

ICS 33.040
M 10



中华人民共和国通信行业标准

YD/T 3162-2016

邮件系统安全防护检测要求

Security protection testing requirements for the mail system

2016-07-11 发布

2016-10-01 实施

中华人民共和国工业和信息化部 发布

目 次

前 言.....II

1 范围.....1

2 规范性引用文件.....1

3 术语、定义和缩略语.....1

 3.1 术语和定义.....1

 3.2 缩略语.....2

4 邮件系统安全防护检测概述.....3

 4.1 安全防护检测范围.....3

 4.2 安全防护检测对象.....3

 4.3 安全防护检测环境.....3

5 邮件系统安全防护检测要求.....4

 5.1 第1级要求.....4

 5.2 第2级要求.....12

 5.3 第3级要求.....48

 5.4 第4级要求.....63

 5.5 第5级要求.....63

参考文献.....64

前 言

本标准是“电信网和互联网安全防护体系”系列标准之一。该系列标准的结构及名称预计如下：

1. 《电信网和互联网安全防护管理指南》
2. 《电信网和互联网安全等级保护实施指南》
3. 《电信网和互联网安全风险评估实施指南》
4. 《电信网和互联网灾难备份及恢复实施指南》
5. 《固定通信网安全防护要求》
6. 《固定通信网安全防护检测要求》
7. 《移动通信网安全防护要求》
8. 《移动通信网安全防护检测要求》
9. 《互联网安全防护要求》
10. 《互联网安全防护检测要求》
11. 《增值业务网—消息网安全防护要求》
12. 《增值业务网—消息网安全防护检测要求》
13. 《增值业务网—智能网安全防护要求》
14. 《增值业务网—智能网安全防护检测要求》
15. 《接入网安全防护要求》
16. 《接入网安全防护检测要求》
17. 《传送网安全防护要求》
18. 《传送网安全防护检测要求》
19. 《IP承载网安全防护要求》
20. 《IP承载网安全防护检测要求》
21. 《信令网安全防护要求》
22. 《信令网安全防护检测要求》
23. 《同步网安全防护要求》
24. 《同步网安全防护检测要求》
25. 《支撑网安全防护要求》
26. 《支撑网安全防护检测要求》
27. 《非核心生产单元安全防护要求》
28. 《非核心生产单元安全防护检测要求》
29. 《电信网和互联网物理环境安全等级保护要求》
30. 《电信网和互联网物理环境安全等级保护检测要求》
31. 《电信网和互联网管理安全等级保护要求》
32. 《电信网和互联网管理安全等级保护检测要求》

33. 《域名系统安全防护要求》
34. 《域名系统安全防护检测要求》
35. 《网上营业厅安全防护要求》
36. 《网上营业厅安全防护检测要求》
37. 《WAP网关系统安全防护要求》
38. 《WAP网关系统安全防护检测要求》
39. 《电信网和互联网信息服务业务系统安全防护要求》
40. 《电信网和互联网信息服务业务系统安全防护检测要求》
41. 《增值业务网 即时消息业务系统安全防护要求》
42. 《增值业务网 即时消息业务系统安全防护检测要求》
43. 《域名注册系统安全防护要求》
44. 《域名注册系统安全防护检测要求》
45. 《移动互联网应用商店安全防护要求》
46. 《移动互联网应用商店安全防护检测要求》
47. 《互联网内容分发网络安全防护要求》
48. 《互联网内容分发网络安全防护检测要求》
49. 《互联网数据中心安全防护要求》
50. 《互联网数据中心安全防护检测要求》
51. 《移动互联网应用安全防护要求》
52. 《移动互联网应用安全防护检测要求》
53. 《公众无线局域网安全防护要求》
54. 《公众无线局域网安全防护检测要求》
55. 《电信网和互联网安全防护基线配置要求及检测要求 网络设备》
56. 《电信网和互联网安全防护基线配置要求及检测要求 安全设备》
57. 《电信网和互联网安全防护基线配置要求及检测要求 操作系统》
58. 《电信网和互联网安全防护基线配置要求及检测要求 数据库》
59. 《电信网和互联网安全防护基线配置要求及检测要求 中间件》
60. 《电信网和互联网安全防护基线配置要求及检测要求 WEB应用系统》
61. 《电信和互联网用户个人电子信息保护通用技术要求和管埋要求》
62. 《电信和互联网用户个人电子信息保护检测要求》
63. 《互联网接入服务安全防护要求》
64. 《互联网接入服务安全防护检测要求》
65. 《网络交易安全防护要求》
66. 《网络交易安全防护检测要求》
67. 《邮件系统安全防护要求》
68. 《邮件系统安全防护检测要求》(本标准)
69. 《公有云服务安全防护要求》

YD/T 3162-2016

70. 《公有云服务安全防护检测要求》

本标准按照GB/T1.1-2009给出的规则起草。

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这些专利的责任。

本标准由中国通信标准化协会提出并归口。

本标准起草单位：中国信息通信研究院、中国电信集团公司、中国联合网络通信集团有限公司。

本标准主要起草人：李 强、魏 薇、苏 鹏、牛 云、姜 楠、刘险峰。

邮件系统安全防护检测要求

1 范围

本标准规定了邮件系统分安全保护等级的安全防护检测要求，涉及到业务及应用安全、网络安全、设备及软件系统安全、物理安全和管理安全的检测要求。

本标准适用于公众电信网和互联网中的邮件系统。

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，仅所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。

- YD/T 1754-2008 电信网和互联网物理环境安全等级保护要求
- YD/T 1756-2008 电信网和互联网管理安全等级保护要求
- YD/T 2692-2014 电信网和互联网用户个人电子信息保护通用技术要求和
- YD/T 2698-2014 电信网和互联网安全防护基线配置要求及检测要求 网络设备
- YD/T 2699-2014 电信网和互联网安全防护基线配置要求及检测要求 安全设备
- YD/T 2700-2014 电信网和互联网安全防护基线配置要求及检测要求 数据库
- YD/T 2701-2014 电信网和互联网安全防护基线配置要求及检测要求 操作系统
- YD/T 2702-2014 电信网和互联网安全防护基线配置要求及检测要求 中间件
- YD/T 2703-2014 电信网和互联网安全防护基线配置要求及检测要求 WEB应用系统

3 术语、定义和缩略语

3.1 术语和定义

下列术语和定义适用于本文件。

3.1.1

邮件系统安全等级 Security Classification of Mail System

邮件系统安全重要程度的表征。重要程度可从邮件系统受到破坏后，对国家安全、社会秩序、经济运行、公共利益、业务运营企业造成的损害来衡量。

3.1.2

邮件系统安全等级保护 Classified Security Protection of Mail System

对邮件系统分等级实施安全保护。

3.1.3

邮件系统安全风险 Security Risk of Mail System

人为或自然的威胁可能利用邮件系统中存在的脆弱性导致安全事件的发生及造成的影响。

3.1.4

邮件系统资产 Asset of Mail System

YD/T 3162-2016

邮件系统中具有价值的资源，是安全防护保护的对象。邮件系统中的资产可能是以多种形式存在，无形的、有形的、硬件、软件，包括物理布局、通信设备、物理线路、数据、软件、文档、规程、业务、人员、管理等各种类型的资源，如邮件系统的主机、网络布局等。

3.1.5

邮件系统威胁 Threat of Mail System

可能导致对邮件系统产生危害的不希望事件潜在起因，它可能是人为的，也可能是非人为的；可能是无意失误，也可能是恶意攻击。常见的邮件系统威胁有光缆中断、设备节点失效、火灾、水灾、垃圾邮件、邮件病毒、钓鱼邮件、拒绝服务攻击等。

3.1.6

邮件系统脆弱性 Vulnerability of Mail System

邮件系统中存在的弱点、缺陷与不足，不直接对资产造成危害，但可能被威胁所利用从而危及资产的安全。

3.1.7

邮件系统灾难 Disaster of Mail System

由于各种原因，造成邮件系统故障或瘫痪，使邮件系统支持的业务功能停顿或服务水平不可接受、达到特定的时间的突发性事件。

3.1.8

邮件系统灾难备份 Backup for Disaster Recovery of Mail System

为了邮件系统灾难恢复而对相关网络要素进行备份的过程。

3.1.9

邮件系统灾难恢复 Disaster Recovery of Mail System

为了将邮件系统从灾难造成的故障或瘫痪状态恢复到正常运行状态或部分正常运行状态、并将其支持的业务功能从灾难造成的不正常状态恢复到可接受状态，而设计的活动和流程。

3.1.10

业务使用用户 Business users

注册邮件、使用邮件的用户。

3.1.11

后台管理用户 Manage Users

对邮件系统进行日常运维的后台管理用户。

3.1.12

客户端 Client

登陆邮件系统的客户端软件，包括邮件系统自开发客户端和第三方客户端。

3.2 缩略语

下列缩略语适用于本文件。

DDoS	Distributed Denial of Service	分布式拒绝服务
DNS	Domain Name System	域名系统
DoS	Denial of Service	拒绝服务

IMAP	Internet Mail Access Protocol	互联网邮件访问协议
POP	Post Office Protocol	邮局协议
SMTP	Simple Mail Transfer Protocol	简单邮件传输协议
SNMP	Simple Network Management Protocol	简单网络管理协议

4 邮件系统安全防护检测概述

4.1 安全防护检测范围

本标准的安全防护检测范围与《邮件系统安全防护要求》一致，检测内容包括业务及应用安全、网络安全、设备及软件系统安全、物理安全和管理安全。

4.2 安全防护检测对象

邮件系统安全防护检测对象是公众电信网和互联网中的邮件系统，本标准主要对邮件系统各项安全防护要求的实施进行检测。

4.3 安全防护检测环境

对邮件系统相关业务系统的安全防护检测需在现网中进行，其检测环境结构示意图如图1所示。

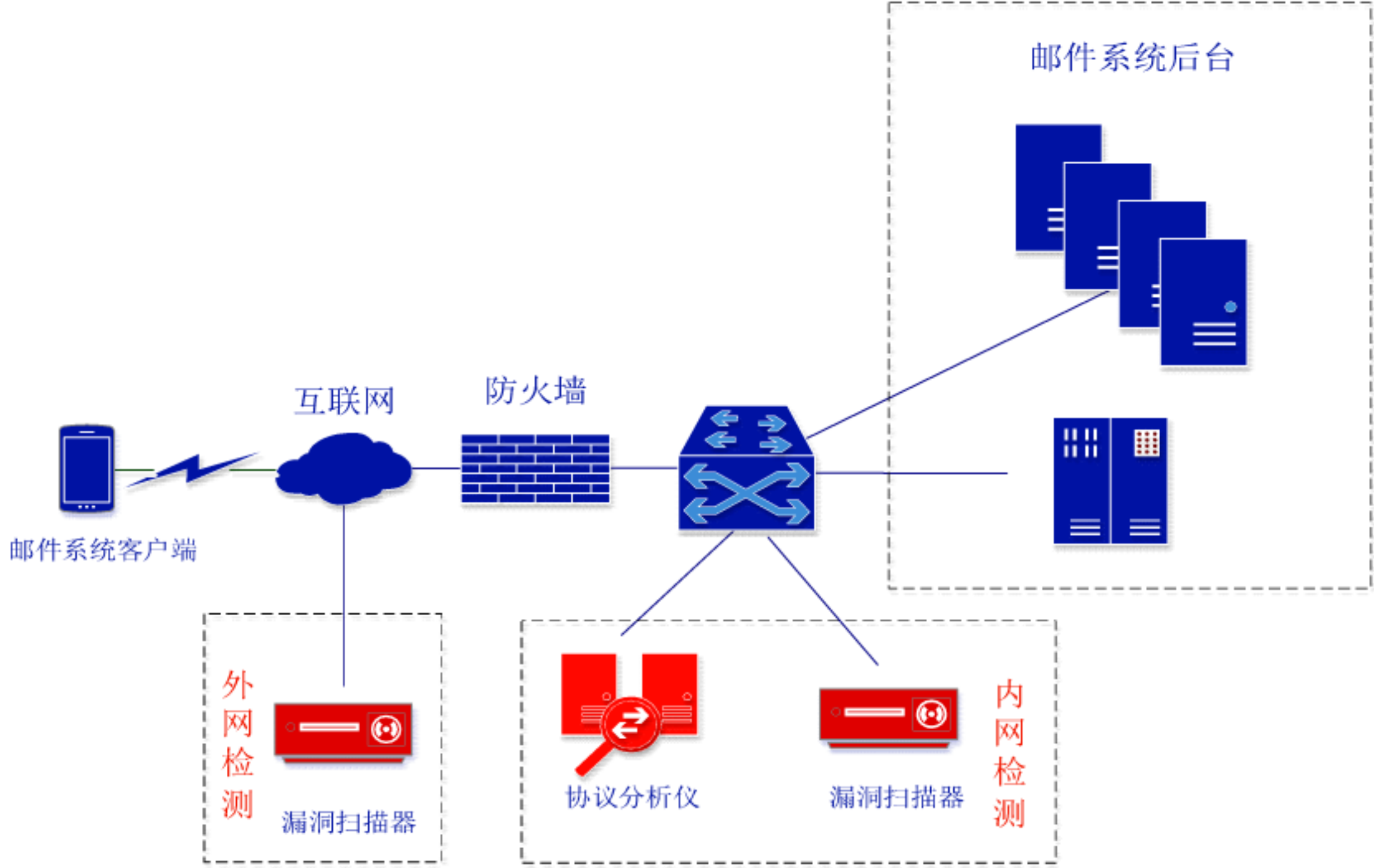


图1 邮件系统安全防护检测环境结构示意图

被测对象包括：邮件系统客户端、后台基础设备（如主机、服务器、路由器、交换机等）及业务应用系统（如注册、业务处理等）。

测试工具包括：嗅探工具（应支持网络流量抓包、解析等功能），端口探测工具（应支持对常用端口和指定端口的扫描），协议分析仪（应支持相关协议的抓包、解析等功能），漏洞扫描器（应支持主机扫描、端口扫描、口令破解、漏洞检测等功能）等。

YD/T 3162-2016

5 邮件系统安全防护检测要求

5.1 第 1 级要求

5.1.1 业务及应用安全

5.1.1.1 身份鉴别

测试编号：邮件系统-第 1 级-业务及应用安全-身份鉴别-01
测试项目：《邮件系统安全防护要求》5.1.1.1-a，应提供专用的登录控制模块对登录系统的业务使用用户进行身份标识和鉴别
测试步骤： 1) 访谈邮件系统运维和安全管理人員，检查业务设计/验收文档、业务安全策略、业务管理和配置文档； 2) 查看邮件系统的功能模块，是否具有身份鉴别模块
预期结果： 1) 相关文档中有身份鉴别模块描述； 2) 具有身份鉴别模块
判定原则： 达到以上预期结果，则通过，否则不通过

5.1.1.2 访问控制

测试编号：邮件系统-第 1 级-业务及应用安全-访问控制-01
测试项目：《邮件系统安全防护要求》5.1.1.2-a，应提供业务使用用户、后台管理用户访问控制功能
测试步骤： 1) 访谈邮件系统运维和安全管理人員，检查业务设计/验收文档、业务安全策略、业务管理和配置文档； 2) 检查邮件系统是否提供访问控制功能，检查系统安全策略配置选项，是否含有严格限制各用户的访问权限的各项内容； 3) 使用测试账号对系统资源进行访问，验证测试账号是否能够访问权限以内的资源，验证测试账号是否能够访问权限以外的资源
预期结果： 1) 邮件系统提供访问控制功能，系统安全策略配置选项中，含有严格限制各用户访问权限的各项内容； 2) 测试账号能够访问权限以内的资源； 3) 测试账号不能访问权限以外的资源
判定原则： 达到以上预期结果，则通过，否则不通过

5.1.1.3 信息保护

测试编号：邮件系统-第 1 级-业务及应用安全-信息保护-01
测试项目：《邮件系统安全防护要 求》5.1.1.3-a，应满足 YD/T 2692-2014《电信网和互联网用户个人电子信息保护通用技术要求和 管理要求》
测试步骤： 1) 访谈邮件系统运维人员，查看邮件系统设计/验收文档等是否符合 YD/T 2692-2014《电信网和互联网用户个人电子信息保护通用技术要求和 管理要求》中相关要求； 2) 检查邮件系统在使用用户数据信息时，是否符合 YD/T 2692-2014《电信网和互联网用户个人电子信息保护通用技术要求和 管理要求》中相关要求
预期结果： 1) 邮件系统设计/验收文档等符合 YD/T 2692-2014《电信网和互联网用户个人电子信息保护通用技术要求和 管理要求》中相关要求； 2) 邮件系统在使用用户数据信息时符合 YD/T 2692-2014《电信网和互联网用户个人电子信息保护通用技术要求和 管理要求》中相关要求
判定原则： 达到以上预期结果，则通过，否则不通过

5.1.1.4 Web 安全

测试编号：邮件系统-第 1 级-业务及应用安全-Web 安全-01
测试项目：《邮件系统安全防护要求》5.1.1.4-a，应满足 YD/T 2703-2014《电信网和互联网安全防护基线配置要求及检测要 Web 应用系统》要求
测试步骤： 1) 访谈邮件系统运维和安全管理 人员，检查邮件系统设计/验收文档等是否符合 YD/T 2703-2014《电信网和互联网安全防护基线配置要求及检测要求 Web 应用系统》中相关要求； 2) 检查邮件系统 Web 应用系统安全基线配置是否符合 YD/T 2703-2014《电信网和互联网安全防护基线配置要求及检测要求-Web 应用系统》中相关要求
预期结果： 1) 邮件系统设计/验收文档等符合 YD/T 2703-2014《电信网和互联网安全防护基线配置要求及检测要求-Web 应用系统》中相关要求； 2) 邮件系统 Web 应用系统安全基线配置符合 YD/T 2703-2014《电信网和互联网安全防护基线配置要求及检测要求-Web 应用系统》中相关要求
判定原则： 达到以上预期结果，则通过，否则不通过

5.1.1.5 对外接口安全

测试编号：邮件系统-第 1 级-业务及应用安全-对外接口安全-01
测试项目：《邮件系统安全防护要求》5.1.1.5-a，应提供数据有效性检验功能，保证通过接口输入或通过通信接口输入的数据格式或长度符合系统设定要求
测试步骤： 1) 访谈相关技术人员，检查业务设计/验收文档、业务安全策略、业务管理和配置文档，检查文档中是否有数据有效性校验功能，对接口数据的格式或长度是否有规定； 2) 测试输入不同格式或长度数据，检查邮件系统是否提供数据有效性检验功能
预期结果： 1) 设计/验收文档中有数据有效性校验功能，且对接口数据的格式或长度做了规定； 2) 邮件系统提供数据有效性检验功能，通过接口输入或通过通信接口输入的数据格式或长度是否符合系统设定要求
判定原则： 达到以上预期结果，则通过，否则不通过

5.1.2 网络安全

5.1.2.1 网络结构

测试编号：邮件系统-第 1 级-网络安全-网络结构-01
测试项目：《邮件系统安全防护要求》5.1.2.1-a，应绘制与当前运行情况相符的系统拓扑结构图
测试步骤： 1) 访谈相关技术人员，检查业务设计/验收文档、业务安全策略、业务管理和配置文档，检查邮件系统是否绘制与当前运行情况相符的系统拓扑结构图； 2) 进入现场检查网络及设备实际组网情况，检查是否与系统拓扑结构图相一致
预期结果： 1) 已绘制与当前运行情况相符的系统拓扑结构图； 2) 网络及设备实际组网情况与系统拓扑结构图相一致
判定原则： 达到以上预期结果，则通过，否则不通过

5.1.2.2 网络监测

测试编号：邮件系统-第 1 级-网络安全-网络监测-01
测试项目：《邮件系统安全防护要求》5.1.2.2-a，应在系统边界部署访问安全监测设备，并启用有效的安全监测控制策略
测试步骤： 1) 检查系统边界是否部署了访问安全监测设备，是否启用了有效的控制策略； 2) 通过技术手段测试相关系统能否在边界处抵御和防范各类攻击和入侵
预期结果： 1) 系统边界部署了访问安全监测设备且启用了有效的控制策略； 2) 系统能有效抵御和防范各种攻击和入侵
判定原则： 达到以上预期结果，则通过，否则不通过

5.1.2.3 安全审计

测试编号：邮件系统-第 1 级-网络安全-安全审计-01
测试项目：《邮件系统安全防护要求》5.1.2.3-a，应对系统中的重要设备运行状况、网络流量监测信息、系统管理及维护等进行日志记录，并且保留一定期限（至少 180 天）
测试步骤： 1) 访谈网络运维人员，检查系统设计/验收文档、系统安全策略、系统管理和配置文档、审计记录/报告； 2) 检查审计日志记录是否包括重要设备运行状况、网络流量监测信息、系统管理及维护等方面，保留期限是否达到 180 天
预期结果： 审计记录/报告包括重要设备运行状况、网络流量监测信息、系统管理及维护等方面信息，且保留期限达到 180 天
判定原则： 达到以上预期结果，则通过，否则不通过

5.1.3 设备及软件系统安全

5.1.3.1 网络及安全设备

测试编号：邮件系统-第 1 级-设备及软件系统安全-网络及安全设备-01
测试项目：《邮件系统安全防护要求》5.1.3.1-a，各类路由器、交换机等网络设备应满足相关通信行业标准要求，具有进网许可证
测试步骤： 1) 检查各类路由器、交换机等网络设备是否满足相关通信行业标准要求； 2) 检查各类路由器、交换机等网络设备是否具有进网许可证
预期结果： 1) 各类路由器、交换机等网络设备均满足相关通信行业标准要求； 2) 各类路由器、交换机等网络设备均具有进网许可证
判定原则： 达到以上预期结果，则通过，否则不通过

测试编号：邮件系统-第 1 级-设备及软件系统安全-网络及安全设备-02
测试项目：《邮件系统安全防护要求》5.1.3.1-b，应满足 YD/T 2698-2014《电信网和互联网安全防护基线配置要求及检测要求 网络设备》要求
测试步骤： 1) 检查邮件系统设计/验收文档等是否符合 YD/T 2698-2014《电信网和互联网安全防护基线配置要求及检测要求 网络设备》中相关要求； 2) 检查邮件系统网络设备安全基线配置是否符合 YD/T 2698-2014《电信网和互联网安全防护基线配置要求及检测要求 网络设备》中相关要求
预期结果： 1) 邮件系统设计/验收文档等符合 YD/T 2698-2014《电信网和互联网安全防护基线配置要求及检测要求 网络设备》中相关要求； 2) 邮件系统网络设备安全基线配置符合 YD/T 2698-2014《电信网和互联网安全防护基线配置要求及检测要求 网络设备》中相关要求
判定原则： 达到以上预期结果，则通过，否则不通过

测试编号：邮件系统-第 1 级-设备及软件系统安全-网络及安全设备-03
测试项目：《邮件系统安全防护要求》5.1.3.1-c，应满足 YD/T 2699-2014《电信网和互联网安全防护基线配置要求及检测要求 安全设备》要求
<p>测试步骤：</p> <p>1) 检查邮件系统设计/验收文档等是否符合 YD/T 2699-2014《电信网和互联网安全防护基线配置要求及检测要求 安全设备》中相关要求；</p> <p>2) 检查邮件系统安全设备安全基线配置是否符合 YD/T 2699-2014《电信网和互联网安全防护基线配置要求及检测要求 安全设备》中相关要求</p>
<p>预期结果：</p> <p>1) 邮件系统设计/验收文档等符合 YD/T 2699-2014《电信网和互联网安全防护基线配置要求及检测要求 安全设备》中相关要求；</p> <p>2) 邮件系统安全设备安全基线配置符合 YD/T 2699-2014《电信网和互联网安全防护基线配置要求及检测要求 安全设备》中相关要求</p>
<p>判定原则：</p> <p>达到以上预期结果，则通过，否则不通过</p>

5.1.3.2 通用主机操作系统

测试编号：邮件系统-第 1 级-设备及软件系统安全-通用主机操作系统- 01
测试项目：《邮件系统安全防护要求》5.1.3.2-a，应满足 YD/T 2701-2014《电信网和互联网安全防护基线配置要求及检测要求 操作系统》要求
<p>测试步骤：</p> <p>1) 检查邮件系统设计/验收文档等是否符合 YD/T 2701-2014《电信网和互联网安全防护基线配置要求及检测要求 操作系统》中相关要求；</p> <p>2) 检查邮件系统中主机操作系统安全基线配置是否符合 YD/T 2701-2014《电信网和互联网安全防护基线配置要求及检测要求 操作系统》中相关要求</p>
<p>预期结果：</p> <p>1) 邮件系统设计/验收文档等符合 YD/T 2701-2014《电信网和互联网安全防护基线配置要求及检测要求 操作系统》中相关要求；</p> <p>2) 邮件系统中主机操作系统安全基线配置符合 YD/T 2701-2014《电信网和互联网安全防护基线配置要求及检测要求 操作系统》中相关要求</p>
<p>判定原则：</p> <p>达到以上预期结果，则通过，否则不通过</p>

测试编号：邮件系统-第 1 级-设备及软件系统安全-通用主机操作系统- 02
测试项目：《邮件系统安全防护要求》5.1.3.2-b，各个功能模块的计算机运维终端、服务器等设备的审计范围应覆盖到主机/服务器上的每个操作系统用户
测试步骤： 1) 应访谈相关技术人员，检查业务设计/验收文档、业务安全策略、业务管理和配置文档、审计记录/报告； 2) 检查邮件系统中各个功能模块的计算机运维终端、服务器等设备的审计记录，检查审计范围是否覆盖到主机/服务器上的每个操作系统用户
预期结果： 1) 邮件系统中各个功能模块的计算机运维终端、服务器等设备均保存审计记录； 2) 审计范围覆盖到主机/服务器上的每个操作系统用户
判定原则： 达到以上预期结果，则通过，否则不通过

5.1.3.3 数据库及中间件软件

测试编号：邮件系统-第 1 级-设备及软件系统安全-数据及中间件软件-01
测试项目：《邮件系统安全防护要求》5.1.3.3-a，应满足《电信网和互联网安全防护基线配置要求及检测要求-中间件》要求
测试步骤： 1) 检查邮件系统设计/验收文档等是否符合 YD/T 2702-2014《电信网和互联网安全防护基线配置要求及检测要求 中间件》中相关要求； 2) 检查邮件系统中间件是否符合 YD/T 2702-2014《电信网和互联网安全防护基线配置要求及检测要求 中间件》中相关要求
预期结果： 1) 邮件系统设计/验收文档等符合 YD/T 2702-2014《电信网和互联网安全防护基线配置要求及检测要求 中间件》中相关要求； 2) 邮件系统中间件符合 YD/T 2702-2014《电信网和互联网安全防护基线配置要求及检测要求 中间件》中相关要求
判定原则： 达到以上预期结果，则通过，否则不通过

测试编号：邮件系统-第 1 级-设备及软件系统安全-数据库及中间件软件-02
测试项目：《邮件系统安全防护要求》5.1.3.3.1-b，应满足 YD/T 2700-2014《电信网和互联网安全防护基线配置要求及检测要求 数据库》要求
<p>测试步骤：</p> <ol style="list-style-type: none"> 1) 检查邮件系统设计/验收文档等是否符合 YD/T 2700-2014《电信网和互联网安全防护基线配置要求及检测要求 数据库》中相关要求； 2) 检查邮件系统数据库是否符合 YD/T 2700-2014《电信网和互联网安全防护基线配置要求及检测要求 数据库》中相关要求
<p>预期结果：</p> <ol style="list-style-type: none"> 1) 邮件系统设计/验收文档等符合 YD/T 2700-2014《电信网和互联网安全防护基线配置要求及检测要求 数据库》中相关要求； 2) 邮件系统数据库符合 YD/T 2700-2014《电信网和互联网安全防护基线配置要求及检测要求 数据库》中相关要求
<p>判定原则：</p> <p>达到以上预期结果，则通过，否则不通过</p>

测试编号：邮件系统-第 1 级-设备及软件系统安全-数据及中间件软件-03
测试项目：《邮件系统安全防护要求》5.1.3.3-c，邮件系统中各个功能模块的数据库及中间件软件的审计范围应覆盖到每个数据库及中间件软件用户
<p>测试步骤：</p> <ol style="list-style-type: none"> 1) 应访谈相关技术人员，检查业务设计/验收文档、业务安全策略、业务管理和配置文档、审计记录/报告； 2) 检查邮件系统中各个功能模块的数据库及中间件软件的审计记录，检查审计范围是否覆盖到每个数据库及中间件软件用户
<p>预期结果：</p> <ol style="list-style-type: none"> 1) 邮件系统中各个功能模块的数据库及中间件软件均保存审计记录； 2) 审计范围覆盖到每个数据库及中间件软件用户
<p>判定原则：</p> <p>达到以上预期结果，则通过，否则不通过</p>

5.2 第2级要求

除按照第1级的要求进行检测之外，还应按照本节内容进行检测。

5.2.1 业务及应用安全

5.2.1.1 身份鉴别

测试编号：邮件系统-第2级-业务及应用安全-身份鉴别-01
测试项目：《邮件系统安全防护要求》5.2.1.1-a，应提供并启用业务使用用户身份标识唯一性检查的功能，保证系统中不存在重复用户身份标识，身份鉴别信息不易被冒用
测试步骤： <ol style="list-style-type: none"> 1) 检查设计/验收文档，确定系统是否能保证用户身份标识唯一性，身份鉴别信息是否不易被冒用； 2) 检查邮件系统是否提供并启用用户身份标识唯一检查功能，保证系统中不存在重复用户身份标识； 3) 检查邮件系统用户身份鉴别信息是否不易被冒用
预期结果： <ol style="list-style-type: none"> 1) 设计/验收文档中，系统提供了保证用户身份标识唯一性以及身份鉴别信息是否不易被冒用的措施； 2) 邮件系统提供并启用用户身份标识唯一检查功能，保证系统中不存在重复用户身份标识； 3) 邮件系统能对用户身份鉴别信息被冒用进行检验
判定原则： 达到以上预期结果，则通过，否则不通过

5.2.1.2 访问控制

测试编号：邮件系统-第2级-业务及应用安全-访问控制-01
测试项目：《邮件系统安全防护要求》5.2.1.2-a，应提供访问控制功能，依据安全策略控制业务使用用户、后台管理用户对系统文件、数据库表等客体的访问，控制粒度为单个用户
测试步骤： <ol style="list-style-type: none"> 1) 应访谈相关技术人员，检查业务设计/验收文档、业务安全策略、业务管理和配置文档，检查文档中访问控制策略要求是否控制业务使用用户、后台管理用户对系统文件、数据库表等客体的访问，控制粒度为单个用户； 2) 模拟单个用户访问系统文件、数据库表等客体等
预期结果： <ol style="list-style-type: none"> 1) 设计/验收文档中对访问控制策略有明确描述，控制业务使用用户、后台管理用户对系统文件、数据库表等客体的访问，控制粒度为单个用户； 2) 邮件系统提供访问控制功能，能够依据安全策略控制业务用户、管理用户对系统文件、数据库表等客体的访问，控制粒度为单个用户
判定原则： 达到以上预期结果，则通过，否则不通过

测试编号：邮件系统-第2级-业务及应用安全-访问控制-02
测试项目：《邮件系统安全防护要求》5.2.1.2-b，应提供并启用业务使用用户登录认证策略，如防范暴力破解、防范暴力获取用户名、限定失败登录次数、锁定时间等
<p>测试步骤：</p> <ol style="list-style-type: none"> 1) 应访谈相关技术人员，检查业务设计/验收文档、业务安全策略、业务管理和配置文档，检查文档中是否有用户登录认证策略的要求如防范暴力破解、防范暴力获取用户名、限定失败登录次数、锁定时间； 2) 模拟用户登录失败，检查邮件系统是否限定失败登录次数、锁定时间等； 3) 模拟暴力破解、暴力获取用户名攻击
<p>预期结果：</p> <ol style="list-style-type: none"> 1) 设计/验收文档中有用户登录认证策略的要求如防范暴力破解、防范暴力获取用户名、限定失败登录次数、锁定时间； 2) 邮件系统提供并启用业务用户登录认证策略，能够防范暴力破解、限定失败登录次数、锁定时间等
<p>判定原则：</p> <p>达到以上预期结果，则通过，否则不通过</p>

测试编号：邮件系统-第2级-业务及应用安全-访问控制-03
测试项目：《邮件系统安全防护要求》5.2.1.2-c，应在屏蔽带病毒网页后，为用户发送消息提示
<p>测试步骤：</p> <ol style="list-style-type: none"> 1) 应访谈相关技术人员，检查业务设计/验收文档、业务安全策略、业务管理和配置文档，检查文档中是否为用户发送消息提示的要求； 2) 测试发送带病毒网页，检查邮件系统是否能屏蔽带病毒网页，并为用户发送消息提示
<p>预期结果：</p> <ol style="list-style-type: none"> 1) 设计/验收文档中有为用户发送提示的相关要求； 2) 邮件系统在屏蔽带病毒网页后能够为用户发送消息提示
<p>判定原则：</p> <p>达到以上预期结果，则通过，否则不通过</p>

5.2.1.3 安全审计

测试编号：邮件系统-第2级-业务及应用安全-安全审计-01
测试项目：《邮件系统安全防护要求》5.2.1.3-a，应提供覆盖到系统每一个业务使用用户、后台管理用户的安全审计功能，至少应能对用户关键操作、重要行为、系统重要安全事件等进行审计
测试步骤： <ol style="list-style-type: none"> 1) 应访谈相关技术人员，检查业务设计/验收文档是否要求业务审计能对用户关键操作、重要行为、系统重要安全事件等进行记录； 2) 检查业务审计记录是否覆盖到系统每一个业务使用用户、后台管理用户； 3) 检查业务审计记录是否能对用户关键操作、重要行为、系统重要安全事件等进行审计
预期结果： <ol style="list-style-type: none"> 1) 设计/验收文档明确要求对用户关键操作、重要行为、系统重要安全事件等进行审计； 2) 业务审计功能能够覆盖到系统每一个业务使用用户、后台管理用户； 3) 业务审计功能能对用户关键操作、重要行为、系统重要安全事件等进行审计
判定原则： 达到以上预期结果，则通过，否则不通过

测试编号：邮件系统-第2级-业务及应用安全-安全审计-02
测试项目：《邮件系统安全防护要求》5.2.1.3-b，应保证无法删除、修改或覆盖审计记录
测试步骤： <ol style="list-style-type: none"> 1) 访谈邮件系统运维人员，询问是否有针对审计记录的保护措施； 2) 模拟删除、修改或覆盖审计记录
预期结果： <ol style="list-style-type: none"> 1) 邮件系统对审计记录采取了保护措施； 2) 邮件系统审计记录能够保证无法删除、修改或覆盖
判定原则： 达到以上预期结果，则通过，否则不通过

测试编号：邮件系统-第2级-业务及应用安全-安全审计-03
测试项目：《邮件系统安全防护要求》5.2.1.3-c，审计记录的内容至少应包括事件日期、时间、发起者信息、类型、描述和结果等
测试步骤： 1) 访谈邮件系统运维人员，询问审计记录内容是否包括事件日期、时间、发起者信息、类型、描述和结果等； 2) 检查审计记录内容是否包括事件日期、时间、发起者信息、类型、描述和结果等
预期结果： 审计记录内容包括事件日期、时间、发起者信息、类型、描述和结果等
判定原则： 达到以上预期结果，则通过，否则不通过

5.2.1.4 数据安全性

测试编号：邮件系统-第2级-业务及应用安全-数据安全性-01
测试项目：《邮件系统安全防护要求》5.2.1.4-a，应提供用户登录认证过程的数据加密传输功能
测试步骤： 1) 应访谈相关技术人员，检查业务设计/验收文档是否有对用户登录认证过程的数据加密传输的要求； 2) 使用协议分析仪对用户的登录过程进行抓包，分析报文的保密性
预期结果： 1) 设计/验收文档有对用户登录认证过程的数据加密传输的要求； 2) 邮件系统对用户登录认证过程的数据进行加密传输
判定原则： 达到以上预期结果，则通过，否则不通过

测试编号：邮件系统-第2级-业务及应用安全-数据安全性-02
测试项目：《邮件系统安全防护要求》5.2.1.4-b，应对邮件内容进行数据保护，采取非明文存储方式
测试步骤： 1) 应访谈相关技术人员，检查业务设计/验收文档是否有对邮件内容进行数据保护的要求； 2) 检查邮件系统存储的邮件内容格式是否为加密格式
预期结果： 1) 业务设计/验收文档有对邮件内容进行数据保护的要求； 2) 邮件系统对邮件内容进行数据保护，采取非明文存储方式
判定原则： 达到以上预期结果，则通过，否则不通过

测试编号：邮件系统-第2级-业务及应用安全-数据安全性-03
测试项目：《邮件系统安全防护要求》5.2.1.4-c，应防范和过滤垃圾邮件，保证用户邮件的正常使用
测试步骤： 1) 应访谈相关技术人员，检查业务设计/验收文档是否有防范和过滤垃圾邮件的要求； 2) 模拟发送垃圾邮件，检查邮件系统是否能够防范和过滤垃圾邮件
预期结果： 1) 业务设计/验收文档有防范和过滤垃圾邮件的要求； 2) 邮件系统能够防范和过滤垃圾邮件，保证用户邮件的正常使用
判定原则： 达到以上预期结果，则通过，否则不通过

测试编号：邮件系统-第2级-业务及应用安全-数据安全性-04
测试项目：《邮件系统安全防护要求》5.2.1.4-d，应对进入邮件服务器的邮件（如发送地址、接收地址、标题等）是否包含恶意链接及恶意代码进行必要的检测，并对邮件收发地址有效性进行验证
测试步骤： 1) 应访谈相关技术人员，检查业务设计/验收文档是否要求对进入邮件服务器的邮件进行恶意链接及恶意代码检测； 2) 测试邮件服务器是否对包含恶意链接及恶意代码进行必要的检测； 3) 测试邮件服务器是否对邮件收发地址有效性进行验证
预期结果： 1) 邮件服务器对包含恶意链接及恶意代码进行必要的检测； 2) 邮件服务器对邮件收发地址有效性进行验证
判定原则： 达到以上预期结果，则通过，否则不通过

5.2.1.5 资源控制

测试编号：邮件系统-第2级-业务及应用安全-资源控制-01
测试项目：《邮件系统安全防护要求》5.2.1.5-a，登录用户在超过限定时间内未作任何操作，系统应该自动登出
测试步骤： 1) 应访谈相关技术人员，检查业务设计/验收文档是否规定了限定登录时间； 2) 检查邮件系统，当登录用户在超过限定时间内未作任何操作，系统是否自动登出
预期结果： 1) 业务设计/验收文档规定了限定登录时间； 2) 登录用户在超过限定时间内未作任何操作，系统自动登出
判定原则： 达到以上预期结果，则通过，否则不通过

测试编号：邮件系统-第2级-业务及应用安全-资源控制-02
测试项目：《邮件系统安全防护要求》5.2.1.5-b，应能够对同类型登录设备中单个用户的多重并发会话进行限制
测试步骤： 1) 应访谈相关技术人员，检查业务设计/验收文档是否规定了单个用户的并发会话数； 2) 模拟同类型登录设备中单个用户并发多个会话
预期结果： 1) 业务设计/验收文档规定了单个用户的并发会话数； 2) 邮件系统能对同类型登录设备中单个用户的多重并发会话进行限制
判定原则： 达到以上预期结果，则通过，否则不通过

5.2.1.6 信息保护

测试编号：邮件系统-第2级-业务及应用安全-信息保护-01
测试项目：《邮件系统安全防护要求》5.2.1.6-a，在获取业务使用用户信息时，应采取传输加密等措施保障相应数据的传输安全
测试步骤： 1) 应访谈相关技术人员，检查业务设计/验收文档是否要求对用户信息进行传输加密保护； 2) 检查邮件系统在获取业务使用用户信息时，使用协议分析仪对用户的登录过程进行抓包，分析报文的保密性
预期结果： 1) 业务设计/验收文档要求对用户信息进行传输加密保护； 2) 邮件系统在获取业务使用用户信息时，采取了传输加密等措施保障相应数据的传输安全
判定原则： 达到以上预期结果，则通过，否则不通过

测试编号：邮件系统-第2级-业务及应用安全-信息保护-02
测试项目：《邮件系统安全防护要求》5.2.1.6-b，应采取充分的安全保障措施保障用户数据信息的存储安全，并保障存储设备的安全
测试步骤： 1) 应访谈相关技术人员，检查业务设计/验收文档是否要求对用户信息进行存储安全保护； 2) 检查邮件系统是否采取充分的安全保障措施保障用户数据信息的存储安全，并保障存储设备的安全
预期结果： 1) 业务设计/验收文档要求对用户信息进行存储安全保护； 2) 邮件系统采取了充分的安全保障措施保障用户数据信息的存储安全，并保障存储设备的安全
判定原则： 达到以上预期结果，则通过，否则不通过

测试编号：邮件系统-第2级-业务及应用安全-信息保护-03
测试项目：《邮件系统安全防护要求》5.2.1.6-c，应妥善保存用户信息数据的纸质资料、电子介质等
测试步骤： 1) 应访谈相关技术人员，检查业务设计/验收文档是否要求妥善保存用户信息数据的纸质资料、电子介质等； 2) 检查邮件系统是否妥善保存用户信息数据的纸质资料、电子介质等
预期结果： 1) 业务设计/验收文档要求妥善保存用户信息数据的纸质资料、电子介质等； 2) 邮件系统能够妥善保存用户信息数据的纸质资料、电子介质等
判定原则： 达到以上预期结果，则通过，否则不通过

测试编号：邮件系统-第2级-业务及应用安全-信息保护-04
测试项目：《邮件系统安全防护要求》5.2.1.6-d，在用户申请、审核及投诉处理过程中使用用户数据信息外，不得将用户数据信息用于任何其他用途
测试步骤： 1) 访谈相关技术人员，询问邮件系统在用户申请、审核及投诉处理过程中使用用户数据信息外，是否还用于其他用途； 2) 检查邮件系统对用户数据信息的使用情况，是否在用户申请、审核及投诉处理过程中使用用户数据信息外，还用于其他用途
预期结果： 邮件系统在用户申请、审核及投诉处理过程中使用用户数据信息外，不再用于其他用途
判定原则： 达到以上预期结果，则通过，否则不通过

测试编号：邮件系统-第2级-业务及应用安全-信息保护-05
测试项目：《邮件系统安全防护要求》5.2.1.6-e，应采取措施加强对接触到用户数据信息人员的管理，严格控制接触用户信息的人员范围，合理设定用户信息操作权限，防止出现人为信息泄漏事件
测试步骤： 1) 访谈相关技术人员，检查业务安全策略相关文档，是否对接触到用户数据信息人员进行安全管理； 2) 检查实际接触用户信息的人员范围，测试人员对用户信息的操作权限，是否能够未授权访问用户信息
预期结果： 1) 业务安全策略相关文档对接触到用户数据信息人员规定了安全管理要求； 2) 未授权的人员无法接触用户信息，授权用户只能获取权限规定范围内的用户信息
判定原则： 达到以上预期结果，则通过，否则不通过

测试编号：邮件系统-第2级-业务及应用安全-信息保护-06
测试项目：《邮件系统安全防护要求》5.2.1.6-f，应当明确告知用户收集和处理用户个人信息的方式、内容和用途以及信息泄漏风险，并向用户说明本系统要采取的信息保护措施，不得将用户提交的资料和信息泄露给他人，利用该信息牟利。在与用户签署的相关合同中，应明确规定运营企业对用户信息安全承担保护责任，写明采取的具体信息保护措施
测试步骤： <ol style="list-style-type: none"> 1) 访谈相关技术人员，检查业务安全策略、业务管理文档是否规定了收集和处理用户个人信息的方式、内容和用途以及信息泄漏风险； 2) 检查邮件系统在使用过程中是否明确告知用户收集和处理用户个人信息的方式、内容和用途以及信息泄漏风险，并向用户说明本系统要采取的信息保护措施，不得将用户提交的资料和信息泄露给他人，利用该信息牟利； 3) 检查邮件系统是否与用户签署相关合同协议，明确规定运营企业对用户信息安全承担保护责任，写明采取的具体信息保护措施
预期结果： <ol style="list-style-type: none"> 1) 业务安全策略、业务管理文档规定了收集和处理用户个人信息的方式、内容和用途以及信息泄漏风险； 2) 邮件系统明确告知用户收集和处理用户个人信息的方式、内容和用途以及信息泄漏风险，并向用户说明本系统要采取的信息保护措施，不得将用户提交的资料和信息泄露给他人，利用该信息牟利； 3) 邮件系统与用户签署相关合同协议明确规定运营企业对用户信息安全承担保护责任，写明采取的具体信息保护措施
判定原则： 达到以上预期结果，则通过，否则不通过

测试编号：邮件系统-第2级-业务及应用安全-信息保护-07
测试项目：《邮件系统安全防护要求》5.2.1.6-g，应对用户信息安全防护工作进行定期检查或抽查，发现有违规行为时，可以依据相关协议等追究其责任
测试步骤： <ol style="list-style-type: none"> 1) 访谈相关运维人员，是否对用户信息安全防护工作进行定期检查或抽查，是否对违规行为依据相关协议等追究其责任； 2) 检查是否有用户信息安全防护工作定期检查或抽查记录，检查违规行为及其责任追究记录
预期结果： <ol style="list-style-type: none"> 1) 对用户信息安全防护工作进行定期检查或抽查，并对违规行为依据相关协议等追究其责任； 2) 保存用户信息安全防护工作定期检查或抽查记录，包括违规行为及其责任追究记录
判定原则： 达到以上预期结果，则通过，否则不通过

5.2.1.7 Web 安全

测试编号：邮件系统-第 2 级-业务及应用安全-Web 安全-01
测试项目：《邮件系统安全防护要求》5.2.1.7-a，应对所有来源输入进行验证并尽量使用白名单验证方法
测试步骤： 1) 访谈相关技术人员，检查业务设计/验收文档是否对所有来源输入进行验证，是否使用白名单验证方法； 2) 采用不同格式的数据测试邮件系统输入，检查邮件系统是否对输入进行验证，是否使用白名单验证方法
预期结果： 1) 业务设计/验收文档规定对所有来源输入进行验证，且使用白名单验证方法； 2) 邮件系统对白名单之外的数据输入验证不通过
判定原则： 达到以上预期结果，则通过，否则不通过

测试编号：邮件系统-第 2 级-业务及应用安全-Web 安全-02
测试项目：《邮件系统安全防护要求》5.2.1.7-b，应设计一套统一的验证接口，向整个应用系统提供一致的验证方法
测试步骤： 1) 应访谈相关技术人员，检查业务设计/验收文档是否设计一套统一的验证接口，向整个应用系统提供一致的验证方法； 2) 检查邮件系统的验证接口和验证方法
预期结果： 1) 业务设计/验收文档设计了一套统一的验证接口，向整个应用系统提供一致的验证方法； 2) 邮件系统具有一套统一的验证接口，向整个应用系统提供一致的验证方法
判定原则： 达到以上预期结果，则通过，否则不通过

测试编号：邮件系统-第 2 级-业务及应用安全-Web 安全-03
测试项目：《邮件系统安全防护要求》5.2.1.7-c，应在服务器端进行输入验证，避免客户端输入验证被绕过
测试步骤： 1) 检查邮件系统是否在服务器端进行输入验证； 2) 使用不同输入用例测试客户端输入验证是否能被绕过
预期结果： 1) 邮件系统在服务器端进行输入验证； 2) 客户端输入验证无法被绕过
判定原则： 达到以上预期结果，则通过，否则不通过

测试编号：邮件系统-第2级-业务及应用安全-Web 安全-04
测试项目：《邮件系统安全防护要求》5.2.1.7-d，应对输入内容进行规范化处理后再进行验证，如文件路径、URL 地址等
测试步骤： 1) 检查邮件系统是否对输入内容进行规范化处理后再进行验证，如文件路径、URL 地址等； 2) 测试输入不同格式的文件路径、URL 地址等，验证邮件系统是否对输入内容进行规范化处理
预期结果： 1) 邮件系统对输入内容进行规范化处理后再进行验证，如文件路径、URL 地址等； 2) 邮件系统对不同格式的数据输入均进行规范化处理
判定原则： 达到以上预期结果，则通过，否则不通过

测试编号：邮件系统-第2级-业务及应用安全-Web 安全-05
测试项目：《邮件系统安全防护要求》5.2.1.7-e，应确保用户不能访问到未授权的功能和数据，未经授权的用户试图访问受限资源时，系统应予以拒绝或提示用户进行身份鉴权
测试步骤： 1) 检查邮件系统是否对用户访问权限进行限制； 2) 测试不同用户的访问权限，试图访问未授权的受限资源验证系统是否能予以拒绝或提示用户进行身份鉴权
预期结果： 1) 邮件系统对用户访问权限进行限制； 2) 邮件系统能保证用户不能访问到未授权的功能和数据，未经授权的用户试图访问受限资源时，系统应予以拒绝或提示用户进行身份鉴权
判定原则： 达到以上预期结果，则通过，否则不通过

测试编号：邮件系统-第2级-业务及应用安全-Web 安全-06
测试项目：《邮件系统安全防护要求》5.2.1.7-f，应采用统一的访问控制机制，保证整体访问控制策略的一致性，同时应确保访问控制策略不被非法修改
测试步骤： 1) 检查邮件系统是否采用统一的访问控制机制，保证整体访问控制策略的一致性； 2) 试图修改访问控制策略，验证邮件系统能否保证访问控制策略不被非法修改
预期结果： 1) 邮件系统采用统一的访问控制机制，保证整体访问控制策略的一致性； 2) 邮件系统能确保访问控制策略不被非法修改
判定原则： 达到以上预期结果，则通过，否则不通过

测试编号：邮件系统-第 2 级-业务及应用安全-Web 安全-07
测试项目：《邮件系统安全防护要求》5.2.1.7-g，应确保会话的安全创建，在用户认证成功后，应为用户创建新的会话并释放原有会话，新创建的会话标识应满足随机性和长度要求，避免被攻击者猜测（如采用会话与 IP 地址绑定的方式），降低会话被盗用的风险
测试步骤： <ol style="list-style-type: none"> 1) 创建测试账号，验证测试账号认证成功后，系统是否为用户创建新的会话并释放原有会话； 2) 获取会话标识，验证是否满足随机性和长度要求
预期结果： <ol style="list-style-type: none"> 1) 在认证成功后，系统为用户创建新的会话并释放原有会话； 2) 创建的会话标识满足随机性和长度要求，避免被攻击者猜测（会话与 IP 地址可绑定，降低会话被盗用的风险）
判定原则： <p>达到以上预期结果，则通过，否则不通过</p>

测试编号：邮件系统-第 2 级-业务及应用安全-Web 安全-08
测试项目：《邮件系统安全防护要求》5.2.1.7-h，应确保会话数据的存储和传输安全，用户登录成功后所生成的会话数据应存储在服务器端，并确保会话数据不能被非法访问，当更新会话数据时，要对数据进行严格的输入验证，以免会话数据的非法篡改
测试步骤： <ol style="list-style-type: none"> 1) 验证用户登录成功后所生成的会话数据是否存储在服务器端； 2) 访问会话数据，验证数据是否会被非法访问； 3) 当更新会话数据时，验证系统是否对数据进行严格的输入验证
预期结果： <ol style="list-style-type: none"> 1) 用户登录成功后所生成的会话数据存储在服务器端； 2) 系统确保会话数据不能被非法访问； 3) 当更新会话数据时，系统对数据进行了严格的输入验证，避免会话数据被非法篡改
判定原则： <p>达到以上预期结果，则通过，否则不通过</p>

测试编号：邮件系统-第2级-业务及应用安全-Web 安全-09
测试项目：《邮件系统安全防护要求》5.2.1.7-i，应确保会话的安全终止，当用户登录成功并成功创建会话后，应在 web 应用系统的各个页面提供用户登出功能，登出时应及时删除服务器端的会话数据；当处于登录状态的用户直接关闭浏览器时，需要提示用户执行安全登出或者自动为用户完成登出过程，从而安全的终止本次会话
测试步骤： <ol style="list-style-type: none"> 1) 观察 WEB 应用系统的各个页面是否提供用户登出功能； 2) 使用测试账号登出时，验证系统是否及时删除服务器端的会话数据； 3) 使用测试账号重新登录后，直接关闭浏览器； 4) 验证系统是否提示用户执行安全登出或者自动为用户完成登出过程
预期结果： <ol style="list-style-type: none"> 1) 当用户登录成功并成功创建会话后，在 WEB 应用系统的各个页面提供用户登出功能； 2) 登出时会及时删除服务器端的会话数据； 3) 当处于登录状态的用户直接关闭浏览器时，提示用户执行安全登出或者自动为用户完成登出过程，从而安全的终止了本次会话
判定原则： 达到以上预期结果，则通过，否则不通过

测试编号：邮件系统-第2级-业务及应用安全-Web 安全-10
测试项目：《邮件系统安全防护要求》5.2.1.7-j，应设置合理的会话超时阈值，在合理范围内尽可能减小会话超时阈值，可以降低会话被劫持和重复攻击的风险，超过会话超时阈值后立刻销毁会话，清除会话的信息
测试步骤： <ol style="list-style-type: none"> 1) 询问系统是否设置了合理的会话超时阈值，该阈值应尽可能减小； 2) 创建测试账号，并保证账号功能正常； 3) 使用测试账号创建会话； 4) 等待会话超时后，验证系统是否立刻销毁会话
预期结果： <ol style="list-style-type: none"> 1) 系统设置了合理的会话超时阈值； 2) 系统在合理范围内已经尽可能的减小了会话超时阈值，降低了会话被劫持和重复攻击的风险； 3) 超过会话超时阈值后，系统会立刻销毁会话，清除会话的信息
判定原则： 达到以上预期结果，则通过，否则不通过

测试编号：邮件系统-第2级-业务及应用安全-Web 安全-11
测试项目：《邮件系统安全防护要求》5.2.1.7-k，在涉及到关键业务操作的 web 页面，应提供保障会话安全的补充机制（如以 web 页面一次性随机令牌的方式，作为主会话标识的补充）
测试步骤： <ol style="list-style-type: none"> 1) 使用测试账号访问涉及到关键业务操作的 WEB 页面； 2) 验证系统是否为该类 WEB 页面生成一次性随机令牌，作为主会话标识的补充（在执行关键业务前，应确保用户提交的一次性随机令牌与服务器端保存的一次性随机令牌匹配）
预期结果： <ol style="list-style-type: none"> 1) 系统为涉及到关键业务操作的 WEB 页面生成了一次性随机令牌，作为主会话标识的补充； 2) 在执行关键业务前，确保了用户提交的一次性随机令牌与服务器端保存的一次性随机令牌匹配
判定原则： 达到以上预期结果，则通过，否则不通过

5.2.1.8 客户端安全

测试编号：邮件系统-第2级-业务及应用安全-客户端安全-01
测试项目：《邮件系统安全防护要求》5.2.1.8-a，客户端应对输入数据做严格验证
测试步骤： <ol style="list-style-type: none"> 1) 检查客户端是否对输入数据做严格验证； 2) 输入各种格式数据验证客户端是否对数据做严格验证
预期结果： 客户端对输入数据做严格验证
判定原则： 达到以上预期结果，则通过，否则不通过

测试编号：邮件系统-第2级-业务及应用安全-客户端安全-02
测试项目：《邮件系统安全防护要求》5.2.1.8-b，客户端应确保身份认证模块不能被非法绕过
测试步骤： <ol style="list-style-type: none"> 1) 使用测试账号访问客户端； 2) 验证身份认证模块能否被非法绕过
预期结果： 测试账号需要经过身份认证，无法被绕过
判定原则： 达到以上预期结果，则通过，否则不通过

测试编号：邮件系统-第2级-业务及应用安全-客户端安全-03
测试项目：《邮件系统安全防护要求》5.2.1.8-c，客户端软件运行时应对自身进行完整性校验，及时有效的发现是否被恶意修改
测试步骤： 1) 检查客户端软件运行时是否对自身进行完整性校验； 2) 检查客户端能否及时有效的发现被恶意修改
预期结果： 1) 客户端软件运行时能对自身进行完整性校验； 2) 客户端软件能及时有效发现被恶意修改
判定原则： 达到以上预期结果，则通过，否则不通过

测试编号：邮件系统-第2级-业务及应用安全-客户端安全-04
测试项目：《邮件系统安全防护要求》5.2.1.8-d，客户端应采取会话保护措施防止软件与服务器之间的会话被篡改、伪造、重放等
测试步骤： 1) 使用测试账号登录，并进行测试操作； 2) 验证客户端是否采取会话保护措施防止软件与服务器之间的会话被篡改、伪造、重放等
预期结果： 客户端采取会话保护措施防止软件与服务器之间的会话被篡改、伪造、重放等
判定原则： 达到以上预期结果，则通过，否则不通过

测试编号：邮件系统-第2级-业务及应用安全-客户端安全-05
测试项目：《邮件系统安全防护要求》5.2.1.8-e，客户端应确保软件配置信息、用户认证信息、本地存储的用户邮件信息等敏感数据采用加密方式存储
测试步骤： 1) 检查客户端是否会对软件配置信息、用户认证信息、本地存储的用户邮件信息等敏感数据采用加密方式存储； 2) 访问软件配置信息、用户认证信息、本地存储的用户邮件信息等敏感数据，检查数据格式是否是加密
预期结果： 客户端能够确保软件配置信息、用户认证信息、本地存储的用户邮件信息等敏感数据采用加密方式存储
判定原则： 达到以上预期结果，则通过，否则不通过

测试编号：邮件系统-第2级-业务及应用安全-客户端安全-06
测试项目：《邮件系统安全防护要求》5.2.1.8-f，客户端软件应具有异常处理功能
测试步骤： 1) 检查客户端软件是否具有异常处理功能； 2) 测试验证客户端是否具有异常处理功能
预期结果： 客户端软件具有异常处理功能
判定原则： 达到以上预期结果，则通过，否则不通过

5.2.1.9 对外接口安全

测试编号：邮件系统-第2级-业务及应用安全-对外接口安全-01
测试项目：《邮件系统安全防护要求》5.2.1.9-a，接口均应分别设置专门前置服务器，通过前置服务器的接口应用实现内外系统的交互
测试步骤： 1) 检查邮件系统接口是否设置了专门前置服务器； 2) 访问对外接口，验证是否通过前置服务器的接口应用实现内外交互
预期结果： 邮件系统接口设置专门前置服务器，通过前置服务器的接口应用实现内外系统的交互
判定原则： 达到以上预期结果，则通过，否则不通过

测试编号：邮件系统-第2级-业务及应用安全-对外接口安全-02
测试项目：《邮件系统安全防护要求》5.2.1.9-b，接口数据传输应尽量采用加密方式，原则上要求内外系统交互时，接口报文中的敏感信息应进行加密传输，如接口认证需要的密码等敏感数据
测试步骤： 1) 通过接口访问邮件系统； 2) 通过协议分析仪抓包分析，查看传输数据是否进行加密
预期结果： 接口数据传输采用加密方式，接口报文中的敏感信息均进行加密传输，如接口认证需要的密码等敏感数据
判定原则： 达到以上预期结果，则通过，否则不通过

测试编号：邮件系统-第2级-业务及应用安全-对外接口安全-03
测试项目：《邮件系统安全防护要求》5.2.1.9-c，接口数据传输应进行校验，确保数据在传输过程中的完整性
测试步骤： 1) 通过接口访问邮件系统； 2) 通过技术手段，查看传输数据是否进行完整性校验
预期结果： 接口数据传输进行校验，确保数据在传输过程中的完整性
判定原则： 达到以上预期结果，则通过，否则不通过

测试编号：邮件系统-第2级-业务及应用安全-对外接口安全-04
测试项目：《邮件系统安全防护要求》5.2.1.9-d，接口认证信息必须以密文的形式单独存储在配置文件中
测试步骤： 查看存储的接口认证信息，验证是否进行加密
预期结果： 接口认证信息以密文的形式单独存储在配置文件中
判定原则： 达到以上预期结果，则通过，否则不通过

5.2.2 网络安全

5.2.2.1 网络结构

测试编号：邮件系统-第2级-网络安全-网络结构-01
测试项目：《邮件系统安全防护要求》5.2.2.1-a，应根据自身应用和服务的特点，在满足高峰期流量需求的基础上，合理设计带宽
测试步骤： 1) 访谈网络运维人员，检查系统设计/验收文档、相关服务管理流程、系统安全策略、网络和业务运营商/服务提供商提供的其他文档； 2) 询问高峰期业务流量； 3) 询问当前的出口带宽； 4) 判定系统的带宽是否满足高峰期业务流量的需求； 5) 根据业务的特点，检查出口带宽是否合理
预期结果： 1) 系统的带宽满足高峰期业务流量的需求； 2) 系统出口带宽合理，符合业务的特点
判定原则： 达到以上预期结果，则通过，否则不通过

5.2.2.2 网络监测

测试编号：邮件系统-第2级-网络安全-网络监测-01
测试项目：《邮件系统安全防护要求》5.2.2.2-a，应在系统边界部署访问安全监测设备，并启用有效的安全监测控制策略
测试步骤： 1) 访谈网络运维人员，检查系统设计/验收文档、系统安全策略、系统管理和配置文档，检查验证是否在系统边界部署访问安全监测设备，并启用有效的安全监测控制策略； 2) 通过技术手段测试验证系统边界安全监测设备能否对外部攻击进行有效监控
预期结果： 1) 安全监测已启用有效的安全监测控制策略； 2) 安全监测设备能对外部攻击进行有效监控
判定原则： 达到以上预期结果，则通过，否则不通过

测试编号：邮件系统-第2级-网络安全-网络监测-02
测试项目：《邮件系统安全防护要求》5.2.2.2-b，应具备恶意代码监测功能，对通过该平台对外发布的信息使用自动程序过滤和人工检查结合的方式进行恶意代码监测、检查、屏蔽和删除，防止恶意代码通过业务网络向公众传播
测试步骤： 1) 访谈网络运维人员，检查系统设计/验收文档、系统安全策略、系统管理和配置文档，检查验证是否具备恶意代码监测功能； 2) 检查是否能够对外发布的信息使用自动程序过滤和人工检查结合的方式进行恶意代码监测、检查、屏蔽和删除； 3) 通过模拟响应攻击等技术手段测试验证恶意代码监测能否防止恶意代码通过业务网络向公众传播
预期结果： 1) 具备恶意代码监测功能； 2) 能够防止恶意代码通过业务网络向公众传播
判定原则： 达到以上预期结果，则通过，否则不通过

测试编号：邮件系统-第2级-网络安全-网络监测-03
测试项目：《邮件系统安全防护要求》5.2.2.2-c，各个功能模块的计算机运维终端、服务器等设备应安装病毒、木马等恶意代码的监测和查杀软件，并能对监测日志进行实时备份，以及定期更新防恶意代码软件版本和恶意代码库
测试步骤： 1) 检查各个功能模块的计算机运维终端、服务器等设备是否安装病毒、木马等恶意代码的监测和查杀软件； 2) 检查监测日志是否实时备份； 3) 检查软件是否定期更新防恶意代码软件版本和恶意代码库
预期结果： 1) 各个功能模块的计算机运维终端、服务器等设备均安装病毒、木马等恶意代码的监测和查杀软件； 2) 监测日志实时备份； 3) 软件定期更新防恶意代码软件版本和恶意代码库
判定原则： 达到以上预期结果，则通过，否则不通过

测试编号：邮件系统-第2级-网络安全-网络监测-04
测试项目：《邮件系统安全防护要求》5.2.2.2-d，各个功能模块的计算机运维终端、服务器等设备应支持防恶意代码监测和查杀软件的统一管理
测试步骤： 检查各个功能模块的计算机运维终端、服务器等设备的防恶意代码监测和查杀软件是否实施统一管理
预期结果： 各个功能模块的计算机运维终端、服务器等设备支持防恶意代码监测和查杀软件的统一管理
判定原则： 达到以上预期结果，则通过，否则不通过

5.2.2.3 安全审计

测试编号：邮件系统-第2级-网络安全-安全审计-01
测试项目：《邮件系统安全防护要求》5.2.2.3-a，审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息
测试步骤： 1) 访谈网络运维人员，检查系统设计/验收文档、系统安全策略、系统管理和配置文档、审计记录/报告； 2) 检查或测试验证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
预期结果： 审计记录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
判定原则： 达到以上预期结果，则通过，否则不通过

5.2.3 设备及软件系统安全

5.2.3.1 网络及设备安全

测试编号：邮件系统-第2级-设备及软件系统安全-网络及设备安全-01
测试项目：《邮件系统安全防护要求》5.2.3.1-a，应对登录网络设备（例如路由器、交换机）以及安全设备（例如入侵检测设备、防火墙设备）的用户进行有效的身份标识和鉴别
测试步骤： 1) 访谈网络运维人员，检查系统设计/验收文档、系统安全策略、系统管理和配置文档； 2) 检查网络设备（例如路由器、交换机）以及安全设备（例如入侵检测设备、防火墙设备）用户身份记录，验证是否对用户进行有效的身份标识和鉴别
预期结果： 对登录网络设备（例如路由器、交换机）以及安全设备（例如入侵检测设备、防火墙设备）的用户进行有效的身份标识和鉴别
判定原则： 达到以上预期结果，则通过，否则不通过

测试编号：邮件系统-第2级-设备及软件系统安全-网络及设备安全-02
测试项目：《邮件系统安全防护要求》5.2.3.1-b，网络及安全设备管理用户的标识应唯一
测试步骤： 1) 访谈网络运维人员，检查系统设计/验收文档、系统安全策略、系统管理和配置文档； 2) 查看或测试验证网络及安全设备管理用户数据库的标识是否唯一
预期结果： 网络及安全设备管理用户的标识唯一
判定原则： 达到以上预期结果，则通过，否则不通过

5.2.3.2 通用主机操作系统

5.2.3.2.1 安全检测

测试编号：邮件系统-第2级-通用主机操作系统-安全检测-01
测试项目：《邮件系统安全防护要求》5.2.3.2.1-a，应对邮件系统中各个功能模块的计算机运维终端、服务器等设备的主机操作系统进行必要的安全检测，出具安全测试及验收报告并妥善保存，相关设备的安全应满足相应设备技术规范、设备安全要求等行业标准的相关规定
测试步骤： 1) 检查邮件系统中各个功能模块的计算机运维终端、服务器等设备的主机操作系统安全测试及验收报告； 2) 检查相关设备的安全是否满足相应设备技术规范、设备安全要求等行业标准的相关规定
预期结果： 1) 邮件系统中各个功能模块的计算机运维终端、服务器等设备的主机操作系统均有安全测试及验收报告； 2) 相关设备的安全满足相应设备技术规范、设备安全要求等行业标准的相关规定
判定原则： 达到以上预期结果，则通过，否则不通过

测试编号：邮件系统-第2级-通用主机操作系统-安全检测-02
测试项目：《邮件系统安全防护要求》5.2.3.2.1-b，各个功能模块的计算机运维终端、服务器等设备的主机操作系统应定期进行安全检测，发现并加固操作系统相关漏洞，避免已发现的漏洞造成安全事件
<p>测试步骤：</p> <p>1) 访谈网络运维人员，询问是否对各个功能模块的计算机运维终端、服务器等设备的主机操作系统定期进行安全检测，发现并加固操作系统相关漏洞；</p> <p>2) 检查安全检测和漏洞加固记录</p>
<p>预期结果：</p> <p>1) 定期对各个功能模块的计算机运维终端、服务器等设备的主机操作系统进行安全检测；</p> <p>2) 定期安全检测能够发现并加固操作系统相关漏洞；</p> <p>3) 具备相关的记录</p>
<p>判定原则：</p> <p>达到以上预期结果，则通过，否则不通过</p>

5.2.3.2.2 身份鉴别

测试编号：邮件系统-第2级-通用主机操作系统-身份鉴别-01
测试项目：《邮件系统安全防护要求》5.2.3.2.2-a，当对各类主机进行远程管理时，应采取必要措施，防止鉴别信息在传输过程中被窃听
<p>测试步骤：</p> <p>1) 检查设计/验收文档，确定对各类主机进行远程管理时，是否采取必要措施，防止鉴别信息在传输过程中被窃听；</p> <p>2) 使用测试账号对各类主机进行远程管理，检查是否采取必要措施，防止鉴别信息在传输过程中被窃听</p>
<p>预期结果：</p> <p>对各类主机进行远程管理时，采取必要措施防止鉴别信息在传输过程中被窃听</p>
<p>判定原则：</p> <p>达到以上预期结果，则通过，否则不通过</p>

5.2.3.2.3 访问控制

测试编号：邮件系统-第2级-通用主机操作系统-访问控制-01
测试项目：《邮件系统安全防护要求》5.2.3.2.3-a，各个功能模块的计算机运维终端、服务器等设备应启用访问控制功能，依据安全策略控制用户对资源的访问
测试步骤： 1) 检查设计/验收文档，各个功能模块的计算机运维终端、服务器等设备是否具有访问控制功能； 2) 使用测试账号访问各个功能模块的计算机运维终端、服务器等设备，验证是否启用访问控制功能，能否依据安全策略控制用户对资源的访问
预期结果： 1) 各个功能模块的计算机运维终端、服务器等设备已启用访问控制功能； 2) 能够依据安全策略控制用户对资源的访问
判定原则： 达到以上预期结果，则通过，否则不通过

测试编号：邮件系统-第2级-通用主机操作系统-访问控制-02
测试项目：《邮件系统安全防护要求》5.2.3.2.3-b，各个功能模块的计算机运维终端、服务器等设备应及时删除多余的、过期的账户，避免共享账户的存在
测试步骤： 1) 检查设计/验收文档，各个功能模块的计算机运维终端、服务器等设备是否具有及时删除多余的、过期的账户的功能； 2) 检查各个功能模块的计算机运维终端、服务器等设备是否具有多余的、过期的账户
预期结果： 各个功能模块的计算机运维终端、服务器等设备能够及时删除多余的、过期的账户，能够避免共享账户的存在
判定原则： 达到以上预期结果，则通过，否则不通过

测试编号：邮件系统-第2级-通用主机操作系统-访问控制-03
测试项目：《邮件系统安全防护要求》5.2.3.2.3-c，各个功能模块的计算机运维终端、服务器等设备应实现操作系统和数据库系统特权用户的权限分离
测试步骤： 1) 检查设计/验收文档，各个功能模块的计算机运维终端、服务器等设备是否具有操作系统和数据库系统特权用户权限分离的功能； 2) 检查各个功能模块的计算机运维终端、服务器等设备的操作系统和数据库系统的特权用户及其权限
预期结果： 各个功能模块的计算机运维终端、服务器等设备均实现操作系统和数据库系统特权用户的权限分离
判定原则： 达到以上预期结果，则通过，否则不通过

测试编号：邮件系统-第2级-通用主机操作系统-访问控制-04
测试项目：《邮件系统安全防护要求》5.2.3.2.3-d，各个功能模块的计算机运维终端、服务器等设备应限制默认账户的访问权限，修改这些账户的默认口令，条件允许下，应重命名默认账户
测试步骤： 1) 检查各个功能模块的计算机运维终端、服务器等设备是否限制默认账户的访问权限； 2) 查看配置文件检查是否已修改这些账户的默认口令或重命名默认账户
预期结果： 各个功能模块的计算机运维终端、服务器等设备已限制默认账户的访问权限，修改这些账户的默认口令或重命名默认账户
判定原则： 达到以上预期结果，则通过，否则不通过

5.2.3.2.4 安全审计

测试编号：邮件系统-第2级-通用主机操作系统-安全审计-01
测试项目：《邮件系统安全防护要求》5.2.3.2.4-a，各个功能模块的计算机运维终端、服务器等设备的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
测试步骤： 1) 访谈网络运维人员，检查系统设计/验收文档、系统安全策略、系统管理和配置文档、审计记录/报告； 2) 检查或测试验证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
预期结果： 审计记录包括重要用户行为、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
判定原则： 达到以上预期结果，则通过，否则不通过

测试编号：邮件系统-第2级-通用主机操作系统-安全审计-02
测试项目：《邮件系统安全防护要求》5.2.3.2.4-b，各个功能模块的计算机运维终端、服务器等设备的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
测试步骤： 1) 访谈网络运维人员，检查系统设计/验收文档、系统安全策略、系统管理和配置文档、审计记录/报告； 2) 检查或测试验证审计记录是否包括事件的日期、时间、类型、主体标识、客体标识和结果等
预期结果： 审计记录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
判定原则： 达到以上预期结果，则通过，否则不通过

5.2.3.2.5 资源控制

测试编号：邮件系统-第2级-通用主机操作系统-资源控制-01
测试项目：《邮件系统安全防护要求》5.2.3.2.5-a，各个功能模块的服务器应通过设定计算机运维终端接入方式、网络地址范围等条件限制管理终端登录
测试步骤： 1) 测试不同的计算机运维终端接入方式，验证各个功能模块的服务器是否能够限制管理终端登录； 2) 测试不同网络地址的计算机运维终端接入，验证各个功能模块的服务器是否能够限制管理终端登录
预期结果： 各个功能模块的服务器通过设定计算机运维终端接入方式、网络地址范围等条件限制管理终端登录
判定原则： 达到以上预期结果，则通过，否则不通过

测试编号：邮件系统-第2级-通用主机操作系统-资源控制-02
测试项目：《邮件系统安全防护要求》5.2.3.2.5-b，各个功能模块的服务器应根据安全策略设置计算机运维终端的操作超时断开链接
测试步骤： 1) 检查各个功能模块的服务器是否有超时断开链接的安全策略； 2) 测试各个功能模块的服务器是否支持超时断开链接
预期结果： 各个功能模块的服务器根据安全策略设置计算机运维终端的操作超时断开链接
判定原则： 达到以上预期结果，则通过，否则不通过

5.2.3.2.6 冗余备份

测试编号：邮件系统-第2级-通用主机操作系统-冗余备份-01
测试项目：《邮件系统安全防护要求》5.2.3.2.6-a，邮件系统中各个功能模块的服务器应具备一定的冗余备份，关键设备、重要部件应采用冗余的方式提供保护
测试步骤： 1) 查看系统冗余备份制度，关键设备配置及运行状态、关键设备冗余数量； 2) 检查重要部件是否采用冗余的方式提供保护
预期结果： 1) 关键设备具备一定的灾难备份和恢复能力； 2) 重要部件采用了冗余的方式提供保护
判定原则： 达到以上预期结果，则通过，否则不通过

5.2.3.3 数据库及中间件软件

5.2.3.3.1 安全检测

测试编号：邮件系统-第 2 级-数据库及中间件软件-安全检测-01
测试项目：《邮件系统安全防护要求》5.2.3.3.1-a，应对邮件系统中各个功能模块的数据库及中间件软件进行必要的安全检测，出具安全测试及验收报告并妥善保存，相关设备的安全应满足相应设备技术规范、设备安全要求等行业标准的相关规定
测试步骤： <ol style="list-style-type: none"> 1) 检查邮件系统中各个功能模块的数据库及中间件软件安全测试及验收报告； 2) 检查相关数据库及中间件软件的安全是否满足相应设备技术规范、设备安全要求等行业标准的相关规定
预期结果： <ol style="list-style-type: none"> 1) 邮件系统中各个功能模块的数据库及中间件软件均有安全测试及验收报告； 2) 相关数据库及中间件软件的安全满足相应设备技术规范、设备安全要求等行业标准的相关规定
判定原则： <p>达到以上预期结果，则通过，否则不通过</p>

测试编号：邮件系统-第 2 级-数据库及中间件软件-安全检测-02
测试项目：《邮件系统安全防护要求》5.2.3.3.1-b，应对邮件系统中各个功能模块的数据库及中间件软件应定期进行安全检测，发现并加固数据库及中间件软件的相关漏洞，避免已发现的漏洞造成安全事件
测试步骤： <ol style="list-style-type: none"> 1) 访谈网络运维人员，询问是否对各个功能模块的数据库及中间件软件定期进行安全检测； 2) 检查安全检测和漏洞加固记录
预期结果： <ol style="list-style-type: none"> 1) 定期对各个功能模块的数据库及中间件软件进行安全检测； 2) 定期安全检测能够发现并加固数据库及中间件软件相关漏洞； 3) 具备相关记录
判定原则： <p>达到以上预期结果，则通过，否则不通过</p>

5.2.3.3.2 身份鉴别

测试编号：邮件系统-第 2 级-数据库及中间件软件-身份鉴别-01
测试项目：《邮件系统安全防护要求》5.2.3.3.2-a，在数据库权限配置能力内，根据用户的业务需要，配置其所需的最小权限
测试步骤： 1) 检查设计/验收文档，数据库权限配置文档是否根据用户的业务需要，配置其所需的最小权限； 2) 使用测试账号登录，验证数据库能否为用户分配最小权限
预期结果： 在数据库权限配置能力内，根据用户的业务需要，配置其所需的最小权限
判定原则： 达到以上预期结果，则通过，否则不通过

测试编号：邮件系统-第 2 级-数据库及中间件软件-身份鉴别-02
测试项目：《邮件系统安全防护要求》5.2.3.3.2-b，使用数据库角色来管理对象的权限
测试步骤： 1) 检查设计/验收文档，数据库是否使用角色来管理对象权限； 2) 使用测试账号登录，验证数据库角色和权限关系
预期结果： 使用数据库角色来管理对象的权限
判定原则： 达到以上预期结果，则通过，否则不通过

5.2.3.3.3 访问控制

测试编号：邮件系统-第 2 级-数据库及中间件软件-访问控制-01
测试项目：《邮件系统安全防护要求》5.2.3.3.3-a，邮件各个功能模块的数据库及中间件软件应启用访问控制功能，依据安全策略控制用户对资源的访问
测试步骤： 1) 检查设计/验收文档，各个功能模块的数据库及中间件软件是否具有访问控制功能； 2) 使用测试账号访问各个功能模块的数据库及中间件软件，验证是否启用访问控制功能，能否依据安全策略控制用户对资源的访问
预期结果： 1) 各个功能模块的数据库及中间件软件已启用访问控制功能； 2) 能够依据安全策略控制用户对资源的访问
判定原则： 达到以上预期结果，则通过，否则不通过

测试编号：邮件系统-第 2 级-数据库及中间件软件-访问控制-02
测试项目：《邮件系统安全防护要求》5.2.3.3.3-b，各个功能模块的数据库及中间件软件应实现数据库、中间件特权用户与操作系统的权限分离
测试步骤： 1) 检查设计/验收文档，各个功能模块的数据库及中间件软件是否具有特权用户权限分离的功能； 2) 检查测试各个功能模块的数据库及中间件软件的特权用户及其权限
预期结果： 各个功能模块的数据库及中间件软件均实现系统特权用户的权限分离
判定原则： 达到以上预期结果，则通过，否则不通过

5.2.3.3.4 安全审计

测试编号：邮件系统-第 2 级-数据库及中间件软件-安全审计-01
测试项目：《邮件系统安全防护要求》5.2.3.3.4-a，各个功能模块的数据库及中间件软件的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
测试步骤： 1) 访谈网络运维人员，检查系统设计/验收文档、系统安全策略、系统管理和配置文档、审计记录/报告； 2) 检查或测试验证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
预期结果： 审计记录包括重要用户行为、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
判定原则： 达到以上预期结果，则通过，否则不通过

测试编号：邮件系统-第 2 级-数据库及中间件软件-安全审计-02
测试项目：《邮件系统安全防护要求》5.2.3.3.4-b，各个功能模块的数据库及中间件软件的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
测试步骤： 1) 访谈网络运维人员，检查系统设计/验收文档、系统安全策略、系统管理和配置文档、审计记录/报告； 2) 检查或测试验证审计记录是否包括事件的日期、时间、类型、主体标识、客体标识和结果等
预期结果： 各个功能模块的数据库及中间件软件的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
判定原则： 达到以上预期结果，则通过，否则不通过

5.2.3.3.5 资源控制

测试编号：邮件系统-第2级-数据库及中间件软件-资源控制-01
测试项目：《邮件系统安全防护要求》5.2.3.3.5-a，各个功能模块的数据库及中间件软件应通过设定计算机运维终端接入方式、网络地址范围等条件限制管理终端登录
测试步骤： 1) 测试不同的计算机运维终端接入方式，验证各个功能模块的数据库及中间件软件是否能够限制管理终端登录； 2) 测试不同网络地址的计算机运维终端接入，验证各个功能模块的数据库及中间件软件是否能够限制管理终端登录
预期结果： 各个功能模块的数据库及中间件软件能通过设定计算机运维终端接入方式、网络地址范围等条件限制管理终端登录
判定原则： 达到以上预期结果，则通过，否则不通过

测试编号：邮件系统-第2级-数据库及中间件软件-资源控制-02
测试项目：《邮件系统安全防护要求》5.2.3.3.5-b，各个功能模块的数据库及中间件软件应根据安全策略设置计算机运维终端的操作超时锁定
测试步骤： 1) 检查各个功能模块的数据库及中间件软件是否有超时锁定的安全策略； 2) 测试各个功能模块的数据库及中间件软件是否支持超时锁定
预期结果： 各个功能模块的数据库及中间件软件能根据安全策略设置计算机运维终端的操作超时锁定
判定原则： 达到以上预期结果，则通过，否则不通过

5.2.3.3.6 冗余备份

测试编号：邮件系统-第 2 级-数据库及中间件软件-冗余备份-01
测试项目：《邮件系统安全防护要求》5.2.3.3.6-a，各个功能模块的数据库及中间件软件应具备一定的冗余备份，关键设备、重要部件应采用冗余的方式提供保护
测试步骤： 1) 查看系统冗余备份制度，关键设备配置及运行状态、关键设备冗余数量； 2) 检查重要部件是否采用冗余的方式提供保护
预期结果： 1) 关键设备具备一定的灾难备份和恢复能力； 2) 重要部件采用了冗余的方式提供保护
判定原则： 达到以上预期结果，则通过，否则不通过

5.2.4 物理环境安全

测试编号：邮件系统-第 2 级-物理环境安全--01
测试项目：《邮件系统安全防护要求》5.2.4-a，应满足 YD/T 1754-2008《电信网和互联网物理环境安全等级保护要求》中的第 2 级要求，在本标准与企业规范标准、企业具体操作维护规范等文档对相同内容有重复要求时，采取从严原则，应符合最严格的安全要求
测试步骤： 1) 访谈邮件系统运维人员，查看邮件系统设计/验收文档等是否符合 YD/T 1754-2008 中的第 2 级要求； 2) 检查邮件系统物理环境设计是否 YD/T 1754-2008 中的第 2 级要求
预期结果： 邮件系统物理环境满足 YD/T 1754-2008 中的第 2 级要求
判定原则： 达到以上预期结果，则通过，否则不通过

5.2.5 管理安全

5.2.5.1 安全管理要求

测试编号：邮件系统-第2级-管理安全-安全管理要求-01
测试项目：《邮件系统安全防护要求》5.2.5.1-a，至少覆盖但不限于安全管理制度、安全管理机构、人员安全管理、安全建设管理、安全运维管理等管理方面
测试步骤： 1) 访谈邮件系统管理人员，询问相关管理制度，至少覆盖但不限于安全管理制度、安全管理机构、人员安全管理、安全建设管理、安全运维管理等管理方面； 2) 查看相关管理制度
预期结果： 管理制度覆盖但不限于安全管理制度、安全管理机构、人员安全管理、安全建设管理、安全运维管理等管理方面
判定原则： 达到以上预期结果，则通过，否则不通过

测试编号：邮件系统-第2级-管理安全-安全管理要求-02
测试项目：《邮件系统安全防护要求》5.2.5.1-b，在本标准与企业规范标准、企业具体操作维护规范等文档对相同内容有重复要求时，采取从严原则，应符合最严格的安全要求
测试步骤： 1) 访谈邮件系统管理人员，询问在本标准与企业规范标准、企业具体操作维护规范等文档对相同内容有重复要求时，是否采取从严原则； 2) 检查管理是否符合最严格的安全要求
预期结果： 在本标准与企业规范标准、企业具体操作维护规范等文档对相同内容有重复要求时，采取从严原则，符合最严格的安全要求
判定原则： 达到以上预期结果，则通过，否则不通过

5.2.5.2 人员和技术支持能力

测试编号：邮件系统-第2级-管理安全-人员和技术支持能力-01
测试项目：《邮件系统安全防护要求》5.2.5.2-a，应有安全管理人员和各类技术人员
测试步骤： 1) 访谈邮件系统管理人员，询问是否有安全管理人员和各类技术人员； 2) 访谈相关安全管理人员和各类技术人员
预期结果： 邮件系统有安全管理人员和各类技术人员
判定原则： 达到以上预期结果，则通过，否则不通过

测试编号：邮件系统-第2级-管理安全-人员和技术支持能力-02
测试项目：《邮件系统安全防护要求》5.2.5.2-b，相关技术人员定期进行灾难备份及恢复方面的技能培训
测试步骤： 1) 访谈邮件系统管理人员，询问是否对技术人员定期进行灾难备份及恢复方面的技能培训； 2) 查看培训记录
预期结果： 相关技术人员定期进行灾难备份及恢复方面的技能培训
判定原则： 达到以上预期结果，则通过，否则不通过

5.2.5.3 运行维护管理能力

测试编号：邮件系统-第2级-管理安全-运行维护管理能力-01
测试项目：《邮件系统安全防护要求》5.2.5.3-a，应有介质存取、验证和转储管理制度，确保备份数据授权访问
测试步骤： 1) 访谈邮件系统运维人员是否有介质存取、验证和转储管理制度； 2) 检查制度能否确保备份数据授权访问
预期结果： 有介质存取、验证和转储管理制度，确保备份数据授权访问
判定原则： 达到以上预期结果，则通过，否则不通过

测试编号：邮件系统-第2级-管理安全-运行维护管理能力-02
测试项目：《邮件系统安全防护要求》5.2.5.3-b，应按介质特性对备份数据进行定期的有效性验证
测试步骤： 1) 访谈邮件系统运维人员，是否按介质特性对备份数据进行定期的有效性验证； 2) 检查定期验证记录
预期结果： 按介质特性对备份数据进行定期的有效性验证
判定原则： 达到以上预期结果，则通过，否则不通过

测试编号：邮件系统-第2级-管理安全-运行维护管理能力-03
测试项目：《邮件系统安全防护要求》5.2.5.3-c，应有相关服务器设备的灾难备份及恢复的管理制度
测试步骤： 1) 访谈邮件系统运维人员，询问是否有相关服务器设备的灾难备份及恢复的管理制度； 2) 查看相关制度
预期结果： 有相关服务器设备的灾难备份及恢复的管理制度
判定原则： 达到以上预期结果，则通过，否则不通过

5.2.5.4 风险评估要求

测试编号：邮件系统-第2级-管理安全-风险评估要求-01
测试项目：《邮件系统安全防护要求》5.2.5.4-a，邮件系统及其所属各类设备、系统应根据安全防护相关规定定期进行安全风险评估（至少每两年一次）
测试步骤： 1) 访谈邮件系统运维人员，询问邮件系统及其所属各类设备、系统应根据安全防护相关规定定期进行安全风险评估（至少每两年一次）； 2) 查看风险评估记录
预期结果： 邮件系统及其所属各类设备、系统应根据安全防护相关规定定期进行安全风险评估（至少每两年一次）
判定原则： 达到以上预期结果，则通过，否则不通过

测试编号：邮件系统-第2级-管理安全-风险评估要求-02
测试项目：《邮件系统安全防护要求》5.2.5.4-b，安全风险评估至少应覆盖业务及应用安全、网络安全、设备及软件系统安全、物理环境安全、管理安全等相关技术风险和人员安全、运维安全等相关管理风险
测试步骤： 1) 访谈邮件系统运维人员，询问安全风险评估是否覆盖业务及应用安全、网络安全、设备及软件系统安全、物理环境安全、管理安全等相关技术风险和人员安全、运维安全等相关管理风险； 2) 查看风险评估记录
预期结果： 安全风险评估覆盖业务及应用安全、网络安全、设备及软件系统安全、物理环境安全、管理安全等相关技术风险和人员安全、运维安全等相关管理风险
判定原则： 达到以上预期结果，则通过，否则不通过

5.2.5.5 灾难恢复预案

测试编号：邮件系统-第2级-管理安全-灾难恢复预案-01
测试项目：《邮件系统安全防护要求》5.2.5.5-a，应按照 YD/T 1731-2008 的相关要求制定完整的灾难恢复预案及对应管理制度
测试步骤： 1) 访谈邮件系统运维人员，询问是否按照 YD/T 1731-2008 的相关要求制定完整的灾难恢复预案及对应管理制度； 2) 查看相关制度
预期结果： 按照 YD/T 1731-2008 的相关要求制定完整的灾难恢复预案及对应管理制度
判定原则： 达到以上预期结果，则通过，否则不通过

测试编号：邮件系统-第 2 级-管理安全-灾难恢复预案-02
测试项目：《邮件系统安全防护要求》5.2.5.5-b，应有灾难恢复预案的教育和培训（至少每半年一次），相关人员应了解灾难恢复预案并具有对灾难恢复预案进行实际操作的能力
测试步骤： 1) 访谈邮件系统运维人员，询问是否有灾难恢复预案的教育和培训（至少每半年一次）； 2) 访谈相关人员，询问是否了解灾难恢复预案并具有对灾难恢复预案进行实际操作的能力
预期结果： 有灾难恢复预案的教育和培训（至少每半年一次），相关人员应了解灾难恢复预案并具有对灾难恢复预案进行实际操作的能力
判定原则： 达到以上预期结果，则通过，否则不通过

测试编号：邮件系统-第 2 级-管理安全-灾难恢复预案-03
测试项目：《邮件系统安全防护要求》5.2.5.5-c，应有灾难恢复预案的演练（至少每年一次），并根据演练结果对灾难恢复预案进行修正
测试步骤： 1) 访谈邮件系统运维人员，询问是否有灾难恢复预案的演练（至少每年一次），并根据演练结果对灾难恢复预案进行修正； 2) 查看演练记录及预案修正记录
预期结果： 有灾难恢复预案的演练（至少每年一次），并根据演练结果对灾难恢复预案进行修正
判定原则： 达到以上预期结果，则通过，否则不通过

5.3 第3级要求

除按照第2级的要求进行检测之外，还应按照本节内容进行检测。

5.3.1 业务及应用安全

5.3.1.1 身份鉴别

测试编号：邮件系统-第3级-业务及应用安全-身份鉴别-01
测试项目：《邮件系统安全防护要求》5.3.1.1-a，应提供并启用用户登录认证口令复杂度强度功能，保证业务使用用户的口令长度不小于8位，口令应有复杂度要求（使用大写字母、小写字母、数字、标点及特殊字符组合，且与用户名或身份标识无相关性）并提示用户定期更换
测试步骤： 1) 访谈网络运维和安全管理人員，查看网络安全策略、账号管理和权限分配记录、设备配置文件、安全检查记录等，查看业务及应用系统的账号口令更新情况； 2) 测试注册账号少于8位或复杂度简单的口令，验证是否能够提示用户修改口令
预期结果： 1) 启用用户登录认证口令复杂度强度功能，保证业务使用用户的口令长度不小于8位，口令有复杂度要求； 2) 提示用户定期更新口令
判定原则： 达到以上预期结果，则通过，否则不通过

5.3.1.2 访问控制

测试编号：邮件系统-第3级-业务及应用安全-访问控制-01
测试项目：《邮件系统安全防护要求》5.3.1.2-a，应严格设置业务使用用户解锁策略，按安全策略要求，被锁定的业务使用用户需通过注册时的标志信息进行密码重新设定或者凭有效证件进行设定
测试步骤： 1) 使用测试账号，验证连续登录； 2) 查看测试账号的操作是否受到系统限制； 3) 在客户端多次尝试失败后，服务器端是否对用户账号进行短时锁定； 4) 验证解锁是否需要使用用户需通过注册时的标志信息或者凭有效证件
预期结果： 1) 已设置业务使用用户解锁策略； 2) 被锁定的业务使用用户需通过注册时的标志信息进行密码重新设定或者凭有效证件进行设定
判定原则： 达到以上预期结果，则通过，否则不通过

5.3.1.3 安全审计

测试编号：邮件系统-第3级-业务及应用安全-安全审计-01
测试项目：《邮件系统安全防护要求》5.3.1.3-a，应提供对审计记录数据进行统计、查询、分析及生成审计报表的功能
测试步骤： <ol style="list-style-type: none"> 1) 检查设计/验收文档，系统是否能根据记录数据进行统计、查询、分析，并生成审计报表； 2) 验证是否对记录数据进行分析； 3) 验证是否生成审计报表
预期结果： <ol style="list-style-type: none"> 1) 设计/验收文档中，系统能根据记录数据进行分析，并生成审计报表； 2) 实际系统对记录数据进行了分析； 3) 实际系统生成了审计报表
判定原则： 达到以上预期结果，则通过，否则不通过

5.3.1.4 数据安全性

测试编号：邮件系统-第3级-业务及应用安全-数据安全性-01
测试项目：《邮件系统安全防护要求》5.3.1.4-a，应采用足够强壮的加密算法保证用户登录认证过程数据不被非授权利用和篡改
测试步骤： <ol style="list-style-type: none"> 1) 查看设计文档，验证是否采用足够强壮的加密算法加密用户登录认证过程数据； 2) 通过技术手段，查看用户登录认证过程数据是否被加密，是否能确保数据不被非授权利用和篡改
预期结果： 采用足够强壮的加密算法保证用户登录认证过程数据不被非授权利用和篡改
判定原则： 达到以上预期结果，则通过，否则不通过

测试编号：邮件系统-第3级-业务及应用安全-数据安全性-02
测试项目：《邮件系统安全防护要求》5.3.1.4-b，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符合系统设定要求，确保非常规数据被过滤
测试步骤： <ol style="list-style-type: none"> 1) 检查设计/验收文档，确认系统是否对输入数据做了严格验证； 2) 向系统输入合法数据，验证系统是否能够正确处理合法数据； 3) 向系统输入非法数据（如恶意链接等），验证系统是否能够过滤非常规数据
预期结果： <ol style="list-style-type: none"> 1) 在系统设计时，对输入数据做了严格验证； 2) 系统对输入的合法数据，能够正确处理； 3) 对输入的非法数据，系统能够过滤非常规数据
判定原则： 达到以上预期结果，则通过，否则不通过

测试编号：邮件系统-第3级-业务及应用安全-数据安全性-03
测试项目：《邮件系统安全防护要求》5.3.1.4-c，应对邮件内容进行数据保护，采取非明文存储方式，确保加密或者编码算法符合国家商用密码管理办法的相关要求
测试步骤： <ol style="list-style-type: none"> 1) 检查设计/验收文档，确认是否对邮件内容进行加密保护； 2) 检查实际系统中是否对邮件内容是否采取非明文存储方式，检查所采取的加密或者编码算法是否符合国家商用密码管理办法的相关要求
预期结果： <ol style="list-style-type: none"> 1) 设计时，系统对邮件内容进行加密保护； 2) 实际系统采取非明文存储方式，且加密或者编码算法符合国家商用密码管理办法的相关要求
判定原则： 达到以上预期结果，则通过，否则不通过

5.3.1.5 信息保护

测试编号：邮件系统-第3级-业务及应用安全-信息保护-01
测试项目：《邮件系统安全防护要求》5.3.1.6-a，应保护系统服务相关信息的安全，避免有关数据被篡改和破坏
测试步骤： <ol style="list-style-type: none"> 1) 检查设计/验收文档，确认系统是否采取措施保护系统服务相关信息； 2) 通过技术手段，检查系统服务相关信息是否采取措施避免数据被篡改和破坏
预期结果： <ol style="list-style-type: none"> 1) 系统采取措施保护系统服务相关信息； 2) 能够避免有关数据被篡改和破坏
判定原则： 达到以上预期结果，则通过，否则不通过

5.3.1.6 Web 安全

测试编号：邮件系统-第3级-业务及应用安全-Web 安全-01
测试项目：《邮件系统安全防护要求》5.3.1.7-a，web 程序上线前或升级后应进行代码审计，形成报告，并对审计出的问题进行代码升级完善
测试步骤： <ol style="list-style-type: none"> 1) 询问是否在 WEB 程序上线前或升级后进行代码审计； 2) 确认代码审计是否形成了审计报告； 3) 查看形成的审计报告； 4) 查看是否对审计发现的问题进行代码升级完善
预期结果： <ol style="list-style-type: none"> 1) WEB 程序上线前或升级后进行了代码审计； 2) 代码审计形成了审计报告； 3) 审计报告符合要求； 4) 对审计发现的问题进行了代码升级完善
判定原则： 达到以上预期结果，则通过，否则不通过

5.3.1.7 客户端安全

测试编号：邮件系统-第3级-业务及应用安全-客户端安全-01
测试项目：《邮件系统安全防护要求》5.3.1.8-a，应避免使用含有已公开漏洞的开源第三方应用组件及代码（漏洞库可参考 CVE、CNVD 等）
测试步骤： 1) 查询相关文档，并询问是否使用开源第三方应用组件及代码； 2) 询问使用的开源第三方应用组件及代码是否存在已公开漏洞（漏洞库可参考 CVE、CNVD 等）； 3) 对已公开漏洞是否已及时更新补丁； 4) 查看是否对已公开漏洞（漏洞库可参考 CVE、CNVD 等）及时更新补丁
预期结果： 使用开源第三方应用组件及代码时，已对已公开漏洞（漏洞库可参考 CVE、CNVD 等）及时更新补丁
判定原则： 达到以上预期结果，则通过，否则不通过

5.3.1.8 对外接口安全

同第2级要求。

5.3.2 网络安全

5.3.2.1 网络结构安全

测试编号：邮件系统-第3级-网络安全-网络结构安全-01
测试项目：《邮件系统安全防护要求》5.3.2.1-a，应根据系统内部网络结构特点，按照统一的管理和控制原则划分不同的子网或网段，设备依照功能划分及其重要性等因素分区部署
测试步骤： 1) 访谈网络运维人员，检查系统设计/验收文档、系统安全策略、系统及设备管理和配置文档、网络和业务运营商/服务提供商提供的其他文档； 2) 检查现有网络划分是否按照统一的管理和控制原则； 3) 检查验证设备是否依照功能划分及其重要性等因素分区部署
预期结果： 1) 实际网络按照统一的管理和控制原则划分不同的子网或网段； 2) 设备依照功能划分及其重要性等因素分区部署
判定原则： 达到以上预期结果，则通过，否则不通过

测试编号：邮件系统-第3级-网络安全-网络结构安全-02
测试项目：《邮件系统安全防护要求》5.3.2.1-b，不考虑主动宕机维护的情况，可靠性应达到99%以上
测试步骤： 1) 访谈网络运维人员，检查系统设计/验收文档、系统安全策略、系统及设备管理和配置文档、网络和业务运营商/服务提供商提供的其他文档； 2) 检查验证系统故障记录，验证可靠性是否达到99%以上
预期结果： 邮件系统可靠性达到99%以上
判定原则： 达到以上预期结果，则通过，否则不通过

测试编号：邮件系统-第3级-网络安全-网络结构安全-03
测试项目：《邮件系统安全防护要求》5.3.2.1-c，应具备必要的流量负荷分担设计
测试步骤： 1) 访谈网络运维人员，检查系统设计/验收文档、系统及设备管理和配置文档、网络和业务运营商/服务提供商提供的其他文档； 2) 检查系统是否具有必要的流量负荷分担设计
预期结果： 1) 具备必要的流量负荷分担设计； 2) 系统分担技术措施有效
判定原则： 达到以上预期结果，则通过，否则不通过

5.3.2.2 网络监测

测试编号：邮件系统-第3级-网络安全-网络监测-01
测试项目：《邮件系统安全防护要求》5.3.2.2-a，应监测并禁止不必要的内嵌网络服务，应禁止在用户端自动安装恶意软件和插件
测试步骤： 1) 访谈网络运维人员，检查系统设计/验收文档、系统及设备管理和配置文档、网络和业务运营商/服务提供商提供的其他文档； 2) 检查系统是否监测并禁止不必要的内嵌网络服务； 3) 检查系统是否禁止在用户端自动安装恶意软件和插件
预期结果： 1) 系统监测并禁止不必要的内嵌网络服务； 2) 系统禁止在用户端自动安装恶意软件和插件
判定原则： 达到以上预期结果，则通过，否则不通过

测试编号：邮件系统-第3级-网络安全-网络监测-02
测试项目：《邮件系统安全防护要求》5.3.2.2-b，应在系统边界处对发生的网络入侵行为（包括但不限于强力攻击、木马后门攻击、DoS/DDoS 攻击、缓冲区溢出攻击、IP 碎片攻击和网络蠕虫攻击）提供有效的监测能力。当监测到入侵行为时应能立即断开入侵者与主机之间的连接，向管理人员发出警报，并记录攻击源 IP、攻击类型、攻击目的、攻击时间
测试步骤： <ol style="list-style-type: none"> 1) 查看系统中是否部署入侵防范软件； 2) 检查系统是否对重要服务器进行入侵行为的监测； 3) 检查系统能否记录入侵的源 IP、攻击的类型、攻击的目的地址、攻击的时间； 4) 检查记录系统在发生严重入侵事件时，是否向管理人员发出警报
预期结果： <ol style="list-style-type: none"> 1) 系统对边界处进行入侵行为监测； 2) 系统能够记录入侵的源 IP、攻击的类型、攻击的目的地址、攻击的时间； 3) 系统能在严重入侵事件发生时向管理人员发出警报
判定原则： 达到以上预期结果，则通过，否则不通过

5.3.2.3 安全审计

测试编号：邮件系统-第3级-网络安全-安全审计-01
测试项目：《邮件系统安全防护要求》5.3.2.3-a，应提供对审计记录数据进行统计、查询、分析及生成审计报表的功能
测试步骤： <ol style="list-style-type: none"> 1) 检查设计/验收文档，系统是否能根据记录数据进行统计、查询、分析，并生成审计报表； 2) 验证是否对记录数据进行分析； 3) 验证是否生成审计报表
预期结果： <ol style="list-style-type: none"> 1) 设计/验收文档中，系统能根据记录数据进行分析，并生成审计报表； 2) 实际系统对记录数据进行了分析； 3) 实际系统生成了审计报表
判定原则： 达到以上预期结果，则通过，否则不通过

5.3.3 设备及软件操作系统安全

5.3.3.1 网络及安全设备

测试编号：邮件系统-第3级-设备及软件操作系统安全-网络及安全设备-01
测试项目：《邮件系统安全防护要求》5.3.3.1-a，网络及安全设备应启用登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施
测试步骤： 1) 访谈网络运维人员，检查系统设计/验收文档、系统安全策略、系统管理和配置文档； 2) 查看网络及安全设备是否启用登录失败处理功能； 3) 查看是否采取结束会话、限制非法登录次数和自动退出等措施
预期结果： 1) 网络及安全设备已启用登录失败处理功能； 2) 网络及安全设备已采取结束会话、限制非法登录次数和自动退出等措施
判定原则： 达到以上预期结果，则通过，否则不通过

测试编号：邮件系统-第3级-设备及软件操作系统安全-网络及安全设备-02
测试项目：《邮件系统安全防护要求》5.3.3.1-b，网络及安全设备应通过设定终端接入方式、网络地址范围等条件限制管理终端登录
测试步骤： 1) 访谈网络运维人员，检查系统设计/验收文档、系统安全策略、系统管理和配置文档； 2) 测试网络及安全设备是否通过设定终端接入方式、网络地址范围等条件限制管理终端登录
预期结果： 网络及安全设备通过设定终端接入方式、网络地址范围等条件限制管理终端登录
判定原则： 达到以上预期结果，则通过，否则不通过

测试编号：邮件系统-第3级-设备及软件操作系统安全-网络及安全设备-03
测试项目：《邮件系统安全防护要求》5.3.3.1-c，网络及安全设备进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听
测试步骤： 1) 检查设计/验收文档，确定对网络及安全设备进行远程管理时，是否采取必要措施，防止鉴别信息在传输过程中被窃听； 2) 使用测试账号对网络及安全设备进行远程管理，检查是否采取必要措施，防止鉴别信息在传输过程中被窃听
预期结果： 对网络及安全设备进行远程管理时，采取必要措施防止鉴别信息在传输过程中被窃听
判定原则： 达到以上预期结果，则通过，否则不通过

5.3.3.2 通用主机操作系统

5.3.3.2.1 安全检测

同第2级要求。

5.3.3.2.2 身份鉴别

测试编号：邮件系统-第3级-通用主机操作系统-身份鉴别-01
测试项目：《邮件系统安全防护要求》5.3.3.2.2-a，各个功能模块的计算机运维终端、服务器等设备的主机操作系统应启用登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施
测试步骤： 1) 访谈网络运维人员，检查系统设计/验收文档、系统安全策略、系统管理和配置文档； 2) 查看各个功能模块的计算机运维终端、服务器等设备的主机操作系统是否启用登录失败处理功能； 3) 查看是否采取结束会话、限制非法登录次数和自动退出等措施
预期结果： 1) 各个功能模块的计算机运维终端、服务器等设备的主机操作系统已启用登录失败处理功能； 2) 采取结束会话、限制非法登录次数和自动退出等措施
判定原则： 达到以上预期结果，则通过，否则不通过

测试编号：邮件系统-第3级-通用主机操作系统-身份鉴别-02
测试项目：《邮件系统安全防护要求》5.3.3.2.2-b，各个功能模块的计算机运维终端、服务器等设备进行远程管理时，应采取必要措施，防止鉴别信息在传输过程中被窃听
测试步骤： 1) 检查设计/验收文档，确定对各个功能模块的计算机运维终端、服务器等设备进行远程管理时，是否采取必要措施，防止鉴别信息在传输过程中被窃听； 2) 使用测试账号对各个功能模块的计算机运维终端、服务器等设备进行远程管理，检查是否采取必要措施，防止鉴别信息在传输过程中被窃听
预期结果： 对各个功能模块的计算机运维终端、服务器等设备进行远程管理时，采取必要措施防止鉴别信息在传输过程中被窃听
判定原则： 达到以上预期结果，则通过，否则不通过

5.3.3.2.3 访问控制

同第2级要求。

5.3.3.2.4 安全审计

测试编号：邮件系统-第3级-通用主机操作系统-安全审计-01
测试项目：《邮件系统安全防护要求》5.3.3.2.4-a，各个功能模块的计算机运维终端、服务器等设备的审计记录，避免其受到未预期的删除、修改或覆盖等，保留一定期限（至少180天）
测试步骤： 1) 查看审计系统及记录； 2) 对记录进行删除、修改、覆盖等操作，验证审计记录是否可避免其受到未预期的删除、修改或覆盖等； 3) 检查是否保留一定期限（至少180天）
预期结果： 1) 系统能够保护审计记录，避免其受到未预期的删除、修改或覆盖等； 2) 审计记录能保留一定期限（至少180天）
判定原则： 达到以上预期结果，则通过，否则不通过

5.3.3.2.5 资源控制

测试编号：邮件系统-第3级-通用主机操作系统-资源控制-01
测试项目：《邮件系统安全防护要求》5.3.3.2.5-a，应能够对各个模块的服务器进行性能和服务水平监控，监控方式可基于监听、SNMP等网管技术和协议；并设定阈值，在监测到服务水平降低到阈值时进行报警
测试步骤： 1) 访谈网络运维人员，查看网络安全策略、设备配置记录、故障告警记录、日志和审计记录等，查看邮件系统对各个模块的服务器进行性能和服务水平监控情况； 2) 检查监控方式是否基于监听、SNMP等网管技术和协议； 3) 检查是否设定阈值，并在监测到服务水平降低到阈值时进行报警
预期结果： 1) 邮件系统能够对各个模块的服务器进行性能和服务水平监控； 2) 监控方式可基于监听、SNMP等网管技术和协议； 3) 邮件系统能够设定阈值，并在监测到服务水平降低到阈值时进行报警
判定原则： 达到以上预期结果，则通过，否则不通过

5.3.3.2.6 冗余备份

测试编号：邮件系统-第3级-通用主机操作系统-冗余备份-01
测试项目：《邮件系统安全防护要求》5.3.3.2.6-a，a)各个功能模块的服务器应对主机关键数据（如主机配置数据、管理员操作维护记录、用户信息等）和重要信息进行异址（同城不同地点的机房或异地）备份，并建立恢复的管理和控制机制；
测试步骤： <ol style="list-style-type: none"> 1) 访谈网络运维人员，检查系统设计/验收文档、系统安全策略、系统管理和配置文档； 2) 询问并现网查看是否对主机关键数据（如主机配置数据、管理员操作维护记录、用户信息等）和重要信息进行异址（同城不同地点的机房或异地）备份； 3) 询问并现网查看是否建立恢复的管理和控制机制
预期结果： <ol style="list-style-type: none"> 1) 对主机关键数据（如主机配置数据、管理员操作维护记录、用户信息等）和重要信息，进行异址（同城不同地点的机房或异地）备份； 2) 已建立恢复的管理和控制机制
判定原则： <p>达到以上预期结果，则通过，否则不通过</p>

测试编号：邮件系统-第3级-通用主机操作系统-冗余备份-02
测试项目：《邮件系统安全防护要求》5.3.3.2.6-b，相关主机数据备份范围和时间间隔、数据恢复能力应满足行业管理、业务运营企业应急预案相关要求
测试步骤： <ol style="list-style-type: none"> 1) 访谈网络运维人员，检查系统设计/验收文档、系统安全策略、系统管理和配置文档； 2) 查看相关主机数据备份文件及记录，检查其范围和时间间隔、数据恢复能力是否满足行业管理、业务运营企业应急预案相关要求
预期结果： <p>相关主机数据备份范围和时间间隔、数据恢复能力满足行业管理、业务运营企业应急预案相关要求</p>
判定原则： <p>达到以上预期结果，则通过，否则不通过</p>

5.3.3.3 数据库及中间件软件

5.3.3.3.1 安全检测

同第2级要求。

5.3.3.3.2 身份鉴别

测试编号：邮件系统-第3级-数据库及中间件软件-身份鉴别-01
测试项目：《邮件系统安全防护要求》5.3.3.3.2-a，应对邮件系统中各个功能模块的数据库及中间件软件应启用登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施
测试步骤： <ol style="list-style-type: none"> 1) 访谈网络运维人员，检查系统设计/验收文档、系统安全策略、系统管理和配置文档； 2) 查看各个功能模块的数据库及中间件软件是否启用登录失败处理功能； 3) 查看是否采取结束会话、限制非法登录次数和自动退出等措施
预期结果： <ol style="list-style-type: none"> 1) 各个功能模块的数据库及中间件软件已启用登录失败处理功能； 2) 采取结束会话、限制非法登录次数和自动退出等措施
判定原则： <p>达到以上预期结果，则通过，否则不通过</p>

测试编号：邮件系统-第3级-数据库及中间件软件-身份鉴别-02
测试项目：《邮件系统安全防护要求》5.3.3.3.2-b，应对邮件系统中各个功能模块的数据库及中间件软件进行远程管理时，应采取必要措施，防止鉴别信息在传输过程中被窃听
测试步骤： <ol style="list-style-type: none"> 1) 检查设计/验收文档，确定对各个功能模块的数据库及中间件软件进行远程管理时，是否采取必要措施，防止鉴别信息在传输过程中被窃听； 2) 使用测试账号对各个功能模块的数据库及中间件软件进行远程管理，检查是否采取必要措施，防止鉴别信息在传输过程中被窃听
预期结果： <p>对各个功能模块的数据库及中间件软件进行远程管理时，采取必要措施防止鉴别信息在传输过程中被窃听</p>
判定原则： <p>达到以上预期结果，则通过，否则不通过</p>

5.3.3.3.3 访问控制

同第2级要求。

5.3.3.3.4 安全审计

测试编号：邮件系统-第3级-数据库及中间件软件-安全审计-01
测试项目：《邮件系统安全防护要求》5.3.3.3.4-a，各个功能模块的数据库及中间件软件的审计记录，避免其受到未预期的删除、修改或覆盖等，保留一定期限（至少180天）
<p>测试步骤：</p> <ol style="list-style-type: none"> 1) 查看审计系统及记录； 2) 对记录进行删除、修改、覆盖等操作，验证审计记录是否可避免其受到未预期的删除、修改或覆盖等； 3) 检查是否保留一定期限（至少180天）
<p>预期结果：</p> <ol style="list-style-type: none"> 1) 系统能够保护审计记录，避免其受到未预期的删除、修改或覆盖等； 2) 审计记录能保留一定期限（至少180天）
<p>判定原则：</p> <p>达到以上预期结果，则通过，否则不通过</p>

5.3.3.3.5 资源控制

测试编号：邮件系统-第3级-数据库及中间件软件-资源控制-01
测试项目：《邮件系统安全防护要求》5.3.3.3.5-a，应对各个功能模块的数据库及中间件软件进行性能和服务水平监控，监控方式可基于监听、SNMP等网管技术和协议；并设定阈值，在监测到服务水平降低到阈值时进行报警
<p>测试步骤：</p> <ol style="list-style-type: none"> 1) 访谈网络运维人员，查看网络安全策略、设备配置记录、故障告警记录、日志和审计记录等，查看邮件系统对各个功能模块的数据库及中间件软件进行性能和服务水平监控情况； 2) 检查监控方式是否基于监听、SNMP等网管技术和协议； 3) 检查是否设定阈值，并在监测到服务水平降低到阈值时进行报警
<p>预期结果：</p> <ol style="list-style-type: none"> 1) 邮件系统能够对各个功能模块的数据库及中间件软件进行性能和服务水平监控； 2) 监控方式可基于监听、SNMP等网管技术和协议； 3) 邮件系统能够设定阈值，并在监测到服务水平降低到阈值时进行报警
<p>判定原则：</p> <p>达到以上预期结果，则通过，否则不通过</p>

5.3.3.3.6 冗余备份

测试编号：邮件系统-第3级-数据库及中间件软件-冗余备份-01
测试项目：《邮件系统安全防护要求》5.3.3.3.6-a，各个功能模块的数据库及中间件软件应对关键数据（如配置数据、管理员操作维护记录、用户信息等）和重要信息进行异址（同城不同地点的机房或异地）备份，并建立恢复的管理和控制机制
测试步骤： <ol style="list-style-type: none"> 1) 访谈网络运维人员，检查系统设计/验收文档、系统安全策略、系统管理和配置文档； 2) 询问并现网查看是否对关键数据（如配置数据、管理员操作维护记录、用户信息等）和重要信息进行异址（同城不同地点的机房或异地）备份； 3) 询问并现网查看是否建立恢复的管理和控制机制
预期结果： <ol style="list-style-type: none"> 1) 对各个功能模块的数据库及中间件软件关键数据（如主机配置数据、管理员操作维护记录、用户信息等）和重要信息进行异址（同城不同地点的机房或异地）备份； 2) 已建立恢复的管理和控制机制
判定原则： 达到以上预期结果，则通过，否则不通过

测试编号：邮件系统-第3级-数据库及中间件软件-冗余备份-02
测试项目：《邮件系统安全防护要求》5.3.3.3.6-b，各个功能模块的数据库及中间件软件中相关数据备份范围和时间间隔、数据恢复能力应满足行业管理、业务运营企业应急预案相关要求
测试步骤： <ol style="list-style-type: none"> 1) 访谈网络运维人员，检查系统设计/验收文档、系统安全策略、系统管理和配置文档； 2) 查看相关各个功能模块的数据库及中间件软件数据备份文件及记录，检查其范围和时间间隔、数据恢复能力是否满足行业管理、业务运营企业应急预案相关要求
预期结果： 相关数据库及中间件软件数据备份范围和时间间隔、数据恢复能力满足行业管理、业务运营企业应急预案相关要求
判定原则： 达到以上预期结果，则通过，否则不通过

5.3.4 物理环境安全要求

测试编号：邮件系统-第3级-物理环境安全要求-01
测试项目：《邮件系统安全防护要求》5.3.4-a，应满足第2级、YD/T 1754-2008 中第3.1级的相关要求
测试步骤： 1) 访谈运维人员，查看邮件系统设计/验收文档等是否符合 YD/T 1754-2008 中的第3.1级要求； 2) 检查邮件系统物理环境设计是否 YD/T 1754-2008 中的第3.1级要求
预期结果： 物理环境满足 YD/T 1754-2008 中的第3.1级要求
判定原则： 达到以上预期结果，则通过，否则不通过

5.3.5 管理安全要求

测试编号：邮件系统-第3级-管理安全要求-01
测试项目：《邮件系统安全防护要求》5.3.5-a，应满足第2级、YD/T 1756-2008 中第3.1级的相关要求
测试步骤： 1) 访谈管理人员，查看邮件系统设计/验收文档等是否符合第2级、YD/T 1756-2008 中第3.1级的相关要求； 2) 检查邮件系统是否符合第2级、YD/T 1756-2008 中第3.1级的相关要求
预期结果： 满足第2级、YD/T 1756-2008 中第3.1级的相关要求
判定原则： 达到以上预期结果，则通过，否则不通过

测试编号：邮件系统-第3级-管理安全要求-02
测试项目：《邮件系统安全防护要求》5.3.5-b，应设有专职的操作、维护技术人员和安全管理人員，应定期组织对相关人员进行技术培训和考核
测试步骤： 1) 访谈管理人员，询问是否设有专职的操作、维护技术人员和安全管理人員，是否定期组织对相关人员进行技术培训和考核； 2) 查看人员名单及培训考核记录
预期结果： 1) 设有专职的操作、维护技术人员和安全管理人員； 2) 定期组织对相关人员进行技术培训和考核，并有相关记录
判定原则： 达到以上预期结果，则通过，否则不通过

测试编号：邮件系统-第 3 级-管理安全要求- 03
测试项目：《邮件系统安全防护要求》5.3.5-c，灾难恢复预案应按照安全管理制度相关的制修订要求进行管理
测试步骤： 1) 访谈管理人员，询问灾难恢复预案是否按照安全管理制度相关的制修订要求进行管理； 2) 查看相关灾难恢复预案
预期结果： 灾难恢复预案按照安全管理制度相关的制修订要求进行管理
判定原则： 达到以上预期结果，则通过，否则不通过

5.4 第 4 级要求

待定。

5.5 第 5 级要求

待定。

参 考 文 献

- | | | |
|---|----------------|--------------------|
| 1 | YD/T 1728-2008 | 电信网和互联网安全防护管理指南 |
| 2 | YD/T 1729-2008 | 电信网和互联网安全等级保护实施指南 |
| 3 | YD/T 1730-2008 | 电信网和互联网安全风险评估实施指南 |
| 4 | YD/T 1731-2008 | 电信网和互联网灾难备份及恢复实施指南 |