在的影响信息系统资产的行为的软件或软硬件组合。它通常分为主机型和网络型两种，由控制台、探测器和/或主机代理组成。

## 3.14

**网络安全基础技术 basis technology of network security**

实现各种类型的网络系统安全需要的所有基础性安全技术。

## 3.15

**应用软件系统 application software system**

信息系统的重要组成部分，是指信息系统中对特定业务进行处理的软件系统。

## 3.16

**数据完整性 data integrity**

数据完整性泛指数据库中数据的正确性和一致性，包括实体完整性、参照完整性和用户定义完整性。

**4 符号和缩略语**

下列缩略语适用于本文件：

BIOS：基本输入输出系统（Basic Input Output System）

CA：数字证书认证中心（Certificate Authority）

CPU：中央处理器（Central Processing Unit）

DHCP：动态主机设置协议（Dynamic Host Configuration Protocol）

FTP：文件传输协议（File Transfer Protocol）

IP：网际协议（Internet Protocol）

MPP：大规模并行处理系统（Massive Parallel Processing）

PC：个人计算机（Personal Computer）

PDF：便携文件格式（Portable Document Format）

SSL：安全套接层（Secure Sockets Layer）

TCP：传输控制协议（Transport Control Protocol）

**5 环境测试****5.1 测试内容**

测试办公信息系统部署、运维的物理环境中机房的建设是否符合GB/T 2887-2011 《计算机场地通用规范》要求、物理环境是否符合GB/T 21052-2007《信息安全技术信息系统物理安全技术要求》要求。

## 5.2 测试方法

环境测试方法见表1。

表1 环境测试方法

序号	测试项	测试方法	备注
1	用户在中国大陆境内的办公信息系统部署、运维、数据备份的物理位置应位于中国大陆境内。	检查其应用服务器、运维服务器、数据库服务器是否位于中国大陆境内，并提供证明材料。	
2	办公信息系统部署、运维的机房建设对GB/T 2887-2011《计算机场地通用规范》的标准符合性测试	检查满足GB/T 2887-2011《计算机场地通用规范》的证明材料。	
3	办公信息系统部署、运维的物理环境对于GB/T 21052-2007《信息安全技术信息系统物理安全技术要求》的标准符合性测试	检查满足GB/T 21052-2007《信息安全技术信息系统物理安全技术要求》的证明材料。	

## 6 基础硬件产品测试

### 6.1 服务器

#### 6.1.1 测试内容

测试办公信息系统所采用的服务器硬件产品的产品结构、可扩充性、BIOS基本功能以及厂商所提供的技术资料完整性。

#### 6.1.2 测试方法

服务器测试方法见表2。

表2 服务器测试方法

序号	测试项	测试方法	备注
1	测试服务器的内存扩展能力	添加与被测服务器相适应的内存，在BIOS中检查内存容量与被测系统的实际内存容量是否符合，并检查被测服务器是否可以正常工作。	
2	测试服务器的以太网支持能力	检查是否具有以太网网络接口，测试被测服务器的网络速度是否达到1000Mb/S速度。	
3	测试BIOS的硬件信息显示能力	检查BIOS是否能够正确显示被测服务器的内存、硬盘、主板、CPU等的必要硬件信息。	
4	测试BIOS的中文显示能力	检查BIOS具有中文显示能力且内容正确。	

5	测试 BIOS 支持固件软件升级的能力	通过 BIOS 自动检测升级工具，检查 BIOS 固件版本信息及其对旧版本的更新能力，包括：全部模块更新、引导模块更新、内存模块更新能力等相关测试。	
6	测试 BIOS 支持对 CPU 及芯片组固件驱动、操作系统内核等的经过国家认可的第三方 CA 机构颁发的代码签名验证	测试系统启动加载过程必须与底层 BIOS 的安全验证接口进行基于证书的认证，经 BIOS 验证通过后系统方可启动引导加载过程。	
7	检查服务器应随机配套用户手册、保修卡等材料的完整性	检查被测服务器是否附带完整的随机配套用户手册、保修卡等材料。	

## 6.2 桌面机

### 6.2.1 测试内容

测试办公信息系统所采用的桌面机硬件产品的产品结构、可扩充性、BIOS 基本功能以及厂商所提供的技术资料完整性。

### 6.2.2 测试方法

桌面机测试方法见表3。

表3 桌面机测试方法

序号	测试项	测试方法	备注
1	测试桌面机的内存容量	在 BIOS 中检查被测桌面机的内存容量与所安装的实际内存容量是否吻合。	
2	测试桌面机的以太网支持能力	检查是否具有以太网网络接口，测试被测桌面机的网络速度是否达到 100Mb/S 速度。	
3	测试提供禁止无线网络模块功能	测试禁止无线网络模块功能是否正常	
4	测试 BIOS 的硬件信息显示能力	检查 BIOS 是否能够正确显示被测桌面机的内存、硬盘、主板、CPU 等的必要硬件信息。	
5	测试 BIOS 的中文显示能力	检查 BIOS 是否具有中文显示能力。	
6	测试 BIOS 支持固件软件升级的能力	通过 BIOS 自动检测升级工具，检查 BIOS 固件版本信息及其对旧版本的更新能力，包括：全部模块更新、引导模块更新、内存模块更新能力等相关测试。	
7	测试 BIOS 支持对 CPU 及芯片组固件驱动、操作系统内核等的经过国家认可的第三方 CA 机构颁发的代码签名验证	测试系统启动加载过程必须与底层 BIOS 的安全验证接口进行基于证书的认证，经 BIOS 验证通过后系统方可启动引导加载过程。	
8	检查桌面机应随机配套用户手册、保修卡等材料的完整性	检查被测桌面机是否附带完整的随机配套用户手册、保修卡等材料。	



## 7 软件产品测试

### 7.1 服务器操作系统

#### 7.1.1 测试内容

测试办公信息系统所采用的服务器操作系统的功能、认证机制、安全性以及厂商所提供的技术资料完整性。

#### 7.1.2 测试方法

服务器操作系统测试方法见表4。

表4 服务器操作系统测试方法

序号	测试项	测试方法	备注
1	应符合 GB 18030-2005《信息交换用汉字编码字符集基本集的扩充》	<p>在系统（分别在操作系统的用户界面、应用程序的用户界面、帮助信息、Console、CLI）、Web 浏览器、邮件客户端、应用程序（声音/图像播放器等）中测试，检查能否正确显示编码格式字符集中单字节、双字节、四字节、少数民族字符（蒙文编码、维吾尔文编码、藏文编码、彝文编码等）区所编码的字符；</p> <p>通过文本和图形编辑器输入、修改编码格式字符集中单字节、双字节、四字节、少数民族字符（蒙文编码、维吾尔文编码、藏文编码、彝文编码等）区所编码的字符，检查能否正确进行输入和修改；</p> <p>通过打印输出编码格式字符集中单字节、双字节、四字节、少数民族字符（蒙文编码、维吾尔文编码、藏文编码、彝文编码等）区所编码的字符，检查能否正确打印。</p>	
2	应满足 GB/T 20008-2005《信息安全技术操作系统安全评估准则》的安全标记保护三级要求	检查满足 GB/T 20008-2005《信息安全技术 操作系统安全评估准则》的安全标记保护三级要求的证明材料。	
3	测试是否提供支持设备驱动程序的添加和删除的管理工具	<p>在系统中接入显卡、声卡、网卡、键盘、鼠标等外设，测试驱动加载情况；</p> <p>针对某一特定设备，在系统中安装老版本的驱动后，安装新版本的驱动，在将新版本驱动卸载，测试系统驱动可否被正常添加和删除；</p> <p>热插入鼠标、键盘等外设，验证系统及外设的工作状态后将外设热拔出，测试设备插入后系统可否正常识别，设备工作正常，热拔出后系统自动删除该设备；</p> <p>通过系统驱动管理程序查询某一特定设</p>	

		备的状态以及设备与驱动程序的映射关系，测试系统提供的设备状态查询功能能否正常。	
4	测试是否提供系统故障监视与自动恢复，全面的系统信息采样等功能	<p>通过硬件变化、硬件损坏、文件系统错误、文件系统损坏、启动过程错误测试启动监视，测试引导启动时对系统加载过程的监视功能；</p> <p>通过桌面程序测试系统监视，测试图形化的系统监视器，测试系统运行时动态信息查看功能；</p> <p>通过系统提供的手段设置一个和多个检查点，关闭系统再启动并按检查点恢复，测试系统的检查点恢复机制。</p>	
5	测试是否支持负载均衡集群	<p>向作业管理系统提交并行的计算作业，检查各节点上的负载，测试系统提供的节点间的负载均衡机制是否有效；</p> <p>配置负载均衡策略，策略包含轮循均衡、权重轮循均衡、随机均衡、权重随机均衡、响应速度均衡、最少连接数均衡、处理能力均衡策略，并通过模拟相关并行的计算作业场景，测试配置的负载均衡策略是否有效；</p> <p>通过关机、断网、终止服务、挂起服务等方式模拟集群环境中的节点和应用故障，检查系统对故障节点上未完成的任务的处理，测试系统对节点的故障诊断和处理能力。</p>	
6	测试是否支持内核参数的配置	使用内核配置工具，安装或去除模块、配置相关参数，编译并安装内核，使用新内核重启，测试内核参数的配置是否有效。	
7	测试是否支持 TCP/IP 等常用网络协议	<p>通过系统提供的网络管理接口，编写客户、服务端程序测试网络常用协议，包括 TCP、UDP、IP（IPv4、IPv6）、ICMP、ARP、IPX/SPX、X. 25、ISDN、PPPoE、SLIP、PLIP、ATM；</p> <p>通过启动系统支持的 HTTP、FTP、DNS、NFS、SMTP、NTP、DHCP、SSH、POP3、SOAP、SSL 服务，分别在网络层协议使用 IPv4、IPv6 的情况下，在本地或远程运行客户端程序进行测试。</p>	
8	测试是否支持服务器应用软件包	<p>测试提供功能完善的网络浏览器；</p> <p>测试提供图形化工具支持访问 FTP 服务器；</p> <p>测试提供 ping 工具，支持按 IP 地址或 web 地址实现 ping 操作；</p> <p>提供查看图片的工具，支持的文件类型包括：BMP、JPG、GIF、TIF 等；</p> <p>测试提供 PostScript 文档查看器及 PDF</p>	

		<p>阅读器；</p> <p>测试提供文本编辑工具，支持新建、编辑、保存、打印文本文件，支持的文件格式包含 DOC、DOCX、ODF、TXT、RTF；</p> <p>测试提供压缩管理工具，支持文件和文件夹的压缩，支持 ZIP、GZIP、BZIP、TAR、RAR、AR 格式，能够在压缩文件中增加新的文件或删除部分文件；</p> <p>测试提供计算器工具，支持三角函数，实现先乘除后加减，有括号功能；</p> <p>测试提供图形化的为生僻字符编辑的工具；</p> <p>测试提供图形化的开发环境和调试环境。</p>	
9	测试是否支持服务器应用的本地及远程图形界面管理工具	测试是否支持 Email、FTP、DHCP、HTTP、NFS、DNS、网络代理服务的图形管理工具，并测试图形管理工具是否正常运行。	
10	测试访问控制结构，测试文件系统完整性检查工具	<p>测试查看文件系统信息，包含高速缓存页大小，文件系统使用过程事件记录，测试文件系统具有记录事件的日志系统和基于页的高速缓存能力；</p> <p>通过桌面程序或终端程序测试重要的文件和目录发生的改变事件是否能够被正确监视，并记录到系统日志中。</p>	
11	测试是否支持防火墙配置工具	<p>测试能够依据网络上传的每个 IP 包所含的源地址、目的地址、端口以及包形态等信息，对包进行过滤，控制封包的流通与否；</p> <p>测试能够控制网络防火墙网络接口，设定允许进出网络接口的条件以防止网络入侵。</p>	
12	测试是否支持多种认证机制	<p>测试至少支持以下 2 种或 2 种以上的认证机制：</p> <p>测试操作系统对用户口令进行强化管理，如对用户名和口令进行分开管理，实现强化管理的口令鉴别；</p> <p>测试操作系统能够采用动态口令鉴别机制，如动态口令；</p> <p>测试操作系统能够使用生物特征鉴别方式，如指纹、虹膜、人脸等生物特征；</p> <p>测试操作系统提供数字证书鉴别机制，如 USB Key。</p>	
13	应支持底层 BIOS 的安全验证及启动	测试系统启动加载过程必须与底层 BIOS 的安全验证接口进行基于证书的认证，经 BIOS 验证通过后系统方可启动引导加载过程。	

14	应禁止安装没有带证书签名的软件和固件组件	通过模拟来自非法证书签名的软件和固件组件的安装测试,验证系统禁止和隔离来自非法数据源的安装策略的有效性、完备性。	
15	应建立策略来管理软件的安装,防止未授权软件安装	验证服务器操作系统是否支持管理员手动创建、修改、配置、删除组策略,通过组策略命令行工具,检测面向特定用户或计算机策略设置的有效性,设置新的散列规则或修改旧的散列规则,检测其是否能阻止未授权软件的安装。	
16	应强制执行最低限度密码复杂度,保障账户安全	测试服务器操作系统在用户口令创建过程中,是否强制执行字符数(大、小写字母、数字和特殊字符)的组合,包括对每个类型的最低限度要求,当检测到口令未满足最低限度要求时,服务器操作系统是否自动采取相关行动(如:提示用户重新输入口令)。	
17	应使用加密机制来保护存储在操作系统数字媒体控制区以外的运输过程中的信息的保密性和完整性	测试服务器操作系统向数字媒体控制区以外传输过程中其是否可提供一条可信的安全路径,并提供加解密功能,检测对非该数据所属用户是否具有不可见性。	
18	应支持对操作系统和其安装的应用进行漏洞扫描的能力,并标识和报告可能影响系统或应用的新漏洞	测试服务器操作系统是否支持各类漏洞扫描工具和技术,其各类扫描工具应具备及时发现和列举系统、软件缺陷和不恰当的配置的能力,及时生成新的安全漏洞报告。	
19	应安装防篡改保护程序,保护系统组件和系统服务	检查服务器操作系统中的防篡改程序,并通过渗透性测试验证其对逆向工程、替代修改等威胁是否具有较强的识别能力和自我修复能力。	
20	应支持在用户丢失密码密钥时维持信息的可用性的能力	测试服务器操作系统是否根据符合国家的方法管理密钥,包括密钥的产生、分发、访问及摧毁,并在用户丢失后提供恢复措施,如:邮件方式、指纹方式、历史记录方式等。	
21	应检测软件和信息的未授权变更并通过执行信息系统的完整性扫描重新评价软件和信息完整性	测试服务器操作系统是否为软件及信息产生真实性证据(如:校验码、单向函数、数字签名),并具备实时监控的能力,当检测到完整性错误时,操作系统可采取相应行动(如:提示管理员)。	
22	应支持三权分立机制,重新划分操作系统管理员权限	检测不同权限的三个管理员角色,即安全管理员、系统管理员以及审计管理员的权限是否与访问控制策略相匹配。	
23	应支持缓冲区溢出防护机制、rootkit 防护机制和内核密封技术	检测服务器操作系统是否能够有效抵御缓冲区溢出和 rootkit 攻击,并测试具有相应权限的用户是否能够访问系统内核。	

24	应支持进程级安全审计，能够记录所有成功和不成功的操作	测试服务器操作系统是否在进程级提供安全审计相关功能，如审计日志、实时报警生成、潜在侵害分析、基于异常检测，基本审计查阅等。	
25	应禁用客体重用机制，保护系统剩余信息安全	测试服务器操作系统中客体在被释放(或删除)时，所占用的磁盘块中的内容是否被清空。	
26	服务器操作系统厂商应为产品测试提供所供应产品的接口、协议、加密方式等	验证服务器操作系统厂商为产品测试提供的产品接口、协议、加密方式的完备性和真实性，对实现安全功能进行验证。	
27	服务器操作系统厂商应支持根据用户需求对所供应产品的功能进行裁剪	根据用户常见使用模式，提出不同量级的功能裁剪需求，包括内核级、模块级、功能级等，服务器操作系统厂商按需求进行功能裁剪实现后，验证服务器操作系统厂商根据用户需求对功能进行裁剪的能力。	

## 7.2 桌面操作系统

### 7.2.1 测试内容

测试办公信息系统所采用的桌面操作系统的功能、安全性以及厂商所提供的技术资料的完整性。

### 7.2.2 测试方法

桌面操作系统测试方法见表5。

表5 桌面操作系统测试方法

序号	测试项	测试方法	备注
1	应符合 GB 18030-2005《信息交换用汉字编码字符集基本集的扩充》	在系统（分别在操作系统的用户界面、应用程序的用户界面、帮助信息、Console、CLI）、Web 浏览器、邮件客户端、应用程序（声音/图像播放器等）中测试，检查能否正确显示编码格式字符集中单字节、双字节、四字节、少数民族字符（蒙文编码、维吾尔文编码、藏文编码、彝文编码等）区所编码的字符； 通过文本和图形编辑器输入、修改编码格式字符集中单字节、双字节、四字节、少数民族字符（蒙文编码、维吾尔文编码、藏文编码、彝文编码等）区所编码的字符，检查能否正确进行输入和修改； 通过打印输出编码格式字符集中单字节、双字节、四字节、少数民族字符（蒙文编码、维吾尔文编码、藏文编码、彝文编码等）区所编码的字符，检查能否正确打印。	
2	应满足 GB/T 20008-2005《信息安全技术	检查满足 GB/T 20008-2005《信息安全技	

	操作系统安全评估准则》的安全标记保护三级要求	术 操作系统安全评估准则》的安全标记保护三级要求的证明材料。	
3	测试是否至少支持形码类、音码类等常用汉字输入法	测试提供五笔字型输入法，支持输入中文字符集； 测试提供拼音输入法，考察能否正确输入中文字符集，可以完成联想式输入，记忆词频，根据词频调整显示输入中文字符等功能； 测试输入法的状态条上的键盘标记能够弹出软键盘，软键盘的种类可包括数字序号、标点、特殊符号等，记录所提供的软键盘种类。	
4	测试是否至少提供宋体、仿宋、黑体、楷体、小标宋体等五种基本输出字体	测试在文本编辑器中输入中文、设置中文字体和字型，系统支持至少五种基本输出字体：宋体、仿宋、黑体、楷体、小标宋体，字型变换方式至少包括常规、倾斜、加粗、加粗并倾斜，其中默认字型为常规字型。	
5	应支持点阵、曲线两种中文字库	测试点阵字库包含 11X12、13X14、15X16、17X18 点阵； 测试曲线字库可缩放字型大小，字型正确，字体规范。	
6	应提供中文图形操作界面	检查系统所提供的图形用户界面中的菜单、标签、提示信息、帮助信息是否支持中文显示（专有术语和缩写词可用英文表示），界面中的中文字体无乱码。	
7	应支持中文打印	编辑中文文本，文本内容覆盖不同的字体字型，对文本进行打印输出，测试系统支持中文页面的打印，输出的文字内容、字体和字型正确，无乱码。	
8	应支持分辨率调整	测试通过桌面程序进行显示器配置，包括配置分辨率、刷新率、色深的调整。	
9	应支持打印机、投影仪、扫描仪、数码相机等外围设备	测试支持打印机，包括打印机识别、文档打印、图片打印、数据和电子表格、字体、纸张方向、接口等测试内容； 测试支持投影仪，包括投影仪识别，切换投影模式、投影配置等测试内容； 测试支持扫描仪，包括扫描仪识别、扫描速度、扫面清晰度、扫描精度、色彩准确度、线条图、灰度图、对纸张适应能力等测试内容。	
10	应提供电子日历、计算器、文本编辑器等常用工具	测试提供电子日历工具，支持日历的浏览功能； 测试提供文本编辑工具，支持新建、编辑、保存、打印文本文件，支持的文件格式包	

		含 DOC、DOCX、ODF、TXT、RTF； 测试提供计算器工具，支持三角函数，实现先乘除后加减，有括号功能。	
11	应提供多媒体播放工具和图像处理工具	测试提供多媒体播放工具，支持 MPEG1、MPEG2、MPEG4 编码格式的音视频文件； 测试提供图像处理工具，支持的文件类型包括：BMP、JPG、GIF、TIF。	
12	应提供统一的控制面板入口，提供硬件配置工具、用户管理工具和桌面管理工具等	<p>测试硬件配置工具、用户管理工具和桌面管理工具等能够通过统一的控制面板进行访问，并检测相关管理工具实现以下功能：</p> <p>显示管理工具</p> <ul style="list-style-type: none"> <li>• 支持调整显示器配置、显卡配置，测试能否配置分辨率、刷新率、色深等；</li> <li>• 支持对桌面风格及背景图案进行配置；对屏幕保护进行配置。</li> </ul> <p>声音管理工具</p> <ul style="list-style-type: none"> <li>• 支持检测声卡，或从列表中选取声卡型号，支持测试音播放；</li> <li>• 支持音量调节。</li> </ul> <p>键盘及鼠标管理工具</p> <ol style="list-style-type: none"> <li>1) 键盘管理 <ul style="list-style-type: none"> <li>• 支持设置键盘属性，配置快捷键信息等；</li> <li>• 支持设置重复键的延时和速度；</li> <li>• 支持设置光标闪烁的频率。</li> </ul> </li> <li>2) 鼠标管理 <ul style="list-style-type: none"> <li>• 支持配置和使用三键和滚轮；</li> <li>• 支持设置使用习惯、鼠标响应性能。</li> </ul> </li> </ol> <p>网卡管理工具</p> <ul style="list-style-type: none"> <li>• 支持自动检测网卡，或从列表选取网卡型号；</li> <li>• 支持设置主机名、IP、掩码、网关、DNS 等参数，支持配置多块网卡，网卡</li> </ul>	

		<p>配置完成后,能自动检测 IP 冲突。</p> <p>打印机管理工具</p> <ul style="list-style-type: none"> <li>支持对本地、远程以及与其它操作系统共享的打印机配置(包括新建打印机、编辑打印机属性、删除打印机等),打印测试页,设置默认打印机,浏览删除打印任务,设置打印机的分辨率、纸张,查看选中打印机的特性描述,包括常规、接口、驱动程序、标题、用户等信息。</li> </ul> <p>硬件设备的管理工具</p> <ul style="list-style-type: none"> <li>提供图形化的查看系统硬件信息的工具;</li> <li>支持增加或更换显卡、声卡、网卡、Modem 等设备,启动时系统能够检测到并自动配置(登录之前)或弹出配置窗口(进入桌面之后),USB 移动存储设备自动加载至指定路径。</li> </ul> <p>用户管理工具</p> <ul style="list-style-type: none"> <li>提供用户管理,包括建立、删除账号和组,设置用户口令,账号及组的信息查询,除超级管理员外,其他人只能修改自己的口令;</li> <li>超级管理员可以设置账号和密码的过期时间。</li> </ul>	
13	测试是否支持 FTP、Telnet 等网络客户端应用	<p>测试是否支持图形化工具支持访问 FTP 服务器;</p> <p>测试是否支持命令行或图形化工具支持访问 Telnet 服务器。</p>	
14	测试是否支持邮件客户端、浏览器等上网工具	<p>测试是否支持图形化的邮件客户端工具;</p> <p>测试是否支持网络浏览器工具。</p>	



15	测试是否支持实现跨操作系统的打印机等网络资源共享	<p>测试以 IP 及以计算机名可以访问网络上的其他计算机；</p> <p>测试对 Windows (XP, Win7、Win8) 系统各类中、英文文件及文件夹的访问，对 Windows (XP, Win7、Win8) 系统中文件（文件夹）名包含特殊字符（@#\$\$等）的文件或文件夹的访问；</p> <p>测试对 Liunx 系统各类中、英文文件及文件夹的访问，对 Liunx 文件（文件夹）名包含特殊字符（@#\$\$等）的文件或文件夹的访问；</p> <p>测试跨操作系统间的打印机访问能力；</p> <p>测试网络间相互复制、粘贴文件/文件夹，支持大文件（容量在 1G 以上）的拷贝及多个文件（数量在 50 个以上）同时拷贝。</p>	
16	应支持第三方辅助设备的驱动	测试支持第三方辅助设备的驱动，第三方辅助设备可包括手写板、指纹识别、扫码枪等。	
17	应支持锁屏操作，新建及结束任务操作，新建、修改名称、复制、剪切、粘贴、解压缩、删除文件（夹）等资源管理操作	<p>通过桌面程序测试资源浏览功能，测试通过地址栏访问本机内容的功能；测试不同的视图来显示文件或文件夹，测试图标视图和列表视图；测试根据文件名、大小、时间、类型等对文件进行排序的功能；</p> <p>通过桌面程序测试文件（夹）操作功能，测试文件（夹）的新建、删除、复制、移动、重命名、权限设置、剪切、粘贴、解压缩操作；</p> <p>通过设置或快捷键方式测试锁屏操作。</p>	
18	应禁止安装没有带证书签名的软件和固件组件	通过模拟来自非法证书签名的软件和固件组件的安装测试，验证系统禁止和隔离来自非法数据源的安装策略的有效性、完备性。	
19	应建立策略来管理软件的安装，防止未授权软件安装	验证桌面操作系统是否支持管理员手动创建、修改、配置、删除组策略，通过组策略命令行工具，检测面向特定用户或计算机策略设置的有效性，设置新的散列规则或修改旧的散列规则，检测其是否能阻止未授权软件的安装。	
20	应强制执行最低限度密码复杂度，保障账户安全	测试桌面操作系统在用户口令创建过程中，是否强制执行字符数（大、小写字母、数字和特殊字符）的组合，包括对每个类型的最低限度要求，当检测到口令未满足最低限度要求时，服务器操作系统是否自动采取相关行动（如：提示用户重新输入口令）。	
21	应使用加密机制来保护存储在操作系统数字媒体控制区以外的运输过程中的信息的保密性和完整性	测试桌面操作系统向数字媒体控制区以外传输过程中其是否可提供一条可信的安全路径，并提供加解密功能，检测对非	

		该数据所属用户是否具有不可见性。	
22	应支持对操作系统和其安装的应用进行漏洞扫描的能力，并标识和报告可能影响系统或应用的新漏洞	测试桌面操作系统是否支持各类漏洞扫描工具和技术，其各类扫描工具应具备及时发现和列举系统、软件缺陷和不恰当的配置的能力，及时生成新的安全漏洞报告。	
23	应安装防篡改保护程序，保护系统组件和系统服务	检查桌面操作系统中的防篡改程序，并通过渗透性测试验证其对逆向工程、替代修改等威胁是否具有较强的识别能力和自我修复能力。	
24	应支持在用户丢失密码密钥时维持信息的可用性的能力	测试桌面操作系统是否根据符合国家的方法管理密钥，包括密钥的产生、分发、访问及摧毁，并在用户丢失后提供恢复措施，如：邮件方式、指纹方式、历史记录方式等。	
25	应检测软件和信息的未授权变更并通过执行信息系统的完整性扫描重新评价软件和信息的完整性	测试桌面操作系统是否为软件及信息产生真实性证据（如：校验码、单向函数、数字签名），并具备实时监控的能力，当检测到完整性错误时，操作系统可采取相应行动（如：提示管理员）。	
26	桌面操作系统厂商应为产品测试提供所供应产品的接口、协议、加密方式等	验证桌面操作系统厂商为产品测试提供的产品接口、协议、加密方式的完备性和真实性，对安全功能进行验证。	
27	桌面操作系统厂商应支持根据用户需求对所供应产品的功能进行裁剪	提出不同量级的功能裁剪需求，包括内核级、模块级、功能级等，桌面操作系统厂商按需求进行功能裁剪实现后，验证桌面操作系统厂商根据用户需求对功能进行裁剪的能力。	

### 7.3 数据库管理系统

#### 7.3.1 测试内容

测试办公信息系统所采用的数据库管理系统的功能、安全性以及厂商所提供的技术资料完整性。

#### 7.3.2 测试方法

数据库管理系统测试方法见表6。

表6 数据库管理系统测试方法

序号	测试项	测试方法	备注
1	应符合 GB/T 28821-2012《信息技术 关系数据管理系统技术要求》	检查满足 GB/T 28821-2012《信息技术关系数据管理系统技术要求》的证明材料，证明材料应有第三方机构提供。	
2	测试数据库管理系统对于 GB 18030-2005《信息交换用汉字编码字符集基本集的扩充》的标准符合性测试	在数据库管理系统中，查看服务器级、数据库级、表级、列级的字符集以及连接字符集，检查能否正确显示编码格式字符集中单字节、双字节、四字节、少数民族字	

		<p>符（蒙文编码、维吾尔文编码、藏文编码、彝文编码等）区所编码的字符；</p> <p>通过文本和图形编辑器输入和修改服务器级、数据库级、表级、列级的字符集以及连接字符集，检查能否正确输入和修改；</p> <p>通过打印输出服务器级、数据库级、表级、列级的字符集以及连接字符集，检查能否正确打印。</p>	
3	检查 GB/T 20273-2006《信息安全技术 数据库管理系统安全技术要求》第三级或以上等级：安全标记保护级的能力证明	检查满足 GB/T 20273-2006《信息安全技术 数据库管理系统安全技术要求》第三级或以上等级：安全标记保护级的证明材料。	
4	测试数据库管理系统的备份功能	依据技术文档和用户手册，测试被测数据库的库级全量备份、增量备份、表级全量备份等备份功能是否正常。	
5	测试数据库管理系统的还原功能	依据技术文档和用户手册，测试被测数据库的库级全量还原、增量还原、表级全量还原等还原功能是否工作正常。	
6	测试事务故障恢复功能	测试在系统掉电重启或在数据库服务器运行过程中发生的非正常中断（条件：掉电重启，数据恢复正常）的情况下，被测数据库是否可恢复到故障点。	
7	测试数据库管理系统的复制功能	依据技术文档和用户手册，测试被测数据库的库级的数据库复制、模式级的数据库复制、表级的数据库复制等功能是否工作正常，检测被复制数据与源数据是否一致。	
8	测试数据库管理系统的性能监测与查询优化功能	依据技术文档和用户手册，检查被测数据库是否具有数据库监控、死锁监测等性能监测与查询优化工具，测试被测数据库的数据库监控、死锁监测等性能监测与查询优化工具是否工作正常。	
9	测试数据库管理系统与其他厂商数据库之间的数据迁移	测试被测数据库的数据导入/导出组件/工具是否支持文本文件、通用数据库表、约束、视图等对象和数据的迁移功能；依据技术文档和用户手册，测试是否支持与其他厂商数据库之间的数据迁移功能。	
10	测试数据库管理系统的大规模并行处理能力	依据技术文档和用户手册，创建测试指令，测试使用国际通用基准测试模型；搭建多个节点的如 MPP 等架构，连接 MPP 等架构中任意节点，执行创建测试表，测试建表是否成功，多个节点上是否均有表；测试使用数据装载工具，连接到 MPP 等架构上进行数据加载，测试数据是否加载成功，连接 MPP 中任意节点是否可查询到各表数据。	
11	测试数据库管理系统的行存表、列存表混	依据技术文档和用户手册，建立行存表和	

	合存储、检索功能	列存表, 测试在一条指令中同时访问行存表和列存表, 检查操作是否成功。	
12	数据库管理系统厂商应为产品测试提供所供应产品的接口、协议、加密方式等	验证数据库管理系统厂商为产品测试提供的产品接口、协议、加密方式的完备性和真实性, 对安全功能进行验证。	
13	数据库管理系统厂商应支持根据用户需求对所供应产品的功能进行裁剪	提出不同量级的功能裁剪需求, 包括内核级、模块级、功能级等, 数据库管理系统厂商按需求进行功能裁剪实现后, 验证数据库管理系统厂商根据用户需求对功能进行裁剪的能力。	
14	数据库稳定性测试	验证数据库在正常业务压力下的 7*24 小时测试稳定性表现	

## 7.4 应用服务器

### 7.4.1 测试内容

测试办公信息系统所采用的应用服务器的功能、安全性以及厂商所提供的技术资料的完整性。

### 7.4.2 测试方法

应用服务器测试方法见表7。

表7 应用服务器测试方法

序号	测试项	测试方法	备注
1	应符合 GB 18030-2005《信息交换用汉字编码字符集基本集的扩充》	<p>在系统（分别在操作系统的用户界面、应用程序的用户界面、帮助信息、Console、CLI）、Web 浏览器、邮件客户端、应用程序（声音/图像播放器等）中测试, 检查能否正确显示编码格式字符集中单字节、双字节、四字节、少数民族字符（蒙文编码、维吾尔文编码、藏文编码、彝文编码等）区所编码的字符；</p> <p>通过文本和图形编辑器输入、修改编码格式字符集中单字节、双字节、四字节、少数民族字符（蒙文编码、维吾尔文编码、藏文编码、彝文编码等）区所编码的字符, 检查能否正确进行输入和修改；</p> <p>通过打印输出编码格式字符集中单字节、双字节、四字节、少数民族字符（蒙文编码、维吾尔文编码、藏文编码、彝文编码等）区所编码的字符, 检查能否正确打印。</p>	
2	测试是否支持事务服务	测试各种分布式事务服务, 能够通过该	

		接口来启动、提交和回滚事务。	
3	测试是否支持消息服务	测试消息服务，包括支持队列的建立、删除；支持连接的建立、关闭；支持订阅的建立、删除；支持消息头/消息体的各个字段属性编辑；支持消息 Selector；支持消息过滤；	
4	测试是否支持安全服务	测试提供安全服务，包括支持在标准的 HTTPS 端口（默认为 443 端口）上发布 HTTPS 服务；支持 JACC 规范。	
5	测试是否支持名字和目录服务	测试支持符合 JNDI 规范的安全服务，包括支持对名字空间的管理；支持非本地缺省的名字服务器；支持 ENC (Enterprise Naming Context)；支持事件上下文空间；支持名字上下文 (JNDI Context)。	
6	测试是否支持邮件服务	测试支持符合 JMail 规范的邮件服务，包括可以发送附件、设置邮件发送的优先级、支持多种格式的邮件发送、密件发送/(CC)抄送/紧急信件发送功能。	
7	测试是否支持数据访问服务	测试符合 JDBC 规范的数据访问服务，支持通过 JDBC 连接到数据库，并能够执行数据的增、删、改、查及事务的回滚操作。	
8	测试是否支持企业应用集成服务	测试符合 JCA 规范的企业应用集成服务，能够通过基于 JCA 的 EIS(企业信息系统)连接适配器连接并使用非 JAVA 类的企业信息系统。	
9	测试是否支持对应用的部署、调试和卸载	测试支持对应用的部署，实现对应用程序包的部署、重启，支持动态部署； 测试提供对应用的调试，实现应用程序的远程调试和动态调试； 测试提供对应用的卸载，实现反部署、停止和卸载。	
10	测试是否支持对系统性能进行监控和调优、日志管理的管理工具	测试支持对系统性能进行监控和调优、日志管理的管理工具，实现对 HTTP、数据库连接池、JVM 虚拟机等的资源计数器，实现实时监控，并可进行关键参数的配置调优；实现日志功能，能够对日志信息进行配置管理。	
11	测试是否支持 Web 组件开发的可视化集成开发工具	测试是否能够以独立或插件形式，提供支持 Web 组件开发的可视化集成开发工具，集成开发工具能够实现对应用服务器的配置部署、启动停止服务、专用工程管理，支持远程部署和调试功能。	
12	应支持在不中断系统运行的情况下动态部署和卸载应用的功能	测试支持在不中断系统运行的情况下动态部署和卸载应用，动态部署包括更新一个文件、一个库文件、一个文件包时的动	

		态部署。	
13	测试是否支持高速缓存、负载均衡、失效恢复的第三方 Web 服务器	测试支持第三方 Web 服务器实现高速缓存、负载均衡、失效恢复功能，包括对应用资源文件的高速缓存；实现静态和动态页面转发；支持一组服务器从逻辑上作为单独的服务器运行，但共同分担系统负载；支持提供附加的服务器来保证一旦其中的某个服务器宕机时服务的延续性；支持确保用户会话生命周期在一台服务器上的完整性；支持通过代码指定或者自动通过底层平台的通信链路进行自动切换到集群中另一节点，延续失败节点上的服务。	
14	测试具有与其他应用系统连接和集成的能力	测试支持通过各类通信协议或程序接口实现与其他应用系统连接和集成功能。	
15	测试是否支持保证数据源恢复和保证事务一致性的系统故障恢复能力	模拟断电、网络、停服务、挂起服务等故障，测试提供保证数据源恢复和保证事务一致性的系统故障恢复能力。	
16	应用服务器厂商应为产品测试提供所供产品的接口、协议、加密方式等，必要时提供安全功能的实现表示	验证应用服务器厂商为产品测试提供的产品接口、协议、加密方式的完备性和真实性，对安全功能进行验证。	
17	应用服务器厂商应支持根据用户需求对所供应产品的功能进行裁剪	提出不同量级的功能裁剪需求，包括内核级、模块级、功能级等，应用服务器厂商按需求进行功能裁剪实现后，验证应用服务器厂商根据用户需求对功能进行裁剪的能力。	
18	测试应用服务器网络接口部分对网络数据流的实时监控能力	测试应用服务器设备同时监控或检测多个网络分片的能力，实现高速聚集的网络数据流的负载均衡；采用主动测试和被动两种不同的检测方法，验证应用服务器依据既定的安全策略和规则，对不同的网络应用行为提供的报警和阻断的能力。	
19	测试是否支持防恶意代码软件	测试应用服务器是否支持各类防恶意代码软件，其各类防恶意软件应具备及时发现和清除进入系统内部的恶意代码、维护恶意软件代码库升级和更新的能力。	
20	测试应用服务器数据的完整性和保密性	检查信息系统的数据完整性保护情况，包括传输完整性、存储完整性保护措施等；检查信息系统的数据保密性保护情况，包括传输保密性和存储保密性。	
21	测试应用服务器是否支持对登录用户进行身份标识和鉴别	测试应用服务器是否提供专用的登陆控制模块对登陆用户身份进行身份验证和鉴别，并检查服务器是否提供了登陆失败处理功能，包括：限制非法登陆次数、登陆失败次数超过设定值则结束会话等； 测试已注册用户身份登陆、查看登陆是否成功；测试错误用户名和口令登陆系统，验证鉴别失败处理是否有效。	

22	应支持访问控制功能，控制用户对服务器数据的访问	测试应用服务器是否提供访问控制用户身份组/用户对服务器数据的访问，检测授权主体是否具有设置用户对服务器数据访问的权限功能，并依据访问控制列表用户和权限的关系，查看不同用户的权限是否与设定的权限是否具有 consistency。	
23	应支持抵御拒绝服务攻击的能力，如，部署边界保护装置，增加容量、带宽并结合服务冗余	模拟分布式拒绝服务攻击测试，观测受攻击应用服务器丢包率、吞吐量等相关情况，分析其边界网关是否具备限制外部 web 只与内部受管接口通信的能力，并对入侵事件提供报警。检测其容量和带宽在受攻击状态是否能满足应用服务器维持正常服务。	
24	应在通信会话结束时或在静默后终止与该会话相关联的网络连接	测试应用服务器会话在一方未作出任何响应时，另一方能够自动结束会话，并释放相应进程及系统资源的能力。	
25	应用服务器应保护公共可用信息和应用的完整性和可用性	检查服务器是否能阻止非授权用户修改或破坏系统公共可用信息，并在检测到完整性错误或可用性破坏时采取必要的恢复措施。	
26	应用服务器应部署垃圾邮件防护机制	检查服务器是否能配置管理策略和程序，部署垃圾邮件防护机制，通过电子邮件，电子邮件附件、web 访问或者其他通用方法传送的非请求的消息，校验其垃圾邮件防护机制的完备性。	

## 7.5 办公软件

### 7.5.1 测试内容

测试办公信息系统所采用的办公软件的功能、安全性以及厂商所提供的技术资料的完整性。

### 7.5.2 测试方法

办公软件测试方法见表8。

表8 办公软件测试方法

序号	测试项	测试方法	备注
1	办公软件对于 GB/T 26856-2011《信息技术 中文办公软件基础要求及符合性测试规范》的标准符合性测试	<p>从中文办公软件的功能性、可靠性、易用性、效率、适应性、中文特性、文档格式、产品描述和用户文档 9 个方面进行测试；</p> <p>采用黑盒测试，验证中文办公软件所有功能的完整性、正确性和一致性；</p> <p>选择性能测试工具，测试中文办公软件的性能；</p> <p>在功能测试的同时，进行可靠性、易用性、适应性、中文特性、产品描述和用户文档测试。</p>	

2	办公软件对于 GB/T 20916-2007《信息技术 中文办公软件文档格式规范》的标准符合性测试	<p>检查办公软件生成的文档是否符合文档格式规范：</p> <p>通过选择存储格式，查看存储格式能否支持用户选择 XML 是否压缩、图像采用有损压缩或无损压缩以及声音文件采用有损压缩或是无损压缩；</p> <p>通过读写 txt/xml/html 格式的文本文件，wav/mid/mp3/amr/ogg/au/ra/snd 格式的声音文件，bmp/tif/gif/png/jpg/svg/pbm/ras 格式的图像文件、avi/mpeg1/mpeg2/mpeg4/qt/rm/asf 格式的视频文件，测试办公软件能否支持上述格式文件。</p>	
3	办公软件对于 GB 18030-2005《信息交换用汉字编码字符集基本集的扩充》的标准符合性测试	<p>在办公软件输入界面中测试，检查能否正确显示编码格式字符集中单字节、双字节、四字节、少数民族字符（蒙文编码、维吾尔文编码、藏文编码、彝文编码等）区所编码的字符；</p> <p>在办公软件输入界面中输入、修改编码格式字符集中单字节、双字节、四字节、少数民族字符（蒙文编码、维吾尔文编码、藏文编码、彝文编码等）区所编码的字符，检查能否正确进行输入和修改。</p>	
4	办公软件对于 GB/T 21026-2007《信息技术 中文办公软件应用编程接口规范》的标准符合性测试	测试是否符合 GB/T 21026-2007《信息技术中文办公软件应用编程接口规范》的技术要求。	
5	办公软件对于 GB/T 9704-2012《党政机关公文格式》标准的电子公文格式模板及排版的标准符合性测试	<p>测试能否编排公文的版头、主体、版记：</p> <p>版头可支持份号、密级和保密期限、紧急程度、发文机关标志、发文字号、签发人、版头中的分隔线这些元素；</p> <p>主体可支持标题、主送机关、正文、附件说明、发文机关署名、成文日期和印章、附注、附件这些元素；</p> <p>版记可支持版记中的分隔线、抄送机关印发机关和印发日期、页码。</p>	
6	测试办公软件对浏览器的支持能力	检查是否具有浏览器插件，并测试是否能够跨浏览器环境正常运行。	
7	测试办公软件对 PDF 文件格式的支持能力	测试是否支持 PDF 文件，检查是否具有 PDF 阅读工具，是否能够打开查阅 PDF 文件、导出 PDF 格式文件，并检查是否可以对导出的 PDF 格式文件进行打印、选择、加密等控制操作。	
8	办公软件厂商应为产品测试提供所供应产品的接口、协议、加密方式等	验证办公软件厂商为产品测试提供的产品接口、协议、加密方式的完备性和真实性，对安全功能进行验证。	
9	办公软件厂商应支持应支持根据用户需求	提出不同量级的功能裁剪需求，包括内核	



	求对所供应产品的功能进行裁剪	级、模块级、功能级等，办公软件厂商按需求进行功能裁剪实现后，验证办公软件厂商根据用户需求对功能进行裁剪的能力。	
10	办公软件应支持对文件加密的能力	检查办公软件是否具有加密选项，并测试在拥有正确密钥的情况下，是否具有正确打开加密文件的能力。	
11	办公软件应支持对文件编辑过程中定时备份的能力	模拟断电、网络、停服务、挂起服务等故障，测试提供保证数据源恢复和保证事务一致性的文件恢复能力。	

## 8 网络设施测试

### 8.1 网络设备

#### 8.1.1 测试内容

测试办公信息系统所采用的交换机、路由器等网络设备的功能以及安全性。

#### 8.1.2 测试方法

网络设备测试方法见表9。

表9 网络设备测试方法

序号	测试项	测试方法	备注
1	检查 GB/T 21050-2007《信息安全技术 网络交换机安全技术要求（评估保证级 3）》的能力证明	检查 GB/T 21050-2007《信息安全技术 网络交换机安全技术要求（评估保证级 3）》的标准符合性测试结果证明材料。	
2	检查 GB/T 18018-2007《信息安全技术 路由器安全技术要求》的能力证明	检查 GB/T 18018-2007《信息安全技术 路由器安全技术要求》的标准符合性测试结果证明材料。	

### 8.2 安全设备

#### 8.2.1 测试内容

测试办公信息系统所采用的防火墙和入侵检测系统等安全设备的功能以及安全性。

#### 8.2.2 测试方法

安全设备测试方法见表10。

表10 安全设备测试方法

序号	测试项	测试方法	备注
1	防火墙应符合 GB/T 20281-2006《信息安全技术 防火墙技术要求和测试评价方法》	检查 GB/T 20281-2006《信息安全技术 防火墙技术要求和测试评价方法》的标准符合性测试结果证明材料。	

2	入侵检测系统应符合 GB/T 26269-2010《网络入侵检测系统技术要求》	检查 GB/T 26269-2010《网络入侵检测系统技术要求》的标准符合性测试结果证明材料。	
3	入侵检测系统应符合 GB/T 28454-2012《信息技术 安全技术 入侵检测系统的选择、部署和操作》	检查 GB/T 28454-2012《信息技术 安全技术 入侵检测系统的选择、部署和操作》的标准符合性测试结果证明材料。	
4	入侵检测系统应符合 GB/T 20275-2006《信息安全技术 入侵检测系统技术要求和测试评价方法》	检查 GB/T 20275-2006《信息安全技术 入侵检测系统技术要求和测试评价方法》的标准符合性测试结果证明材料。	

## 9 应用系统测试

### 9.1 功能

#### 9.1.1 测试内容

测试办公信息系统的功能，包括公文管理、档案管理、公告、通知、会议管理、个人工作区、个人信息管理、在线人员列表、管理员用户等。

#### 9.1.2 测试方法

办公信息系统功能性测试方法见表11。

表11 办公信息系统功能性测试方法

序号	测试项	测试方法	备注
1	公文管理功能	通过操作应用系统测试公文流转功能，测试拟稿、核稿、编辑、审核、撤销、退回、签发、选择下一环节、发送、签收、会签、登记、拟办、审阅、分办、承办、办结、归档等功能，测试增加和删除附件功能，测试流程跟踪和查看功能。	
2	档案管理功能	通过操作应用系统测试档案管理功能，测试公文归档、归档查询功能。	
3	公告功能	通过操作应用系统测试公告管理功能，测试新建、修改、删除、发布等功能。	
4	通知功能	通过操作应用系统测试通知功能，测试新建、修改、删除、发布等功能。	
5	会议管理功能	通过操作应用系统测试会议室管理功能，测试新建、修改、删除、查询会议室等功能；通过操作应用系统测试会议安排功能，测试新建、修改、删除、查询、打印会议信息等功能。	
6	个人工作区功能	通过操作应用系统测试个人工作区功能，测试个人待办、个人已办功能。	
7	个人信息管理功能	通过操作应用系统测试个人信息管理功	

		能，测试修改个人信息、修改个人密码功能。	
8	在线人员列表功能	通过操作应用系统测试在线人员列表功能功能，测试在线人员的姓名、所属部门、职位信息等。	
9	管理员用户	通过管理员用户登录应用系统，测试管理员用户支持用户管理、统一权限管理等功能，测试用户的新建、修改、删除功能，测试基于功能授权功能，测试基于用户授权功能。	

## 9.2 安全性

### 9.2.1 测试内容

测试办公信息系统的安全性，包括身份鉴别、访问控制、客体重用、安全审计、安全标记、数据完整性等。

### 9.2.2 测试方法

办公信息系统安全性测试方法见表13。

表12 办公信息系统安全性测试方法

序号	测试项	测试方法	备注
1	测试系统的身份鉴别功能	检查系统是否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；检查系统不存在重复身份标识；检查系统对于登录失败能否采取结束会话、限制非法登录次数和自动退出等措施。	
2	测试系统的访问控制功能	检查系统能否控制用户对文件、数据库表等客体的访问；检查授权主体能否配置访问控制策略；检查系统能否控制用户对有敏感标记重要信息的操作。	
3	测试系统的客体重用	验证在计算机信息系统可信计算基的空闲存储客体空间中，对客体初始指定、分配或再分配一个主体之前，是否已撤销客体所含信息的所有授权；验证当主体获得对一个已被释放的客体的访问权时，当前主体是否无法获得原主体活动所产生的任何信息。	
4	测试系统的安全审计功能	查看审计记录，检查其是否包含了应用系统重要安全事件并覆盖所有用户，检查其是否包括了事件的日期、事件、发起者、类型、描述和结果；通过尝试人为删除、修改或覆盖审计记录，检查系统能否阻止删除、修改或覆盖行为；通过对审计记录进行统计、查询、生成审计报表操作，检查操作结果的正确性。	

5	测试系统的数据完整性	<p>检查系统能否阻止非授权用户修改或破坏系统管理数据、鉴别信息和重要数据；</p> <p>检查系统能否检测到系统管理数据、鉴别信息和重要数据在传输过程中完整性受到破坏，并在检测到完整性错误时采取必要的恢复措施；</p> <p>检查系统能否检测到系统管理数据、鉴别信息和重要数据在存储过程中完整性受到破坏，并在检测到完整性错误时采取必要的恢复措施。</p>	
6	测试系统的密码技术	检查系统中所采用的密码技术，能否满足国家密码主管部门的要求。	
7	测试系统的边界保护能力	<p>检查系统是否具有监视并控制发生在应用系统外部边界上和系统内的关键内部边界上通信的能力；</p> <p>检查系统在连接外部网络或其他系统的接口上使用的边界保护装置是否符合规范。</p>	

### 9.3 可靠性

#### 9.3.1 测试内容

可靠办公信息系统的可靠性，包括成熟度、容错性、易恢复性等。

#### 9.3.2 测试方法

办公信息系统可靠性测试方法见表14。

表13 办公信息系统可靠性测试方法

序号	测试项	测试方法	备注
1	系统长时间运行的能力	通过人工和工具相结合的方式，7×24小时运行应用系统，验证应用系统服务器端、客户端能支持7×24小时稳定运行，不崩溃不丢失数据。	
2	系统的数据有效性检验功能	通过边界值分析法、等价类划分法等方法设计测试数据，检查系统是否提供数据有效性检验功能，保证输入的数据格式或长度符合系统设定的要求。	
3	系统对用户非法的输入或操作的容错能力	通过边界值分析法、等价类划分法、错误推断法、场景法等方法设计非法的测试数据，测试用户非法的输入或操作时，系统不崩溃、不退出。	
4	系统的自动保护功能	人工模拟制造网络故障，验证由于网络故障所导致的系统故障恢复后，系统可恢复到故障点状态，数据不丢失。	

### 9.4 易用性

### 9.4.1 测试内容

可靠办公信息系统的易用性，包括易理解性、易操作性、易学习性等。

### 9.4.2 测试方法

办公信息系统易用性测试方法见表15。

表14 办公信息系统易用性测试方法

序号	测试项	测试方法	备注
1	用户手册	通过检查系统提供用户手册，对照系统实际操作，确认手册中的功能描述与软件的实际功能一致。	
2	过程文档	通过检查系统研制过程中形成的所有文档，确认文档内容语言简练、前后一致、易于理解以及语句无歧义。	
3	页面布局	通过检查系统各页面，确认系统页面布局合理，不过于密集，也不过于空旷，合理利用空间。	
4	系统的提示、警告、或错误说明	通过实际操作应用系统，确认系统的提示、警告、或错误说明清楚、明了、恰当，避免歧义。	
5	必填项标识	通过检查系统各编辑页面，确认编辑页面中的必填项都给出了标识。	
6	“非法”的输入或操作，系统应给予提示信息	通过实际操作应用系统，确认系统对于用户非法的输入或操作，给予提示信息，且提示信息能引导用户进行正确输入或操作。	
7	对可能造成数据无法恢复的操作，系统应给予提示信息	通过实际操作应用系统，确认系统对于可能造成数据无法恢复的操作，给予提示信息，给用户放弃选择的机会。	
8	日期类型数据输入应提供日历选择功能	通过检查系统各页面，确认日期类型数据输入提供了日历选择功能。	
9	系统应支持快捷键操作	通过实际操作应用系统，确认系统对于Ctrl-A全选、Ctrl-C拷贝、Ctrl-V粘贴、Ctrl-X剪切、Ctrl-Z撤消等快捷键的支持。	
10	Tab键变更光标焦点	通过实际操作应用系统，确认系统中有多个输入框的页面，支持通过Tab键变更光标焦点，按照从左到右、从上到下的原则。	

## 天億网络安全

「天億网络安全」全面介绍网络安全相关知识、安全建设方案、分享网络安全行业法律法规及相关政策，一个学习网络安全知识、技术、业务交流的全国性平台。

「天億网络安全」每天推送高质量的优秀博文，并为读者建立**网络安全知识、技术、业务交流群**，**安全技术沙龙群**，公众号关联的**【群友通讯录】**；天億网络安全**【知识星球】**可下载大量网络安全相关学习资料。

