

YD

中华人民共和国通信行业标准

YD/T 3215—2017

互联网资源协作服务 信息安全管理系统及接口测试方法

Test methods of information security management system
for Internet resource collaboration service

2017-01-09 发布

2017-01-09 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 术语和定义	1
4 缩略语	1
5 测试对象概述	1
6 测试环境	2
7 ISMS 技术要求测试	2
7.1 概述	2
7.2 基础数据管理	3
7.3 动态资源管理	8
7.4 业务状态管理	10
7.5 信息安全管理	12
7.6 访问日志管理	19
7.7 系统功能管理	20
7.8 性能要求	22
7.9 安全性要求	26
7.10 基础数据查询与上报	27
7.11 动态资源查询与上报	32
7.12 业务状态记录上报	32
7.13 信息安全记录上报	33
7.14 访问日志查询与上报	39
7.15 性能要求测试	39
7.16 安全性要求测试	44
8 ISMS 接口测试	44
8.1 消息流程测试	44
8.2 接口方法测试	46
8.3 健壮性测试	50

前 言

本标准是“互联网信息安全管理技术手段”系列标准之一，该系列标准结构和名称预计如下：

YD/T 2248 《互联网数据中心和互联网接入服务信息安全管理系统技术要求》；

YD/T 2405 《互联网数据中心和互联网接入服务信息安全管理系统接口规范》；

YD/T 2406 《互联网数据中心和互联网接入服务信息安全管理系统及接口测试方法》；

YD/T 3165 《内容分发网络服务信息安全管理系统技术要求》；

YD/T 3212 《内容分发网络服务信息安全管理系统接口规范》；

YD/T 3213 《内容分发网络服务信息安全管理系统及接口测试方法》；

YD/T 3164 《互联网资源协作服务信息安全管理系统技术要求》；

YD/T 3214 《互联网资源协作服务信息安全管理系统接口规范》；

YD/T 3215 《互联网资源协作服务信息安全管理系统及接口测试方法》。

随着互联网各类业务和应用的发展，将不断补充和完善本系列的相关标准。

本标准按照 GB/T 1.1—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、浙江省通信管理局、阿里云计算有限公司。

本标准主要起草人：景慧昀、柳青、杨剑锋、干萌、罗亮、王丽耀、魏薇、张慧珍、谷长信、郭岳、张昊星、杜伟、钱康、杨振雄、金字、张旭洲、吴振刚、周丽丽、李冠华、苗琳。

互联网资源协作服务信息安全管理系统及接口测试方法

1 范围

本标准规定了互联网资源协作服务（IRCS）信息安全管理系统及接口相关的测试要求，包括测试方法、测试内容、测试用例等。

本标准适用于 IRCS 信息安全管理系统的测试和评估工作。

2 规范性引用文件

下列文件中的条款通过本标准的引用而成为本标准的条款。凡是注日期的引用文件，其随后所有的修改单（不包括勘误的内容）或修订版均不适用于本标准。然而，鼓励根据本标准达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件，其最新版本适用于本标准。

YD/T 3164—2016 互联网资源协作服务信息安全管理系统技术要求

YD/T 3214 互联网资源协作服务信息安全管理系统接口规范

3 术语和定义

YD/T 3164—2016 界定的术语和定义适用于本文件。

4 缩略语

下列缩略语适用于本文件：

IRCS	互联网资源协作服务	Internet Resource Collaboration Service
IP	互联网协议	Internet Protocol
ISMI	信息安全管理接口	Information Security Management Interface
ISMS	信息安全管理系统	Information Security Management System
SMMS	安全监管系统	Security Monitor Management System
SUT	被测系统	System Under Test
URL	统一资源定位符	Uniform Resource Locator

5 测试对象概述

测试对象为 IRCS 经营单位建设和管理的 IRCS 信息安全管理系统。

IRCS 信息安全管理系统是 IRCS 业务经营者建设的具有基础数据管理、动态资源管理、业务状态管理、信息安全管理、访问日志管理等功能的信息安全管理系统，以满足 IRCS 业务经营者和电信管理部门的信息安全管理需求。

ISMS 与 SMMS 之间的关系如图 1 所示。

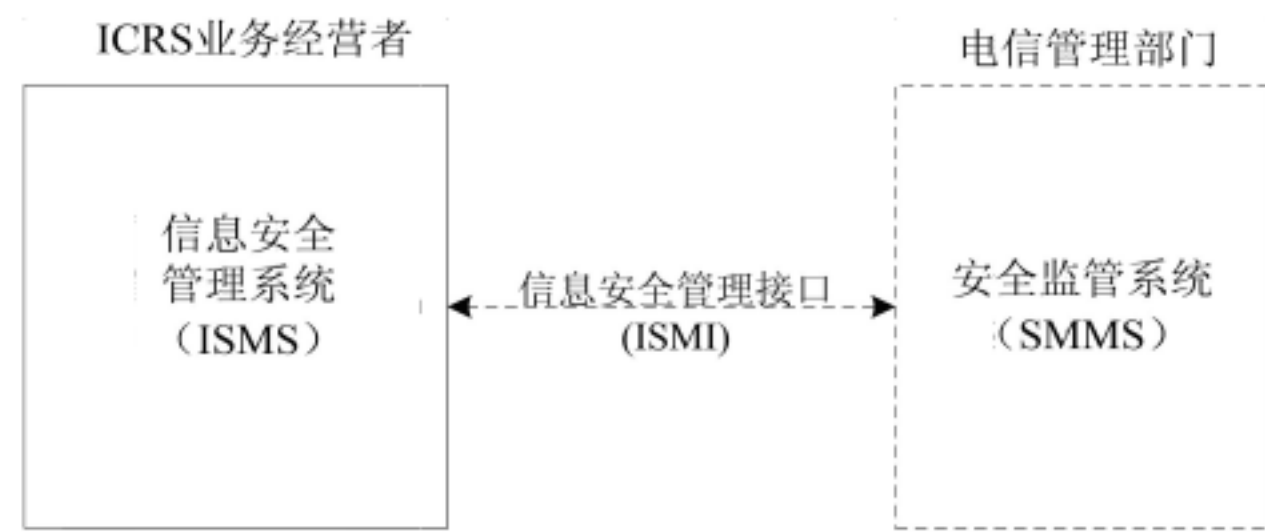


图 1 ISMS 与 SMMS 关系示意

6 测试环境

测试环境示意如图 2 所示。

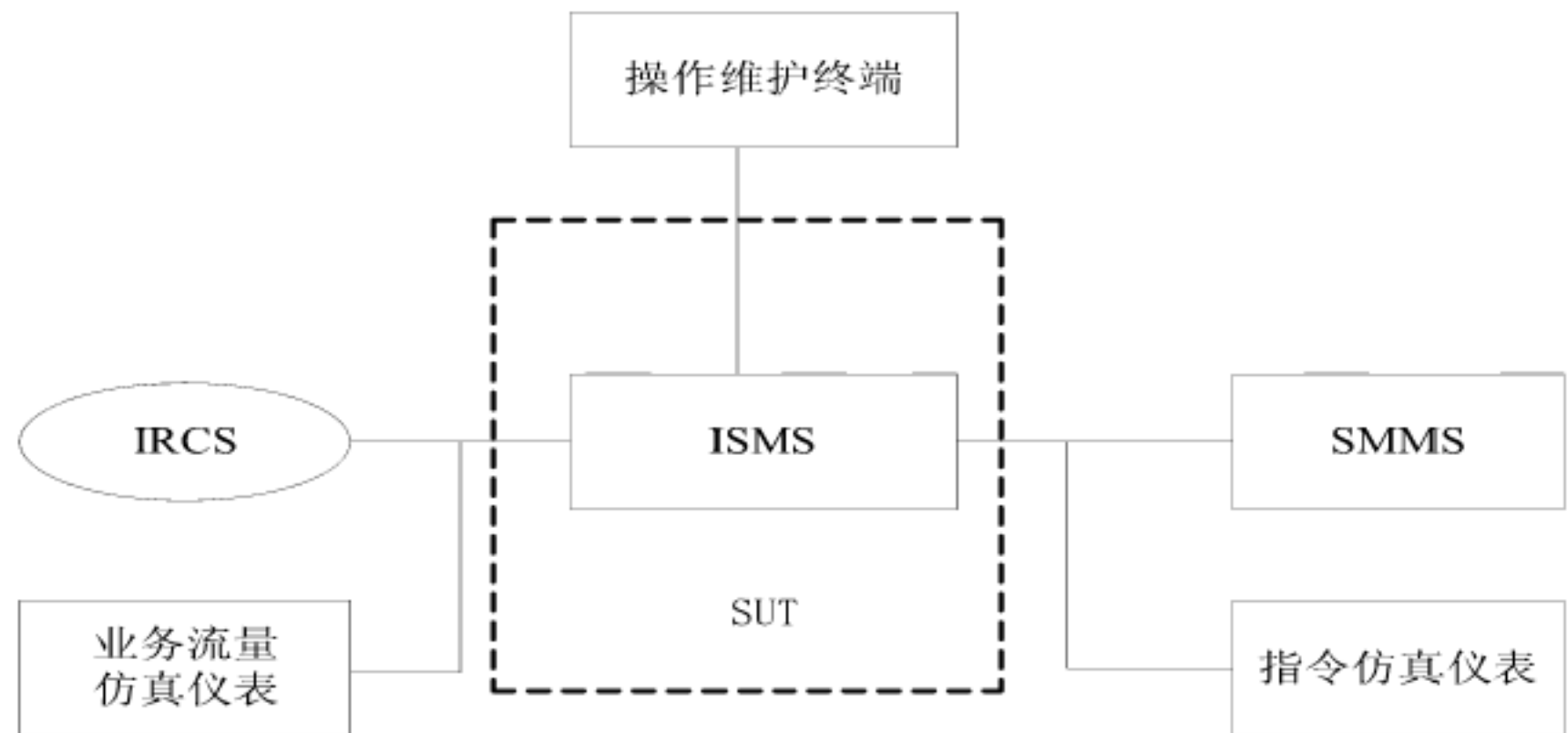


图 2 测试环境

其中，指令仿真仪表可模拟和仿真 SMMS 发送各类测试消息和指令，并可接收和解析 ISMS 的各类响应消息、上报数据；操作维护终端可对 ISMS 进行正常操作和管理；业务流量仿真仪表可模拟和仿真 IRCS 内各类业务资源和应用流量。

7 ISMS 技术要求测试

7.1 概述

ISMS 技术要求测试主要评测内容包括两部分，第一部分为系统功能与性能指标测试，第二部分为系统对接功能指标测试。

系统功能与性能指标测试内容包括：

- a) 基础数据管理，包括如基础数据本地管理、查询和导入核验等相关功能；
- b) 动态资源管理，包括动态资源使用日志记录、动态资源使用日志查询；
- c) 业务状态管理，包括活跃状态监测管理、异常状态监测管理；
- d) 信息安全管理，包括如违法违规网站管理，违法信息监测、过滤，规则优先级验证等相关功能；
- e) 访问日志管理，包括如访问日志记录功能、内容和查询等相关功能；
- f) 系统功能管理，系统权限管理和运行维护管理等相关功能；
- g) 性能指标及安全性，包括规则容量、规则匹配准确率、数据更新时间、日志查询响应时间、时钟同步、数据备份与恢复等相关指标。

具体评测项目见 7.2 至 7.8。

系统对接功能指标测试内容包括：

- a) 基础数据查询与上报，在企业完整上报真实基础数据的前提下，验证基础数据更新上报与查询，基础数据异常核验等相关功能；
- b) 动态资源查询与上报，验证现网环境下动态资源使用日志查询及响应的相关功能；
- c) 业务状态记录上报，包括活跃资源监测记录上报与查询的相关功能，基础数据异常监测记录上报与查询的相关功能；
- d) 信息安全记录上报，在现网环境下验证违法违规网站列表下发及监测处置记录上报，违法信息监测过滤指令下发与记录上报，规则优先级及指令可见性管理等相关功能；
- e) 访问日志查询与上报，验证现网环境下访问日志查询及响应的相关功能；
- f) 性能要求，在现网环境下验证规则容量、规则匹配准确率、数据更新上报时间、日志查询响应时间、数据错漏率、时钟同步等相关指标。

具体评测项目见 7.9 至 7.13。

7.2 基础数据管理

测试编号：1
测试项目：IRCS 业务主体信息本地添加测试
测试目的：验证 ISMS 系统添加 IRCS 主体信息的功能
测试环境：现网环境
测试步骤： <ul style="list-style-type: none"> 1) 确认评测环境； 2) 登录 ISMS 系统； 3) 添加 IRCS 主体信息（IRCS 业务经营许可证号、单位名称（应与许可证上登记信息一致）、单位地址及邮编、企业法人、网络信息安全责任人、应急联系人信息、IRCS 业务机房数量、以及各个 IRCS 业务机房相关信息。其中，IRCS 业务机房相关信息包括各个 IRCS 业务机房的名称、编号、IRCS 业务机房所处机房的性质、IRCS 业务机房所在地、地址及邮编、IRCS 业务机房驻地网络信息安全责任人信息）并查询添加结果
预期结果： <ul style="list-style-type: none"> 1) 在步骤（2）中，成功登录 ISMS 系统； 2) 步骤（3）中，成功添加 IRCS 主体信息
判定原则： <p>应符合预期结果要求，否则为不合格</p>

测试编号：2
测试项目：IRCS 业务资源信息本地添加测试
测试目的：验证 ISMS 系统添加 IRCS 业务资源信息的功能
测试环境：现网环境
测试步骤： <ul style="list-style-type: none"> 1) 确认评测环境； 2) 登录 ISMS 系统； 3) 添加 IRCS 的 IP 段信息（IP 段编号、起始 IP 地址、终止 IP 地址、来源、分配单位、分配使用时间、使用单位信

<p>息、IP 地址使用方式（静态/动态）），并查询添加结果；</p> <p>4) 添加 IRCS 业务机房机架信息（可选），包括（机架/机位编号、所在 IRCS 业务机房编号、分配状态（未分配/已分配）、占用状态（未占用/已占用）），并查询添加结果；</p> <p>5) 添加 IRCS 的链路信息（互联网出入口链路编号、网关 IP 地址、链路带宽、链路类型、链路接入单位信息、互联网接入地），并查询添加结果；</p> <p>6) 添加 IRCS 的公共域名信息（域名地址、用户自定义域名级别），并查询添加结果</p>
<p>预期结果：</p> <p>1) 在步骤（2）中，成功登录 ISMS 系统；</p> <p>2) 在步骤（4）中，成功添加 IRCS 的 IP 段信息；</p> <p>3) 在步骤（5）中，成功添加 IRCS 业务机房机架信息；</p> <p>4) 在步骤（6）中，成功添加 IRCS 的链路信息；</p> <p>5) 在步骤（7）中，成功添加 IRCS 的公共域名信息</p>
<p>判定原则：</p> <p>应符合预期结果要求，否则为不合格</p>

测试编号：3
测试项目：IRCS 业务用户信息本地添加测试
测试目的：验证 ISMS 系统添加 IRCS 业务用户信息的功能
测试环境：现网环境
<p>测试步骤：</p> <p>1) 确认评测环境；</p> <p>2) 登录 ISMS 系统；</p> <p>3) 添加业务用户信息（用户编号、用户属性（分为提供应用服务、其他等类）、用户单位名称（或姓名）、用户单位地址及邮编、用户单位属性、证件类型、证件号码、网络信息安全责任人信息、服务开通时间），并查询添加结果；</p> <p>4) 添加提供内部应用的应用服务用户信息（应用服务类型、接入方式（见技术要求附录 A.4）、域名信息列表（提供支持域名指向的应用服务如：HTTP、FTP、SMTP、POP3 等需提供本级域名）），并查询添加结果；</p> <p>5) 添加提供电信业务的应用服务用户信息（应用服务类型、业务许可证号、接入方式、预登记的服务内容（可多选）、域名信息列表（提供支持域名指向的应用服务如：HTTP、FTP、SMTP、POP3 等需提供本级域名）），并查询添加结果；</p> <p>6) 添加提供互联网服务的应用服务用户信息（应用服务类型、备案号、接入方式、预登记的服务内容（可多选）、域名信息列表（提供支持域名指向的应用服务如：HTTP、FTP、SMTP、POP3 等需提供本级域名）），并查询添加结果</p>
<p>预期结果：</p> <p>1) 在步骤（2）中，成功登录 ISMS 系统；</p> <p>2) 在步骤（3）中，成功添加业务用户信息；</p> <p>3) 在步骤（4）中，成功添加提供内部应用的应用服务用户信息；</p> <p>4) 在步骤（5）中，成功添加提供电信业务的应用服务用户信息；</p> <p>5) 在步骤（6）中，成功添加提供互联网服务的应用服务用户信息</p>
<p>判定原则：</p> <p>应符合预期结果要求，否则为不合格</p>

测试编号：4
测试项目：IRCS 业务主体信息本地修改测试
测试目的：验证 ISMS 系统修改 IRCS 业务主体信息的功能
测试环境：现网环境
测试步骤： <ol style="list-style-type: none"> 1) 确认评测环境； 2) 登录 ISMS 系统； 3) 修改 IRCS 业务主体信息（IRCS 业务经营许可证号、单位名称（应与许可证上登记信息一致）、单位地址及邮编、企业法人、网络信息安全责任人、应急联系人信息、IRCS 业务机房数量、以及各个 IRCS 业务机房相关信息。其中，IRCS 业务机房相关信息包括各个 IRCS 业务机房的名称、编号、IRCS 业务机房所处机房的性质、IRCS 业务机房所在地、地址及邮编、IRCS 业务机房驻地网络信息安全责任人信息）并查询修改结果
预期结果： <ol style="list-style-type: none"> 1) 在步骤（2）中，成功登录 ISMS 系统； 2) 在步骤（3）中，成功修改 IRCS 业务主体信息。 在步骤（3）中，成功修改 IRCS 业务主体的业务机房信息
判定原则： <p>应符合预期结果要求，否则为不合格</p>

测试编号：5
测试项目：IRCS 业务资源信息本地修改测试
测试目的：验证 ISMS 系统修改 IRCS 业务资源数据的功能
测试环境：现网环境
测试步骤： <ol style="list-style-type: none"> 1) 确认评测环境； 2) 登录 ISMS 系统； 3) 修改 IRCS 的 IP 段信息（IP 段编号、起始 IP 地址、终止 IP 地址、来源、分配单位、分配使用时间、使用单位信息、IP 地址使用方式（静态/动态）），并查询修改结果； 4) 修改 IRCS 业务机房机架信息（可选），包括（机架/机位编号、所在 IRCS 业务机房编号、分配状态（未分配/已分配）、占用状态（未占用/已占用）），并查询修改结果； 5) 修改 IRCS 的链路信息（互联网出入口链路编号、网关 IP 地址、链路带宽、链路类型、链路接入单位信息、互联网接入地），并查询修改结果。 6) 修改 IRCS 的公共域名信息（域名地址、用户自定义域名级别），并查询修改结果
预期结果： <ol style="list-style-type: none"> 1) 在步骤（2）中，成功登录 ISMS 系统； 2) 在步骤（4）中，成功修改 IRCS 的 IP 段信息； 3) 在步骤（5）中，成功修改 IRCS 业务机房机架信息； 4) 在步骤（6）中，成功修改 IRCS 的链路信息； 5) 在步骤（7）中，成功修改 IRCS 的公共域名信息
判定原则： <p>应符合预期结果要求，否则为不合格</p>

测试编号：6
测试项目：IRCS 业务用户信息本地修改测试
测试目的：验证 ISMS 系统修改 IRCS 业务用户信息的功能
测试环境：现网环境
测试步骤： <ol style="list-style-type: none"> 1) 确认评测环境； 2) 登录 ISMS 系统； 3) 修改业务用户信息（用户编号、用户属性（分为提供应用服务、其他等类）、用户单位名称（或姓名）、用户单位地址及邮编、用户单位属性、证件类型、证件号码、网络信息安全责任人信息、服务开通时间），并查询修改结果； 4) 修改提供内部应用的应用服务用户信息（应用服务类型、接入方式（见附录 A.4）、域名信息列表（提供支持域名指向的应用服务如：HTTP、FTP、SMTP、POP3 等需提供本级域名）），并查询修改结果； 5) 修改提供电信业务的应用服务用户信息（应用服务类型、业务许可证号、接入方式、预登记的服务内容（可多选）、域名信息列表（提供支持域名指向的应用服务如：HTTP、FTP、SMTP、POP3 等需提供本级域名）），并查询修改结果； 6) 修改提供互联网服务的应用服务用户信息（应用服务类型、备案号、接入方式、预登记的服务内容（可多选）、域名信息列表（提供支持域名指向的应用服务如：HTTP、FTP、SMTP、POP3 等需提供本级域名）），并查询修改结果
预期结果： <ol style="list-style-type: none"> 1) 在步骤（2）中，成功登录 ISMS 系统； 2) 在步骤（3）中，成功修改业务用户信息； 3) 在步骤（4）中，成功修改提供内部应用的应用服务用户信息； 4) 在步骤（5）中，成功修改提供电信业务的应用服务用户信息； 5) 在步骤（6）中，成功修改提供互联网服务的应用服务用户信息
判定原则： <p>应符合预期结果要求，否则为不合格</p>

测试编号：7
测试项目：IRCS 业务主体信息本地删除测试
测试目的：验证 ISMS 系统删除 IRCS 业务主体信息的功能
测试环境：现网环境
测试步骤： <ol style="list-style-type: none"> 1) 确认评测环境； 2) 登录 ISMS 系统； 3) 删除 IRCS 业务主体信息（IRCS 业务经营许可证号、单位名称（应与许可证上登记信息一致）、单位地址及邮编、企业法人、网络信息安全责任人、应急联系人信息、IRCS 业务机房数量、以及各个 IRCS 业务机房相关信息。其中，IRCS 业务机房相关信息包括各个 IRCS 业务机房的名称、编号、IRCS 业务机房所处机房的性质、IRCS 业务机房所在地、地址及邮编、IRCS 业务机房驻地网络信息安全责任人信息）并查询删除结果
预期结果： <ol style="list-style-type: none"> 1) 在步骤（2）中，成功登录 ISMS 系统； 2) 在步骤（3）中，成功删除 IRCS 业务主体信息； 3) 在步骤（3）中，成功删除 IRCS 业务主体信息下的业务节点相关信息
判定原则：

应符合预期结果要求，否则为不合格

测试编号：8
测试项目：IRCS 业务资源信息本地删除测试
测试目的：验证 ISMS 系统删除 IRCS 业务资源信息的功能
测试环境：现网环境
测试步骤： <ol style="list-style-type: none"> 1) 确认评测环境； 2) 登录 ISMS 系统； 3) 删除 IRCS 的 IP 段信息（IP 段编号、起始 IP 地址、终止 IP 地址、来源、分配单位、分配使用时间、使用单位信息、IP 地址使用方式（静态/动态）），并查询删除结果； 4) 删除 IRCS 业务机房下的机架信息（可选），包括（机架/机位编号、所在 IRCS 业务机房编号、分配状态（未分配/已分配）、占用状态（未占用/已占用）），并查询删除结果； 5) 删除 IRCS 的链路信息（互联网出入口链路编号、网关 IP 地址、链路带宽、链路类型、链路接入单位信息、互联网接入地），并查询删除结果； 6) 删除 IRCS 公共域名信息（域名地址、用户自定义域名级别），并查询删除结果
预期结果： <ol style="list-style-type: none"> 1) 在步骤（2）中，成功登录 ISMS 系统； 2) 在步骤（3）中，成功删除 IRCS 业务资源信息； 3) 在步骤（4）中，成功删除 IRCS 的 IP 段信息； 4) 在步骤（5）中，成功删除 IRCS 业务机房机架信息； 5) 在步骤（6）中，成功删除 IRCS 链路信息； 6) 在步骤（7）中，成功删除 IRCS 公共域名信息
判定原则： <p>应符合预期结果要求，否则为不合格</p>

测试编号：9
测试项目：IRCS 业务用户信息本地删除测试
测试目的：验证 ISMS 系统删除 IRCS 业务用户信息的功能
测试环境：现网环境
测试步骤： <ol style="list-style-type: none"> 1) 确认评测环境； 2) 登录 ISMS 系统； 3) 删除业务用户信息（用户编号、用户属性（分为提供应用服务、其他等类）、用户单位名称（或姓名）、用户单位地址及邮编、用户单位属性、证件类型、证件号码、网络信息安全责任人信息、服务开通时间），并查询删除结果； 4) 删除提供内部应用的应用服务用户信息（应用服务类型、接入方式（见附录 A.4）、域名信息列表（提供支持域名指向的应用服务如：HTTP、FTP、SMTP、POP3 等需提供本级域名）），并查询修改结果，并查询删除结果； 5) 删除提供电信业务的应用服务用户信息（应用服务类型、业务许可证号、接入方式、预登记的服务内容（可多选）、域名信息列表（提供支持域名指向的应用服务如：HTTP、FTP、SMTP、POP3 等需提供本级域名）），并查询删除结果； 6) 删除提供互联网服务的应用服务用户信息（应用服务类型、备案号、接入方式、预登记的服务内容（可多选）、

域名信息列表（提供支持域名指向的应用服务如：HTTP、FTP、SMTP、POP3 等需提供本级域名）），并查询删除结果

预期结果：

- 1) 在步骤（2）中，成功登录 ISMS 系统；
- 2) 在步骤（3）中，成功删除业务用户信息；
- 3) 在步骤（4）中，成功删除提供内部应用的应用服务用户信息；
- 4) 在步骤（5）中，成功删除提供电信业务的应用服务用户信息；
- 5) 在步骤（6）中，成功删除提供互联网服务的应用服务用户信息

判定原则：

应符合预期结果要求，否则为不合格

测试编号：10

测试项目：基础数据本地导入测试

测试目的：验证 IRCS 基础数据本地导入的功能

测试环境：现网环境

测试步骤：

- 1) 确认评测环境；
- 2) 登录 ISMS 系统；
- 3) 将基础数据信息按照相应格式填写到导入模板（XML 或 XLS 等常见数据格式）中，包括 IRCS 经营单位信息、业务客户数据、业务资源数据；
- 4) 将填写好的模板导入到 ISMS 系统中，并查询导入结果

预期结果：

- 1) 在步骤（2）中，成功登录 ISMS 系统；
- 2) 在步骤（3）中，尝试在模板中填写正确的基础数据信息；
- 3) 在步骤（4）中，将填有正确基础数据信息的文件导入 ISMS 系统，系统对导入基础数据信息校验无误，系统功能正常；
- 4) 重复步骤（3），尝试在模板中填写有误（格式有误或与既有数据产生冲突）的基础数据信息；
- 5) 在步骤（4）中，将上述文件导入 ISMS 系统，系统导入基础数据信息失败，系统功能正常；将提示有误的基础数据信息文件更正后，重新导入，系统对导入基础数据信息校验无误，系统功能正常

判定原则：

应符合预期结果要求，否则为不合格

7.3 动态资源管理

测试编号：11

测试项目：IRCS 动态资源使用日志记录功能

测试目的：验证 ISMS 系统记录使用 IRCS 动态资源的记录功能

测试环境：现网环境

测试步骤：

- 1) 确认评测环境；
- 2) 用户通过公网终端申请使用 IRCS 动态网络资源的虚拟资源或申请使用网络资源（IP 地址）；

3) 申请成功后 2 个小时内，登录 ISMS 系统，查看申请 IRCS 动态资源日志记录情况； 4) 用户在用户操作控制台删除新申请的虚拟资源或网络资源； 5) 删除成功后 2 个小时内，登录 ISMS 系统，查看 IRCS 动态资源日志记录情况
<p>预期结果：</p> <p>1) 在步骤（3）中，可以看到该用户的动态资源使用日志中多了一条用户可用资源变更时间为新申请资源生成时间的记录；</p> <p>2) 在步骤（5）中，可以看到该用户的动态资源使用日志中多了一条用户可用资源变更时间为资源删除时间的记录</p>
<p>判定原则：</p> <p>应符合预期结果要求，否则为不合格</p>

测试编号：12
测试项目：IRCS 动态资源使用日志记录内容
测试目的：验证 ISMS 系统记录 IRCS 动态资源的日志内容
测试环境：现网环境
<p>测试步骤：</p> <p>1) 确认评测环境；</p> <p>2) 用户通过公网终端申请使用 IRCS 动态网络资源的虚拟资源或申请使用网络资源（IP 地址）；</p> <p>3) 申请成功后 2 个小时内，登录 ISMS 系统，查看申请 IRCS 动态资源日志记录情况；</p> <p>4) 用户在用户操作控制台删除新申请的虚拟资源或网络资源；</p> <p>5) 删除成功后 2 个小时内，登录 ISMS 系统，查看 IRCS 动态资源日志记录情况</p>
<p>预期结果：</p> <p>1) 在步骤（2）前先查看用户最新的动态资源使用日志，记录内容包含用户编号，用户可用资源变更时间（精确到秒），对应时间用户提供应用服务的域名列表，用户拥有的公网 IP 地址列表及公网 IP 地址资源对应的虚拟资源编号、虚拟资源类型；</p> <p>2) 在步骤（3）中，可以查看到用户最新的资源快照中除包含（6）中的资源外，还包含了此次新申请的资源数据；</p> <p>3) 在步骤（5）中，可以查看到用户最新的动态资源使用日志中不包含（4）中删除的资源数据</p>
<p>判定原则：</p> <p>应符合预期结果要求，否则为不合格</p>

测试编号：13
测试项目：动态资源使用日志本地查询方式测试
测试目的：验证 ISMS 系统按照条件查询动态资源使用日志的功能
测试环境：现网环境
<p>测试步骤：</p> <p>1) 确认评测环境；</p> <p>2) 通过公网终端申请使用 IRCS 的虚拟资源、网络资源（IP 地址和域名），形成动态资源使用日志；</p> <p>3) 登录 ISMS，通过单个用户编号及查询时间段对使用日志进行查询；</p> <p>4) 登录 ISMS，通过单个公网 IP 地址及查询时间段对使用日志进行查询；</p> <p>5) 登录 ISMS，通过单个域名及查询时间段对使用日志进行查询</p>
预期结果：

<p>1) 在步骤(3)中,可在查询指令下发 10 分钟内查询到用户编号在查询时间段内所有可用的域名信息列表、公网 IP 信息列表,查询内容包含用户编号、用户查询时间段内所有可用的域名信息列表、用户拥有的公网 IP 地址列表及公网 IP 地址资源对应的虚拟资源编号、虚拟资源类型;</p> <p>2) 在步骤(4)中,可在查询指令下发 10 分钟内查询到该公网 IP 地址在查询时间段内所属的用户及对应的虚拟资源信息,查询内容包含用户编号、查询 IP 地址对应的虚拟资源编号、虚拟资源类型;</p> <p>3) 在步骤(5)中,可在查询指令下发 10 分钟内查询到该域名在查询时间段内所属的用户信息,查询内容包含用户编号</p>
<p>判定原则:</p> <p>应符合预期结果要求,否则为不合格</p>
<p>备注:</p> <p>1) 用户的域名网络资源数据,由于需要备案,需要评测前准备;</p> <p>2) 查询时间段不超过 30 天</p>

7.4 业务状态管理

测试编号: 14
测试项目: 活跃状态监测功能测试
测试目的: 验证 ISMS 系统活跃状态监测功能
测试环境: 现网环境
<p>测试步骤:</p> <p>1) 确认评测环境;</p> <p>2) 登录 ISMS 系统;</p> <p>3) 通过公网终端访问 IRCS 业务节点内特定 IP+端口(或 IP+端口列表)、特定域名(或特定域名列表);</p> <p>4) 登录 ISMS 系统,查看活跃状态监测记录</p>
<p>预期结果:</p> <p>在步骤(4)中,可成功记录公网终端对系统覆盖范围内活跃状态(IP、域名)的活跃度</p>
<p>判定原则:</p> <p>应符合预期结果要求,否则为不合格</p>

测试编号: 15
测试项目: 活跃状态监测记录内容测试
测试目的: 验证 ISMS 活跃状态监测记录内容
测试环境: 现网环境
<p>测试步骤:</p> <p>1) 确认评测环境;</p> <p>2) 登录 ISMS 系统;</p> <p>3) 通过公网终端访问 IRCS 业务节点内特定 IP+端口(或 IP+端口列表)、特定域名(或特定域名列表),形成活跃资源监测记录;</p> <p>4) 登录 ISMS 系统,查看活跃状态监测记录内容</p>
预期结果:

在步骤（4）中，成功显示活跃状态监测记录，对于活跃域名监测记录应包括发现的活跃域名、关联 IP、首次访问时间（当日）、最后访问时间（实时）、24 小时累计活跃度；对于活跃 IP 及应用端口监测记录应包括发现的活跃 IP、应用端口、传输层协议类型（TCP/UDP）、首次访问时间（当日）、最后访问时间（实时）、24 小时累计活跃度
判定原则： 应符合预期结果要求，否则为不合格
备注： IP/域名活跃资源列表应当能按照 24 小时累计活跃度进行排序，以体现活跃程度

测试编号：16
测试项目：异常状态监测功能测试
测试目的：验证 ISMS 系统对异常状态监测发现功能
测试环境：现网环境
测试步骤： 1) 确认评测环境； 2) 登录 ISMS 系统，确认开启异常状态监测发现功能； 3) 访问使用未报备 IP 地址接入的站点，查看监测信息； 4) 访问已报备且登记使用方式为保留的 IP 地址接入的站点，查看监测信息
预期结果： 1) 在步骤（2）中，IP 地址异常发现功能正常； 2) 在步骤（3）中，成功实时发现未报备 IP 地址接入情况； 3) 在步骤（4）中，成功实时发现已报备的，且登记使用方式为保留实际为启用的 IP 地址接入
判定原则： 应符合预期结果要求，否则为不合格

测试编号：17
测试项目：异常状态监测记录内容测试
测试目的：验证 ISMS 系统对异常状态的监测信息记录功能
测试环境：现网环境
测试步骤： 1) 确认评测环境； 2) 登录 ISMS 系统，确认开启异常状态监测发现功能； 3) 访问未报备 IP 地址接入的站点、已报备且登记使用方式为保留的 IP 地址接入的站点； 4) 在 ISMS 查询异常状态信息的监测结果，并验证内容正确性和完整性（记录内容至少包括异常 IP 地址、登记使用方式和实际使用方式、异常类型、实际域名（仅适用于支持域名指向的应用服务）、首次发现时间、最近发现时间、当前状态（已处置或未处置））； 5) 对监测到的异常基础数据进行处置，然后通过公网终端访问，再次查看基础数据异常监测记录
预期结果： 1) 在步骤（2）中，成功登录 ISMS 系统； 2) 在步骤（4）中，成功查询到本地的异常状态记录，且内容正确、完整（不支持域名指向的应用可不记录实际域名）；

3) 在步骤（5）中，已处置的 IP 或域名无法访问，且本地异常监测记录中生成新的记录，处置状态发生变化
判定原则： 应符合预期结果要求，否则为不合格

7.5 信息安全管理

测试编号：18
测试项目：违法违规网站监测功能测试
测试目的：验证 ISMS 系统违法违规网站发现功能
测试环境：现网环境
测试步骤： 1) 确认评测环境； 2) 登录 ISMS 系统； 3) 访问属于违法网站列表中的违法网站； 4) 访问属于未备案状态的网站（无备案记录的网站）； 5) 查看系统对违法违规网站发现监测结果
预期结果： 1) 在步骤（3）、步骤（4）中，可成功记录公网终端对系统覆盖范围内违法违规网站的访问； 2) 在步骤（5）中，可成功查看违法违规网站监测记录
判定原则： 应符合预期结果要求，否则为不合格
备注： 1) 如果 ISMS 系统操作界面可选择对违法违规网站进行仅监测不处置的操作，则监测记录中处置状态可为未处置； 2) 如果在此基础上进行手动处置，则处置后本地违法违规网站监测记录中生成新的记录，处置状态发生变化

测试编号：19
测试项目：违法违规网站监测记录内容测试
测试目的：验证 ISMS 系统违法违规网站监测记录功能
测试环境：现网环境
测试步骤： 1) 确认评测环境； 2) 登录 ISMS 系统，查看系统对违法违规网站发现监测结果
预期结果： 在步骤（2）中，违法违规网站监测记录完整、准确（至少记录违法违规网站的域名、IP、服务内容、违法违规情况、24 小时累计访问量、记录时间（实时的最后访问时间）、当前状态（未处置或已处置）、处置人帐号等）
判定原则： 应符合预期结果要求，否则为不合格
备注： 1) 如果 ISMS 系统操作界面可选择对违法违规网站进行仅监测不处置的操作，则监测记录中处置状态可为未处置； 2) 如果在此基础上进行手动处置，则处置后本地违法违规网站监测记录中生成新的记录，处置状态发生变化

测试编号：20
测试项目：违法违规网站处置功能测试
测试目的：验证 ISMS 系统对发现的违法违规网站处置的功能
测试环境：现网环境
测试步骤： <ol style="list-style-type: none"> 1) 确认评测环境； 2) 登录 ISMS 系统； 3) 访问属于违法网站列表中的违法网站； 4) 访问属于未备案状态的网站（无备案记录的网站）； 5) 查看系统对违法违规网站处置记录信息
预期结果： <ol style="list-style-type: none"> 1) 在步骤（3）、步骤（4）中，无法访问违法违规网站，其他访问不受影响； 2) 在步骤（5）中，可成功登录系统，成功对违法违规网站处置情况进行记录
判定原则： <p>应符合预期结果要求，否则为不合格</p>

测试编号：21
测试项目：违法违规网站处置记录内容测试
测试目的：验证 ISMS 系统对发现的违法违规网站处置的功能
测试环境：现网环境
测试步骤： <ol style="list-style-type: none"> 1) 确认评测环境； 2) 登录 ISMS 系统，查看系统对违法违规网站处置记录信息
预期结果： <p>在步骤（2）中，违法违规网站处置记录完整、准确（至少记录违法违规网站的域名、IP、服务内容、违法违规情况、24 小时累计访问量、记录时间（最后访问时间）、当前状态（已处置）、处置人账号等）</p>
判定原则： <p>应符合预期结果要求，否则为不合格</p>

测试编号：22
测试项目：违法网站列表管理功能测试
测试目的：验证 ISMS 系统对违法违规网站列表的管理功能
测试环境：现网环境
测试步骤： <ol style="list-style-type: none"> 1) 确认评测环境，登录 ISMS 系统； 2) 打开违法网站列表，对列表内网站进行添加、删除操作； 3) 通过公网终端对违法网站列表内进行过上述操作的网站进行访问验证； 4) 打开免过滤网站列表，对列表内网站进行添加、删除操作；

5) 通过公网终端对免过滤网站列表内进行过上述操作的网站进行访问
<p>预期结果：</p> <ol style="list-style-type: none"> 1) 在步骤（2）中，可成功对违法网站列表进行添加、删除操作； 2) 在步骤（3）中，无法访问存在于违法网站列表中的网站，可成功查看违法网站监测/处置记录； 3) 在步骤（4）中，可成功对免过滤网站列表进行添加、删除操作； 4) 在步骤（5）中，无法访问同时存在于违法网站列表和免过滤网站列表中的网站，可成功查看违法违规网站监测/处置记录；可以正常访问仅在免过滤网站列表中的网站
<p>判定原则：</p> <p>应符合预期结果要求，否则为不合格</p>

测试编号：23
测试项目：违法信息监测发现功能测试（IP+端口）
测试目的：验证 ISMS 系统对数据流中的违法信息发现监测功能
测试环境：现网环境
<p>测试步骤：</p> <ol style="list-style-type: none"> 1) 确认评测环境； 2) 登录 ISMS 系统，创建并下发基于 IP 地址+端口的监测规则； 3) 通过公网终端访问 IRCS 业务节点内应用资源（客户站点或测试参考站），触发特定 IP 地址+特定传输层协议（TCP/UDP）端口的监测行为； 4) 查看系统对违法信息监测记录的信息
<p>预期结果：</p> <ol style="list-style-type: none"> 1) 在步骤（2）中，监测规则正常下发； 2) 在步骤（3）中，可访问符合违法信息监测规则的资源； 3) 在步骤（4）中，系统正常记录监测到的访问行为（使用特定源/目的 IP、源/目的端口的数据包或会话）
<p>判定原则：</p> <p>应符合预期结果要求，否则为不合格</p>

测试编号：24
测试项目：违法信息监测发现功能测试（域名）
测试目的：验证 ISMS 系统对数据流中的违法信息发现监测功能
测试环境：现网环境
<p>测试步骤：</p> <ol style="list-style-type: none"> 1) 确认评测环境； 2) 登录 ISMS 系统，创建并下发基于域名的监测规则； 3) 通过公网终端访问 IRCS 业务节点内应用资源（客户站点或测试参考站），触发特定域名的监测行为； 4) 查看系统对违法信息监测记录的信息
<p>预期结果：</p> <ol style="list-style-type: none"> 1) 在步骤（2）中，监测规则正常下发； 2) 在步骤（3）中，可访问符合违法信息监测规则的资源；

3) 在步骤(4)中, 系统正常记录监测到的访问行为(使用特定域名的应用)
判定原则: 应符合预期结果要求, 否则为不合格

测试编号: 25
测试项目: 违法信息监测发现功能测试(URL)
测试目的: 验证 ISMS 系统对数据流中的违法信息发现监测功能
测试环境: 现网环境
测试步骤: 1) 确认评测环境; 2) 登录 ISMS 系统, 创建并下发基于 URL 字符串的监测规则; 3) 通过公网终端访问 IRCS 业务节点内应用资源(客户站点或测试参考站), 触发特定 URL 的监测行为; 4) 查看系统对违法信息监测记录的信息
预期结果: 1) 在步骤(2)中, 监测规则正常下发; 2) 在步骤(3)中, 可访问符合违法信息监测规则的资源; 3) 在步骤(4)中, 系统正常记录监测到的访问行为(使用包含特定字符串的 URL 所指向的资源)
判定原则: 应符合预期结果要求, 否则为不合格

测试编号: 26
测试项目: 违法信息监测发现功能测试(关键词)
测试目的: 验证 ISMS 系统对数据流中的违法信息发现监测功能
测试环境: 现网环境
测试步骤: 1) 确认评测环境; 2) 登录 ISMS 系统, 创建并下发基于关键词的监测规则; 3) 通过公网终端访问 IRCS 业务节点内应用资源(客户站点或测试参考站), 触发特定关键词监测行为; 4) 查看系统对违法信息监测记录的信息
预期结果: 1) 在步骤(2)中, 监测规则正常下发; 2) 在步骤(3)中, 可访问符合违法信息监测规则的资源; 3) 在步骤(4)中, 系统正常记录监测到的访问行为(页面标题和正文中含有特定明文关键词的 WEB 页面)
判定原则: 应符合预期结果要求, 否则为不合格

测试编号: 27
测试项目: 违法信息监测记录内容测试

测试目的：验证 ISMS 系统的违法信息监测记录的内容
测试环境：现网环境
测试步骤： 1) 确认评测环境； 2) 登录 ISMS 系统，查询违法信息监测日志的内容
预期结果： 1) 在步骤（2）中，成功查询违法信息监测日志，内容正确、完整，监测记录至少包括源/目的 IP，源/目的端口、违法信息、首次触发时间、最近触发时间、触发指令次数以及触发的指令标识，对浏览类应用还需记录 URL； 2) 对于页面标题或正文含有违法信息监测规则指定关键词的页面，ISMS 应在当日的首次监测记录保存相应页面的纯文本页面快照（页面缓存）
判定原则： 应符合预期结果要求，否则为不合格

测试编号：28
测试项目：违法信息过滤功能测试（IP+端口）
测试目的：验证 ISMS 系统对数据流中的违法信息过滤处置功能
测试环境：现网环境
测试步骤： 1) 确认评测环境； 2) 登录 ISMS 系统，创建并下发基于 IP 地址的过滤规则； 3) 通过公网终端访问 IRCS 业务节点内应用资源（客户站点或测试参考站），触发特定 IP 地址+特定传输层协议（TCP/UDP）端口的过滤行为； 4) 查看系统对违法信息过滤记录的信息
预期结果： 1) 在步骤（2）中，过滤规则正常下发； 2) 在步骤（3）中，无法访问符合违法信息过滤规则的资源，其他访问不受影响； 3) 在步骤（4）中，系统正常记录过滤处置的访问行为（使用特定源/目的 IP、源/目的端口的数据包或会话）
判定原则： 应符合预期结果要求，否则为不合格

测试编号：29
测试项目：违法信息过滤功能测试（域名）
测试目的：验证 ISMS 系统对数据流中的违法信息过滤处置功能
测试环境：现网环境
测试步骤： 1) 确认评测环境； 2) 登录 ISMS 系统，创建并下发基于域名的过滤规则； 3) 通过公网终端访问 IRCS 业务节点内应用资源（客户站点或测试参考站），触发特定域名的过滤行为（TCP+UDP）； 4) 查看系统对违法信息过滤记录的信息

预期结果：
1) 在步骤（2）中，过滤规则正常下发； 2) 在步骤（3）中，无法访问符合违法信息过滤规则的资源，其他访问不受影响； 3) 在步骤（4）中，系统正常记录过滤处置的访问行为（使用特定域名的应用）
判定原则：
应符合预期结果要求，否则为不合格

测试编号：30
测试项目：违法信息过滤功能测试（URL）
测试目的：验证 ISMS 系统对数据流中的违法信息过滤处置功能
测试环境：现网环境
测试步骤： 1) 确认评测环境； 2) 登录 ISMS 系统，创建并下发基于 URL 字符串的过滤规则； 3) 通过公网终端访问 IRCS 业务节点内应用资源（客户站点或测试参考站），触发特定 URL 的过滤行为； 4) 查看系统对违法信息过滤记录的信息
预期结果：
1) 在步骤（2）中，过滤规则正常下发； 2) 在步骤（3）中，无法访问符合违法信息过滤规则的资源，其他访问不受影响； 3) 在步骤（4）中，系统正常记录过滤处置的访问行为（使用包含特定字符串的 URL 所指向的资源）
判定原则：
应符合预期结果要求，否则为不合格

测试编号：31
测试项目：违法信息过滤功能测试（关键词）
测试目的：验证 ISMS 系统对数据流中的违法信息过滤处置功能
测试环境：现网环境
测试步骤： 1) 确认评测环境； 2) 登录 ISMS 系统，创建并下发基于关键词的过滤规则； 3) 通过公网终端访问 IRCS 业务节点内应用资源（客户站点或测试参考站），触发特定关键词过滤行为； 4) 查看系统对违法信息过滤记录的信息
预期结果：
1) 在步骤（2）中，过滤规则正常下发； 2) 在步骤（3）中，无法访问符合违法信息过滤规则的资源，其他访问不受影响； 3) 在步骤（4）中，系统正常记录过滤处置的访问行为（页面标题和正文中含有特定明文关键词的 WEB 页面）
判定原则：
应符合预期结果要求，否则为不合格

测试编号：32
测试项目：违法信息过滤记录内容测试
测试目的：验证 ISMS 系统的违法信息过滤记录的内容
测试环境：现网环境
测试步骤： <ol style="list-style-type: none"> 1) 确认评测环境； 2) 登录 ISMS 系统，查询违法信息过滤日志的内容
预期结果： <ol style="list-style-type: none"> 1) 在步骤（2）中，成功查询违法信息过滤日志，内容正确、完整，过滤记录至少包括源/目的 IP，源/目的端口、违法信息（域名、URL）、首次触发时间、最近触发时间、触发指令次数以及触发的指令标识，（对于属于浏览类应用，留存内容包括 URL）； 2) 对于页面标题或正文含有违法信息过滤规则指定关键词的页面，ISMS 应在当日的首次过滤记录保存相应页面的纯文本页面快照（页面缓存）
判定原则： <p>应符合预期结果要求，否则为不合格</p>

测试编号：33
测试项目：规则优先级与冲突校验测试
测试目的：验证 ISMS 系统对规则优先级的冲突校验功能
测试环境：现网环境
测试步骤： <ol style="list-style-type: none"> 1) 确认评测环境，登录 ISMS 系统； 2) ISMS 创建并下发基于域名的违法信息过滤指令； 3) 通过公网终端进行访问验证； 4) 基于违法信息过滤指令，ISMS 下发免过滤网站指令； 5) 通过公网终端进行访问验证； 6) 基于免过滤网站指令，ISMS 下发违法网站指令； 7) 通过公网终端进行访问验证； 8) ISMS 删除违法网站指令； 9) 通过公网终端访问验证； 10) ISMS 删除免过滤网站指令； 11) 通过公网终端验证； 12) ISMS 删除违法信息过滤指令； 13) 通过公网终端验证
预期结果： <ol style="list-style-type: none"> 1) 在步骤（3）（11）中，无法正常访问存在于过滤规则中的网站；可以正常访问不存在于过滤规则中的网站； 2) 在步骤（4）（9）中，可以正常访问同时存在于免过滤网站列表和违法信息过滤规则中的网站；无法访问仅存在于违法信息过滤规则中的网站； 3) 在步骤（7）中，无法正常访问同时存在于违法网站列表、免过滤网站列表和违法信息过滤规则中的网站；

4) 在步骤(13)中, 规则都删除之后, 网站可以正常访问
判定原则: 应符合预期结果要求, 否则为不合格
备注: 1) 如果 ISMS 系统实现了规则冲突提醒功能并阻止冲突规则下发, 核实规则之间的逻辑后则对此项不作要求; 2) 测试方法不仅限于测试步骤中的举例, 可以从更多方面的角度验证规则优先级与冲突校验

7.6 访问日志管理

测试编号: 34
测试项目: 访问日志记录功能测试
测试目的: 验证 ISMS 系统记录访问日志的功能
测试环境: 现网环境
测试步骤: 1) 确认评测环境; 2) 通过公网终端访问 IRCS 业务节点内支持 TCP 协议的应用资源 (客户站点或测试参考站); 3) 通过公网终端访问 IRCS 业务节点内支持 UDP 协议的应用资源 (客户站点或测试参考站); 4) 登录 ISMS 系统, 查看访问日志记录情况
预期结果: 在步骤(4)中, ISMS 正常实现访问日志记录功能。对于可通过传输层协议或应用层协议头信息区分会话特征的数据流量, ISMS 应以会话为单位记录访问日志; 对于无法通过传输层协议或应用层协议报文头内容区分会话特征的数据流量, ISMS 应以数据流 (源 IP、目的 IP、源端口、目的端口均相同, 速率大于 1 帧/s 且持续时间大于 10s 的数据流量) 为单位记录访问日志
判定原则: 应符合预期结果要求, 否则为不合格

测试编号: 35
测试项目: 访问日志记录内容测试
测试目的: 验证 ISMS 系统访问日志记录内容
测试环境: 现网环境
测试步骤: 1) 确认评测环境; 2) 通过公网终端访问 IRCS 业务节点内支持 TCP 协议的应用资源 (客户站点或测试参考站), 形成访问日志; 3) 通过公网终端访问 IRCS 业务节点内支持 UDP 协议的应用资源 (客户站点或测试参考站), 形成访问日志; 4) 登录 ISMS 系统, 查看访问日志记录内容
预期结果: 在步骤(4)中, 访问日志内容至少包括源 IP、目的 IP、源端口、目的端口、访问时间 (起始时间, 精确到秒), 属于浏览类协议的访问需留存 URL (对于采用加密方式的会话, 至少记录源 IP、目的 IP、源端口、目的端口、访问时间 (起始时间, 精确到秒)); 对于无法通过传输层协议或应用层协议报文头内容区分会话特征的数据流量, 至少记录源 IP、目的 IP、源端口、目的端口、访问时间 (起始时间, 精确到秒)、持续时长 (精确到秒))

判定原则：

应符合预期结果要求，否则为不合格

测试编号：36

测试项目：访问日志本地查询方式测试

测试目的：验证 ISMS 系统按照条件查询访问日志的功能

测试环境：现网环境

测试步骤：

- 1) 确认评测环境；
- 2) 通过公网终端访问 IRCS 业务节点内应用资源（客户站点或测试参考站），形成访问日志；
- 3) 登录 ISMS，通过源 IP 地址、源端口、查询时间对访问日志进行查询；
- 4) 登录 ISMS，通过目的 IP 地址、目的端口、查询时间对访问日志进行查询；
- 5) 登录 ISMS，通过源 IP 地址、查询时间对访问日志进行查询（可选）；
- 6) 对于浏览类访问日志，应支持通过用户访问 URL、查询时间的组合条件查询本地访问日志

预期结果：

- 1) 在步骤（3）中，可查询和统计符合源 IP 地址、源端口、查询时间条件的全部日志记录信息；
- 2) 在步骤（4）中，可查询和统计符合目的 IP 地址、目的端口、查询时间条件的全部日志记录信息；
- 3) 在步骤（5）中，可查询和统计符合源 IP 地址、查询时间条件的全部日志记录信息（可选）；
- 4) 在步骤（6）中，对于浏览类访问日志，可查询和统计符合用户访问 URL、查询时间条件的全部日志记录信息

判定原则：

应符合预期结果要求，否则为不合格

7.7 系统功能管理

测试编号：37

测试项目：系统用户的身份认证测试

测试目的：验证 ISMS 系统用户的身份认证管理功能

测试环境：现网环境

测试步骤：

- 1) 确认评测环境；
- 2) 尝试以不同的身份（系统用户和非系统用户）登录 ISMS 系统

预期结果：

- 1) ISMS 系统正常对登录的系统用户进行身份认证；
- 2) 系统用户可按授权进行相关操作

判定原则：

应符合预期结果要求，否则为不合格

测试编号：38

测试项目：系统用户权限划分测试

测试目的：验证 ISMS 系统用户的权限划分功能

测试环境：现网环境
测试步骤： <ol style="list-style-type: none"> 1) 确认评测环境； 2) 以系统管理员身份登录 ISMS 系统； 3) 将 ISMS 系统中的多个功能操作分配给一个操作员； 4) 以操作员身份登录系统，对已分配权限的功能进行操作，尝试进行其他未授权的各类操作； 5) 将 ISMS 系统中的一个功能单元分配给多个操作员； 6) 分别以不同操作员身份登录系统，对已分配权限的功能进行操作，尝试进行其他未授权的各类操作
预期结果： <ol style="list-style-type: none"> 1) 在步骤（3）、步骤（5）中，权限分配成功； 2) 在步骤（4）、步骤（6）中，用户可按授权进行相关操作
判定原则： <p>应符合预期结果要求，否则为不合格</p>

测试编号：39
测试项目：系统操作日志记录功能测试
测试目的：验证 ISMS 系统操作日志记录功能
测试环境：现网环境
测试步骤： <ol style="list-style-type: none"> 1) 确认评测环境； 2) 以不同的身份登录 ISMS 系统，尝试进行各类操作
预期结果： <p>系统准确的记录全体用户的全部操作日志</p>
判定原则： <p>应符合预期结果要求，否则为不合格</p>

测试编号：40
测试项目：系统运行维护管理测试
测试目的：验证 ISMS 系统运行状态实时监控功能
测试环境：现网环境
测试步骤： <ol style="list-style-type: none"> 1) 确认评测环境； 2) 登录 ISMS 系统； 3) 对系统相关软件功能模块和组成设备等进行配置和管理； 4) 查看系统各软件模块、服务程序、组成设备的运行情况
预期结果： <ol style="list-style-type: none"> 1) 在步骤（2）中，成功登录 ISMS 系统； 2) 在步骤（3）中，成功进行系统维护和管理； 3) 在步骤（4）中，可实时查看系统运行状态

判定原则：

应符合预期结果要求，否则为不合格

7.8 性能要求

测试编号：41
测试项目：信息安全规则容量测试
测试目的：验证 ISMS 系统的规则容量
测试环境：现网环境
测试步骤： <ol style="list-style-type: none"> 1) 确认评测环境； 2) 登录 ISMS 系统，添加（或导入）违法信息监测（或处置）规则； 3) 通过公网终端访问 IRCS 业务节点内应用资源（客户站点或测试参考站），对规则有效性进行验证； 4) 查看违法信息监测（或处置）规则的执行结果
预期结果： <ol style="list-style-type: none"> 1) 步骤（2）中，规则下发正常； 2) 步骤（3）、步骤（4）中，规则执行正常； 3) ISMS 系统支持违法信息监测（或处置）规则不少于 5 万条，其中特定域名、特定 URL、特定关键词的规则至少各 1 万条
判定原则： <p>应符合预期结果要求，否则为不合格</p>
备注： <p>单个违法信息监测（或处置）指令最多携带 100 条规则，规则之间为逻辑“与”关系</p>

测试编号：42
测试项目：信息安全规则匹配准确率测试
测试目的：验证 ISMS 的规则匹配准确率
测试环境：现网环境
测试步骤： <ol style="list-style-type: none"> 1) 确认评测环境； 2) 登录 ISMS 系统，添加（或导入）至少有 5 万条生效的违法信息监测、过滤规则； 3) 在正常业务流量背景下，通过公网终端访问符合监测规则的应用资源（客户站点或测试参考站）至少 1 万次； 4) 计算违法信息监测规则匹配的准确率； 5) 在正常业务流量背景下，通过公网终端访问符合过滤规则的应用资源（客户站点或测试参考站）至少 1 万次； 6) 计算违法信息过滤规则匹配的准确率
预期结果： <ol style="list-style-type: none"> 1) 在步骤（2）中，生效的规则不少于 5 万条，其中特定域名、特定 URL、特定关键词的规则至少各 1 万条； 2) 在步骤（4）中，对于匹配监测规则的访问，准确比例不低于 95%、漏判和错判总比例不高于 5%； 3) 在步骤（6）中，对于匹配过滤规则的访问，准确比例不低于 95%、漏判和错判总比例不高于 5%
判定原则：

应符合预期结果要求，否则为不合格。
备注： 1) 准确比例=系统有效监测识别（或成功过滤）的访问量/实际匹配监测（或过滤）规则的访问总量×100%； 2) 漏判和错判总比例=（系统未有效监测识别（或未成功过滤）的访问量+系统监测识别（或过滤）的无关访问量）/实际匹配监测（或过滤）规则的访问总量×100%

测试编号：43
测试项目：信息安全记录查询响应时间测试
测试目的：验证 ISMS 的信息安全记录上报时间
测试环境：现网环境
测试步骤： 1) 确认评测环境； 2) 登录 ISMS 系统，确认违法违规网站监测（和处置）功能状态； 3) 访问属于违法网站列表中的违法网站、访问属于未备案状态的网站（无备案记录的网站）； 4) 查询系统本地违法违规网站监测（和处置）记录信息； 5) 登录 ISMS 系统，下发至少 5 万条违法信息监测（和过滤）规则； 6) 通过公网终端访问业务机房/业务节点内应用资源（客户站点或测试参考站）； 7) 查询系统本地违法信息监测（和处置）记录信息
预期结果： 1) 在步骤（2）中，系统违法违规网站监测（和处置）功能状态正常； 2) 在步骤（4）、步骤（7）中，本地违法违规网站监测（和处置）记录、本地违法信息监测（和处置）记录信息查询结果完整、正确，本地查询响应时间少于 10min
判定原则： 应符合预期结果要求，否则为不合格

测试编号：44
测试项目：基础数据更新时间测试
测试目的：验证 ISMS 基础数据更新后的时间
测试环境：现网环境
测试步骤： 1) 确认评测环境； 2) 登录 ISMS 系统，对基础数据信息进行更新（修改、删除）； 3) 验证基础数据信息本地更新情况
预期结果： 1) 在步骤（2）中，正常登录系统，经营单位信息、机房信息、用户信息修改、删除功能更新正常； 2) 在步骤（3）中，基础数据更新操作实时生效
判定原则： 应符合预期结果要求，否则为不合格

测试编号：45
测试项目：基础数据查询响应时间测试
测试目的：验证 ISMS 基础数据查询结果的时间
测试环境：现网环境
测试步骤： <ol style="list-style-type: none"> 1) 确认评测环境； 2) 登录 ISMS 系统，查询本地基础数据信息； 3) 登录 ISMS 系统，查询本地基础数据异常监测信息
预期结果： <p>在步骤（2）、步骤（3）中，本地基础数据信息、本地基础数据异常监测信息查询结果完整、正确，查询响应时间少于 15min</p>
判定原则： <p>应符合预期结果要求，否则为不合格</p>

测试编号：46
测试项目：基础数据异常监测错漏率测试
测试目的：验证 ISMS 系统监测基础数据异常的错漏率
测试环境：现网环境
测试步骤： <ol style="list-style-type: none"> 1) 确认评测环境； 2) 登录 ISMS 系统； 3) 根据实际测试环境，模拟 N 个异常的基础数据（IP）； 4) 在正常业务流量背景下，通过公网终端进行访问； 5) 查看基础数据异常监测记录，计算基础数据异常监测错漏率
预期结果： <p>在步骤（5）中，要求 ISMS 基础数据监测异常记录错漏比例应不高于 1%</p>
判定原则： <p>应符合预期结果要求，否则为不合格</p>

测试编号：47
测试项目：访问日志记录入库时间测试
测试目的：验证 ISMS 访问日志留存及查询上报时间
测试环境：现网环境
测试步骤： <ol style="list-style-type: none"> 1) 确认评测环境； 2) 登录 ISMS 系统，确认访问日志功能正常； 3) 在正常业务流量背景下，通过公网终端访问 IRCS 业务节点内应用资源（客户站点或测试参考站）至少 1 万次；查看系统本地访问日志记录情况，计算访问日志入库时间

<p>预期结果：</p> <ol style="list-style-type: none"> 1) 在步骤（2）中，系统功能正常； 2) 在步骤（4），访问行为发生 2h 内可有效查询访问日志（访问日志入库时间不大于 2h）
<p>判定原则：</p> <p>应符合预期结果要求，否则为不合格</p>
<p>备注：</p> <ol style="list-style-type: none"> 1) 访问日志中记录的访问时间为起始时间，对于 TCP 类数据流量即会话首个数据包通过系统所覆盖监测链路的时间，对于 UDP 类数据流量即数据流首个数据包通过系统所覆盖监测链路的时间（如 UDP 类数据流量的数据包间隔大于 10s 则应逐包记录）； 2) 访问日志记录源 IP、目的 IP、源端口、目的端口完全正确（对属于 HTTP 的访问还包括记录 URL 完全正确），且访问时间记录误差不大于 10s 的为有效的访问日志

测试编号：48
测试项目：访问日志查询响应时间测试
测试目的：验证 ISMS 访问日志查询响应时间
测试环境：现网环境
<p>测试步骤：</p> <ol style="list-style-type: none"> 1) 确认评测环境； 2) 登录 ISMS 系统，确认访问日志功能正常； 3) 基于 IP、URL 和时间的组合条件查询系统本地访问日志记录，计算访问日志查询响应时间
<p>预期结果：</p> <ol style="list-style-type: none"> 1) 在步骤（2）中，系统功能正常； 2) 在步骤（3）中，本地访问日志查询结果完整、正确，响应时间少于 10min
<p>判定原则：</p> <p>应符合预期结果要求，否则为不合格</p>
<p>备注：</p> <p>如匹配查询条件的日志记录总量大于 1 万条，则应在响应时间内（10min）至少完成前 1 万条匹配记录（按时间由近到远排序）的回显</p>

测试编号：49
测试项目：访问日志记录错漏率测试
测试目的：验证 ISMS 系统记录访问日志的错漏率
测试环境：现网环境
<p>测试步骤：</p> <ol style="list-style-type: none"> 1) 确认评测环境； 2) 登录 ISMS 系统，确认访问日志功能正常； 3) 在正常业务流量背景下，通过公网终端访问 IRCS 业务节点内应用资源（客户站点或测试参考站）至少 1 万次； 4) 查看系统本地访问日志记录情况，计算访问日志记录错漏率
预期结果：

在步骤（4）中，访问日志记录错漏比例不高于 1%
判定原则： 应符合预期结果要求，否则为不合格
备注： 访问日志记录错漏比例=（1-访问行为发生 2h 后查询到的有效日志记录数/访问总量）×100%

测试编号：50
测试项目：活跃资源监测记录错漏率测试
测试目的：验证 ISMS 系统监测活跃资源的错漏率
测试环境：现网环境
测试步骤： 1) 确认评测环境； 2) 在正常业务流量背景下，通过公网终端访问特定 IP+端口（或 IP+端口列表）不少于 5000 次、特定域名（或特定域名列表）不少于 5000 次； 3) 登录 ISMS 系统，查看 ISMS 系统活跃资源监测记录情况，计算活跃资源监测记录访问量错漏率
预期结果： 在步骤（4）中，要求 ISMS 活跃资源监测记录访问量错漏比例应不高于 1%
判定原则： 应符合预期结果要求，否则为不合格
备注： 活跃资源监测错漏率=（1-活跃资源访问量监测结果/实际访问总量）×100%

7.9 安全性要求

测试编号：51
测试项目：时钟同步测试
测试目的：验证 ISMS 系统时间同步功能
测试环境：现网环境
测试步骤： 1) 确认评测环境； 2) 登录 ISMS 系统，查看系统时钟同步设置； 3) 查看系统有关设备本地时间； 4) 查验系统相关记录时间戳
预期结果： 1) 在步骤（2）、步骤（3）中，ISMS 系统及所有相关设备的时钟保持一致，系统时间与国家标准时间同步； 2) 在步骤（4）中，系统各类记录时间戳与国家标准时间误差不超过 1s
判定原则： 应符合预期结果要求，否则为不合格

测试编号：52
测试项目：数据备份及恢复测试
测试目的：验证 ISMS 系统的数据备份、恢复功能
测试环境：现网环境
测试步骤： <ol style="list-style-type: none"> 1) 确认评测环境； 2) 登录 ISMS 系统，查看系统相关数据备份、恢复功能设置； 3) 对系统本地数据进行备份操作； 4) 对备份的系统数据进行恢复操作
预期结果： <ol style="list-style-type: none"> 1) 系统提供完整的数据备份和恢复功能； 2) 系统本地数据可正常进行备份和转储，备份数据完整； 3) 系统支持备份数据的还原恢复功能，导入恢复过程中数据及库表等内容无异常
判定原则： <p>应符合预期结果要求，否则为不合格</p>

7.10 基础数据查询与上报

测试编号：53
测试项目：IRCS 业务主体信息上报测试
测试目的：验证 ISMS 系统添加 IRCS 业务主体信息的功能
测试环境：现网环境
测试步骤： <ol style="list-style-type: none"> 1) 确认评测环境； 2) 登录 ISMS 系统； 3) 添加 IRCS 业务主体信息（IRCS 业务经营许可证号、单位名称（应与许可证上登记信息一致）、单位地址及邮编、企业法人、网络信息安全责任人、应急联系人信息、IRCS 业务机房数量、以及各个 IRCS 业务机房相关信息。其中，IRCS 业务机房相关信息包括各个 IRCS 业务机房的名称、编号、IRCS 业务机房所处机房的性质、IRCS 业务机房所在地、地址及邮编、IRCS 业务机房驻地网络信息安全责任人信息）； 4) 登录 SMMS，查验 ISMS 上报的添加信息，并验证正确性
预期结果： <ol style="list-style-type: none"> 1) 在步骤（3）中，成功添加信息，并在保存后自动上报至 SMMS 系统； 2) 在步骤（4）中，成功接收上报的添加信息且与 ISMS 系统本地信息一致
判定原则： <p>应符合预期结果要求，否则为不合格</p>
备注： <p>如果测试前，ISMS 已完成和 SMMS 的对接及全部数据的上报，则测试步骤（3）中可使用临时测试数据进行功能验证；完成测试步骤（5）后，可根据 SMMS 已存在的活跃资源记录数据，随机抽取至少 10 条记录，并在 ISMS 已上报的基础数据中查验相应的业务资源信息，如果有关数据记录不全、不实，则判定该项不合格</p>

测试编号：54
测试项目：IRCS 业务资源信息上报测试
测试目的：验证 ISMS 系统添加 IRCS 业务资源信息的功能
测试环境：现网环境
测试步骤： <ol style="list-style-type: none"> 1) 确认评测环境； 2) 登录 ISMS 系统； 3) 添加 IRCS 的 IP 段信息（IP 段编号、起始 IP 地址、终止 IP 地址、来源、分配单位、分配使用时间、使用单位信息、IP 地址使用方式（静态/动态））； 4) 添加 IRCS 业务机房机架信息（可选），包括（机架/机位编号、所在 IRCS 业务机房编号、分配状态（未分配/已分配）、占用状态（未占用/已占用））； 5) 添加 IRCS 的链路信息（互联网出入口链路编号、网关 IP 地址、链路带宽、链路类型、链路接入单位信息、互联网接入地）； 6) 添加 IRCS 的公共域名信息（域名地址、用户自定义域名级别）； 7) 登录 SMMS，查验 ISMS 上报的添加信息，并验证正确性
预期结果： <ol style="list-style-type: none"> 1) 在步骤（3）、（4）、（5）、（6）中，成功添加信息，并在保存后自动上报至 SMMS 系统； 2) 在步骤（8）中，成功接收上报的添加信息且与 ISMS 系统本地信息一致
判定原则： <p>应符合预期结果要求，否则为不合格</p>
备注： <p>如果测试前，ISMS 已完成和 SMMS 的对接及全部数据的上报，则测试步骤（3）、（4）、（5）、（6）中可使用临时测试数据进行功能验证；完成测试步骤（7）后，可根据 SMMS 已存在的活跃资源记录数据，随机抽取至少 10 条记录，并在 ISMS 已上报的基础数据中查验相应的业务资源数据，如果有关数据记录不全、不实，则判定该项不合格</p>

测试编号：55
测试项目：IRCS 业务用户信息上报测试
测试目的：验证 ISMS 系统添加 IRCS 业务用户信息的功能
测试环境：现网环境
测试步骤： <ol style="list-style-type: none"> 1) 确认评测环境； 2) 登录 ISMS 系统； 3) 添加业务用户信息（用户编号、用户属性（分为提供应用服务、其他等类）、用户单位名称（或姓名）、用户单位地址及邮编、用户单位属性、证件类型、证件号码、网络信息安全责任人信息、服务开通时间）； 4) 添加提供内部应用的应用服务用户信息（应用服务类型、接入方式（见技术要求附录 A.4）、域名信息列表（提供支持域名指向的应用服务如：HTTP、FTP、SMTP、POP3 等需提供本级域名））； 5) 添加提供电信业务的应用服务用户信息（应用服务类型、业务许可证号、接入方式、预登记的服务内容（可多选）、域名信息列表（提供支持域名指向的应用服务如：HTTP、FTP、SMTP、POP3 等需提供本级域名））； 6) 添加提供互联网服务的应用服务用户信息（应用服务类型、备案号、接入方式、预登记的服务内容（可多选）、域名信息列表（提供支持域名指向的应用服务如：HTTP、FTP、SMTP、POP3 等需提供本级域名））；

7) 登录 SMMS, 查验 ISMS 上报的添加信息, 并验证正确性
<p>预期结果:</p> <p>1) 在步骤 (3)、(4)、(5)、(6) 中, 成功添加信息, 并在保存后自动上报至 SMMS 系统, 上报至 SMMS 的信息字段至少包括用户编号、用户属性、用户的应用服务信息, 针对业务用户总量有变化的, 需把对应的业务用户总量也更新上报至 SMMS 系统;</p> <p>2) 在步骤 (7) 中, 成功接收上报的添加信息且与 ISMS 系统本地信息一致</p>
<p>判定原则:</p> <p>应符合预期结果要求, 否则为不合格</p>
<p>备注:</p> <p>1) 根据管理要求, 同一 IP 地址 (段) 不能同时供多个用户共同使用, 在添加 IRCS 业务机房时, 客户应用相关 IP 地址中的地址段范围应为经营单位业务资源数据中某一 IP 段的子集;</p> <p>2) 如果测试前, ISMS 已完成和 SMMS 的对接及全部数据的上报, 则测试步骤 (3)、(4)、(5)、(6)、中可使用临时测试数据进行功能验证; 完成测试步骤 (7) 后, 可根据 SMMS 已存在的活跃资源记录数据, 随机抽取至少 10 条记录, 并在 ISMS 已上报的基础数据中查验相应的业务客户数据, 如果有关数据记录不全、不实, 则判定该项不合格</p>

测试编号: 56
测试项目: IRCS 业务主体信息修改与更新上报测试
测试目的: 验证 ISMS 系统修改更新 IRCS 业务主体信息后的上报功能
测试环境: 现网环境
<p>测试步骤:</p> <p>1) 确认评测环境;</p> <p>2) 登录 ISMS 系统;</p> <p>3) 修改或删除 IRCS 业务主体信息 (IRCS 业务经营许可证号、单位名称 (应与许可证上登记信息一致)、单位地址及邮编、企业法人、网络信息安全责任人、应急联系人信息、IRCS 业务机房数量以及各个 IRCS 业务机房相关信息。其中, IRCS 业务机房相关信息包括各个 IRCS 业务机房的名称、编号、IRCS 业务机房所处机房的性质、IRCS 业务机房所在地、地址及邮编、IRCS 业务机房驻地网络信息安全责任人信息);</p> <p>4) 登录 SMMS, 查验 ISMS 上报的修改信息, 并验证正确性</p>
<p>预期结果:</p> <p>1) 在步骤 (3) 中, 成功修改或删除信息, 并在保存后自动增量上报至 SMMS 系统;</p> <p>2) 在步骤 (4) 中, 成功接收上报的修改更新信息且与 ISMS 系统本地信息一致</p>
<p>判定原则:</p> <p>应符合预期结果要求, 否则为不合格</p>
<p>备注:</p> <p>如果测试前, ISMS 已完成和 SMMS 的对接及全部数据的上报, 则测试步骤 (3)、(4) 中可使用临时测试数据进行功能验证</p>

测试编号: 57
测试项目: IRCS 业务资源修改与更新测试
测试目的: 验证 ISMS 系统修改修改 IRCS 业务资源的功能

测试环境：现网环境
<p>测试步骤：</p> <ol style="list-style-type: none"> 1) 确认评测环境； 2) 登录 ISMS 系统； 3) 修改或删除 IRCS 的 IP 段信息（IP 段编号、起始 IP 地址、终止 IP 地址、来源、分配单位、分配使用时间、使用单位信息、IP 地址使用方式（静态/动态））； 4) 修改或删除 IRCS 业务机房机架信息（可选），包括机架/机位编号、所在 IRCS 业务机房编号、分配状态（未分配/已分配）、占用状态（未占用/已占用）； 5) 修改或删除 IRCS 的链路信息（互联网出入口链路编号、网关 IP 地址、链路带宽、链路类型、链路接入单位信息、互联网接入地）； 6) 修改或删除 IRCS 的公共域名信息（域名地址、用户自定义域名级别） 7) 登录 SMMS，查询 ISMS 上报的修改信息，并验证正确性
<p>预期结果：</p> <ol style="list-style-type: none"> 1) 在步骤（3）、（4）、（5）、（6）、（7）中，成功修改或删除信息，并在保存后自动增量上报至 SMMS 系统； 2) 在步骤（8）中，成功接收上报的修改更新信息且与 ISMS 系统本地信息一致
<p>判定原则：</p> <p>应符合预期结果要求，否则为不合格</p>
<p>备注：</p> <p>如果测试前，ISMS 已完成和 SMMS 的对接及全部数据的上报，则测试步骤（3）、（4）、（5）、（6）、（7）中可使用临时测试数据进行功能验证</p>

测试编号：58
测试项目：IRCS 业务用户信息修改与更新测试
测试目的：验证 ISMS 系统修改 IRCS 业务用户信息的功能
测试环境：现网环境
<p>测试步骤：</p> <ol style="list-style-type: none"> 1) 确认评测环境； 2) 登录 ISMS 系统； 3) 修改或删除业务用户信息（用户编号、用户属性（分为提供应用服务、其他等类）、用户单位名称（或姓名）、用户单位地址及邮编、用户单位属性、证件类型、证件号码、网络信息安全责任人信息、服务开通时间）； 4) 修改或删除提供内部应用的应用服务用户信息（应用服务类型、接入方式（见附录 A.4）、域名信息列表（提供支持域名指向的应用服务如：HTTP、FTP、SMTP、POP3 等需提供本级域名）），并查询修改结果； 5) 修改或删除提供电信业务的应用服务用户信息（应用服务类型、业务许可证号、接入方式、预登记的服务内容（可多选）、域名信息列表（提供支持域名指向的应用服务如：HTTP、FTP、SMTP、POP3 等需提供本级域名））； 6) 修改或删除提供互联网服务的应用服务用户信息（应用服务类型、备案号、接入方式、预登记的服务内容（可多选）、域名信息列表（提供支持域名指向的应用服务如：HTTP、FTP、SMTP、POP3 等需提供本级域名））； 7) 登录 SMMS，查验 ISMS 上报的修改信息，并验证正确性
<p>预期结果：</p> <ol style="list-style-type: none"> 1) 在步骤（3）、（4）、（5）、（6）中，成功修改或删除信息，并在保存后自动增量上报至 SMMS 系统，上报至 SMMS 的信息字段至少包括用户编号、用户属性、用户的应用服务信息，针对业务用户总量有变化的，需把对应的业务用

户总量也更新上报至 SMMS 系统； 2) 在步骤（7）中，成功接收上报的修改更新信息且与 ISMS 系统本地信息一致
判定原则： 应符合预期结果要求，否则为不合格
备注： 如果测试前，ISMS 已完成和 SMMS 的对接及全部数据的上报，则测试步骤（3）、（4）、（5）、（6）中可使用临时测试数据进行功能验证

测试编号：59
测试项目：核验异常数据处理与重新上报测试
测试目的：验证 ISMS 系统接收 IRCS 业务主体信息的核验信息的功能
测试环境：现网环境
测试步骤： 1) 确认评测环境； 2) 登录 ISMS 系统； 3) 添加或导入与 SMMS 系统内既有数据记录会产生冲突的 IRCS 业务主体信息及其他信息并上报至 SMMS 系统，查看 SMMS 系统反馈的核验信息文件； 4) 添加数据内容不完整的 IRCS 业务主体信息及其他信息并上报至 SMMS 系统，查看 SMMS 系统反馈的核验信息文件； 5) 添加数据内容错误的 IRCS 业务主体信息及其他信息并上报至 SMMS 系统，查看 SMMS 系统反馈的核验信息文件
预期结果： 1) 在步骤（3）中，ISMS 成功接收 SMMS 系统反馈的核验异常记录及提示，其中显示数据错误原因为“上报数据与既有数据记录冲突”； 2) 在步骤（4）中，ISMS 成功接收 SMMS 系统反馈的核验异常记录及提示，其中显示数据错误原因为“上报数据内容不完整”； 3) 在步骤（5）中，ISMS 成功接收 SMMS 系统反馈的核验异常记录及提示，其中显示数据错误原因为“上报数据内容错误”； 4) 在步骤（3）、（4）、（5）中，要求 ISMS 系统对核验异常数据进行修改并重新上报，直至无误
判定原则： 应符合预期结果要求，否则为不合格
备注： 1) 测试步骤（3）中，根据 SMMS 系统已有基础数据信息，通过 ISMS 系统上报与既有记录信息存在冲突的数据（例如企业法人）； 2) 测试步骤（4）中，通过 ISMS 系统上报数据内容不完整的记录（例如缺失必填字段）； 3) 测试步骤（5）中，通过 ISMS 系统上报数据内容存在逻辑错误的记录（例如字段超出规定长度、填写非法字符）； 4) 如果在测试步骤（4）、（5）中，ISMS 系统在系统操作界面提供数据格式、内容校验，则不做要求； 5) 如果测试前，ISMS 已完成和 SMMS 的对接及全部数据的上报，则测试步骤（3）、（4）、（5）中可使用临时测试数据进行功能验证；完成测试步骤（5）后，可根据 SMMS 已存在的活跃资源记录数据，随机抽取至少 10 条记录，并在 ISMS 已上报的基础数据中查验相应的业务资源信息、业务客户数据，如果有关数据记录不全、不实，则退回 ISMS 补正，判定该项不合格

测试编号：60
测试项目：IRCS 业务用户信息查询测试
测试目的：验证 ISMS 系统 IRCS 业务用户信息查询上报功能
测试环境：现网环境
测试步骤： <ol style="list-style-type: none"> 1) 确认评测环境； 2) 登录 SMMS 系统，下发经营单位下某个或某几个业务用户信息的查询指令； 3) 查看 ISMS 上报结果的查询结果，并验证正确性
预期结果： <p>在步骤（3）中，SMMS 成功接收 ISMS 系统上报的用户信息，且与 ISMS 系统本地信息一致</p>
判定原则： <p>应符合预期结果要求，否则为不合格</p>

7.11 动态资源查询与上报

测试编号：61
测试项目：动态资源使用日志查询和上报测试
测试目的：验证 ISMS 系统按照条件上报动态资源使用日志查询结果的功能
测试环境：现网环境
测试步骤： <ol style="list-style-type: none"> 1) 确认评测环境； 2) 通过公网终端申请使用 IRCS 的虚拟资源、网络资源（IP 地址和域名），形成动态资源使用日志； 3) 登录 SMMS，下发基于单个用户编号及查询时间段的使用日志查询指令； 4) 登录 SMMS，下发基于单个公网 IP 地址及查询时间段的使用日志查询指令； 5) 登录 SMMS，下发基于单个域名及查询时间段的使用日志查询指令
预期结果： <ol style="list-style-type: none"> 1) 在步骤（3）中，ISMS 在查询指令下发 10 分钟内完整上报用户编号、用户查询时间段内所有可用的域名信息列表、用户拥有的公网 IP 地址列表及公网 IP 地址资源对应的虚拟资源编号、虚拟资源类型；在步骤（4）中，ISMS 在查询指令下发 10 分钟内完整上报用户编号、查询 IP 地址对应的虚拟资源编号、虚拟资源类型； 2) 在步骤（5）中，ISMS 在查询指令下发 10 分钟内完整上报该域名在查询时间段内所属的用户信息，查询内容包含用户编号
判定原则： <p>应符合预期结果要求，否则为不合格</p>

7.12 业务状态记录上报

测试编号：62
测试项目：活跃资源监测记录上报与查询功能测试
测试目的：验证 ISMS 系统上报活跃资源监测内容的功能
测试环境：现网环境
测试步骤： <ol style="list-style-type: none"> 1) 确认评测环境；

2) 登录 ISMS 系统; 3) 通过公网终端访问 IRCS 业务节点内应用资源 (客户站点或测试参考站, IP 和域名), 形成活跃资源监测记录; 4) 登录 SMMS, 查询 ISMS 上报的监测记录 (或通过下发查询指令, 查询 ISMS 上报的监测记录)
预期结果: 1) 在步骤 (4) 中, ISMS 定时 (上报周期为日) 向 SMMS 上报监测结果 (或根据查询指令, 向 SMMS 上报的监测记录信息), 上报记录内容正确、完整 (对于活跃域名监测记录至少应包括发现的活跃域名、关联 IP、首次访问时间、最后访问时间、24 小时累计活跃度; 对于活跃 IP 及应用端口监测记录至少应包括发现的活跃 IP、应用端口、传输层协议类型 (TCP/UDP)、首次访问时间、最后访问时间、24 小时累计活跃度); 2) 在步骤 (4) 中, SMMS 系统下发查询指令的上报记录应为当天 0 点截止到查询指令下发时的实时记录
判定原则: 应符合预期结果要求, 否则为不合格
备注: 不建议在基于某 IP 地址或域名的过滤指令或处置操作生效的情况下, 将用户对该资源的访问行为记入访问量

测试编号: 63
测试项目: 基础数据异常监测记录上报测试
测试目的: 验证 ISMS 系统对基础数据异常状态的监测信息内容上报功能
测试环境: 现网环境
测试步骤: 1) 确认评测环境; 2) 登录 ISMS 系统, 确认基础数据异常发现功能正常; 3) 访问未报备 IP 地址接入的站点、已报备且登记使用方式为保留的 IP 地址接入的站点; 4) 登录 SMMS, 查询 ISMS 上报的监测记录
预期结果: 1) 在步骤 (4) 中, ISMS 定时 (上报周期为日) 向 SMMS 上报监测结果, 上报记录内容正确、完整; 2) 当 ISMS 系统内未有异常记录时, 按“零报告”要求上报监测结果; 当在一个上报周期内即完成处置 (ISMS 监测恢复正常), ISMS 应基于处置状态的不同生成至少两条独立的记录并向 SMMS 上报
判定原则: 应符合预期结果要求, 否则为不合格
备注: 1) 在测试过程中, 可适当临时调整定时上报任务, 缩短上报周期, 方便测试; 2) 为配合测试, 可临时通过 SMMS 退回特定的已通过核验的基础数据记录, 以便模拟未报备 IP 地址接入的站点、已报备且登记使用方式为保留的 IP 地址接入的站点; 3) 如果在现网环境条件下进行测试时, 不便模拟基础数据异常情况, 则需要在业务节点内搭建临时性测试参考靶站来配合完成该项测试

7.13 信息安全记录上报

测试编号: 64
测试项目: 违法网站列表下发功能测试

测试目的：验证 ISMS 系统接收并更新本地违法违规网站列表和免过滤网站列表功能
测试环境：现网环境
测试步骤： <ol style="list-style-type: none"> 1) 确认评测环境； 2) 登录 SMMS 系统，分别向企业下发违法网站列表和免过滤网站列表； 3) 登录 ISMS 系统，查询 ISMS 系统本地的违法网站列表和免过滤网站列表名单
预期结果： <p>在步骤（3）中，ISMS 系统成功接收 SMMS 系统下发的违法网站列表和免过滤网站列表，且同步更新至本地的列表信息，与 SMMS 系统下发的列表内容一致</p>
判定原则： <p>应符合预期结果要求，否则为不合格</p>

测试编号：65
测试项目：违法违规网站监测记录上报测试
测试目的：验证 ISMS 系统违法违规网站发现及监测记录上报功能
测试环境：现网环境
测试步骤： <ol style="list-style-type: none"> 1) 确认评测环境； 2) 登录 ISMS 系统，确认违法违规网站发现功能正常（仅监测不处置）； 3) 访问属于违法网站列表中的违法网站； 4) 访问属于未备案状态的网站（无备案记录的网站）； 5) 登录 SMMS，查询 ISMS 上报的监测记录（或通过下发查询指令，查询 ISMS 上报的监测记录）
预期结果： <ol style="list-style-type: none"> 1) 在步骤（2）中，成功下发违法违规网站监测指令； 2) 在步骤（3）、步骤（4）中，可访问违法违规网站； 3) 在步骤（5）中，ISMS 定时（上报周期为日）向 SMMS 上报监测记录信息，（或根据查询指令，向 SMMS 上报实时的监测记录信息），上报记录内容正确、完整（至少包括违法违规网站的域名、IP、服务内容、违法违规情况以及当前状态（未处置）等）； 4) 当 ISMS 系统内未有异常记录时，按“零报告”要求上报监测结果
判定原则： <p>应符合预期结果要求，否则为不合格</p>
备注： <p>如果在现网环境条件下进行测试时，不便模拟违法违规网站情况，则需要业务机房/业务节点内搭建临时性测试参考靶站来配合完成该项测试</p>

测试编号：66
测试项目：违法违规网站处置记录上报测试
测试目的：验证 ISMS 系统违法违规网站处置记录上报功能
测试环境：现网环境

<p>测试步骤：</p> <ol style="list-style-type: none"> 1) 确认评测环境； 2) 登录 ISMS 系统，确认违法违规网站发现功能正常（发现即处置）； 3) 访问属于违法网站列表中的违法网站； 4) 访问属于未备案状态的网站（无备案记录的网站）； 5) 登录 SMMS，查询 ISMS 上报的处置记录（或通过下发查询指令，查询 ISMS 上报的处置记录）
<p>预期结果：</p> <ol style="list-style-type: none"> 1) 在步骤（2）中，成功下发违法违规网站处置指令； 2) 在步骤（3）、步骤（4）中，无法访问违法违规网站，其他访问不受影响； 3) 在步骤（5）中，ISMS 定时（上报周期为日）向 SMMS 上报处置记录信息，（或根据查询指令，向 SMMS 上报实时的处置记录信息），上报记录内容正确、完整（至少包括违法违规网站的域名、IP、服务内容、违法违规情况以及当前状态（已处置）、处置人账号等）； 4) 对于在一个上报周期内处置状态发生变化，ISMS 应基于处置状态生成至少两条独立的记录并向 SMMS 上报
<p>判定原则：</p> <p>应符合预期结果要求，否则为不合格</p>
<p>备注：</p> <p>如果在现网环境条件下进行测试时，不便模拟违法违规网站情况，则需要在业务机房/业务节点内搭建临时性测试参考靶站来配合完成该项测试</p>

测试编号：67
测试项目：违法信息监测指令下发测试
测试目的：验证 SMMS 系统向 ISMS 系统下发违法信息监测指令的功能
测试环境：现网环境
<p>测试步骤：</p> <ol style="list-style-type: none"> 1) 确认评测环境； 2) 登录 SMMS 系统，下发基于特定 IP+特定传输层协议（TCP/UDP）端口的违法信息监测指令； 3) 通过公网终端访问 IRCS 业务节点内应用资源（客户站点或测试参考站），查看 ISMS 系统中相应的违法信息监测记录； 4) 下发基于域名、URL、关键词的违法信息监测指令，重复步骤（3）
<p>预期结果：</p> <ol style="list-style-type: none"> 1) 在步骤（2）、步骤（4）中，成功下发违法信息监测指令； 2) 在步骤（3）中，可访问符合违法信息监测规则的资源，同时在 ISMS 系统生成相应的日志记录
<p>判定原则：</p> <p>应符合预期结果要求，否则为不合格</p>
<p>备注：</p> <p>如果在现网环境条件下进行测试时，不便下发指令，则需要在 IRCS 业务节点内搭建临时性测试参考靶站来配合完成该项测试</p>

测试编号：68
测试项目：违法信息监测记录上报测试
测试目的：验证 ISMS 系统违法信息监测日志上报的功能
测试环境：现网环境
测试步骤： <ol style="list-style-type: none"> 1) 确认评测环境； 2) 登录 SMMS 系统，下发基于特定 IP+特定传输层协议（TCP/UDP）端口的违法信息监测指令； 3) 通过公网终端访问 IRCS 业务节点内应用资源（客户站点或测试参考站）； 4) 查看 ISMS 系统上报的违法信息监测记录； 5) 下发基于域名、URL、关键词的违法信息监测指令，重复步骤（3）、步骤（4）
预期结果： <ol style="list-style-type: none"> 1) 在步骤（2）、步骤（5）中，成功下发违法信息监测指令； 2) 在步骤（3）中，可访问符合违法信息监测规则的资源； 3) 在步骤（4）中，ISMS 系统上报违法信息监测记录信息完整、准确； 4) 对于关键字监测指令，在指令生效后生成的首次监测记录应当留存页面快照并上报
判定原则： <p>应符合预期结果要求，否则为不合格</p>

测试编号：69
测试项目：违法信息过滤指令下发测试
测试目的：验证 SMMS 系统向 ISMS 系统下发违法信息过滤指令的功能
测试环境：现网环境
测试步骤： <ol style="list-style-type: none"> 1) 确认评测环境； 2) 登录 SMMS 系统，下发基于特定 IP+特定传输层协议（TCP/UDP）端口的违法信息过滤指令； 3) 通过公网终端访问 IRCS 业务节点内应用资源（客户站点或测试参考站），查看 ISMS 系统中相应的违法信息过滤记录； 4) 下发基于域名、URL、关键词的违法信息过滤指令，重复步骤（3）
预期结果： <ol style="list-style-type: none"> 1) 在步骤（2）、步骤（4）中，成功下发违法信息过滤指令； 2) 在步骤（3）中，不可访问符合违法信息过滤规则的资源，同时在 ISMS 系统生成相应的日志记录
判定原则： <p>应符合预期结果要求，否则为不合格</p>
备注： <p>如果在现网环境条件下进行测试时，不便下发指令，则需要 IRCS 业务节点内搭建临时性测试参考靶站来配合完成该项测试</p>

测试编号：70
测试项目：违法信息过滤管理指令申诉功能测试
测试目的：验证违法信息过滤管理指令的申诉功能
测试环境：现网环境
测试步骤： <ol style="list-style-type: none"> 1) 确认评测环境； 2) 登录 SMMS 系统，下发基于域名、URL 的违法信息过滤管理指令； 3) 登录 ISMS 系统，查看相应的违法信息管理过滤指令，并申诉； 4) 登录 SMMS 系统，处理 ISMS 的申诉结果为通过，并把申诉结果反馈给 ISMS； 5) 通过公网终端访问违法信息过滤管理指令规则中的域名、URL； 6) 登录 SMMS 系统，下发基于域名、URL 的违法信息过滤管理指令； 7) 登录 ISMS 系统，查看相应的违法信息管理过滤指令，并申诉； 8) 登录 SMMS 系统，处理 ISMS 的申诉结果为不通过，并把申诉结果反馈给 ISMS； 9) 通过公网终端访问违法信息过滤管理指令规则中的域名、URL
预期结果： <ol style="list-style-type: none"> 1) 在步骤（5）中，可访问符合违法信息过滤规则的资源； 2) 在步骤（9）中，不可访问符合违法信息过滤规则的资源
判定原则： <p>应符合预期结果要求，否则为不合格</p>

测试编号：71
测试项目：违法信息过滤记录上报测试
测试目的：验证 ISMS 系统违法信息过滤日志上报的功能
测试环境：现网环境
测试步骤： <ol style="list-style-type: none"> 1) 确认评测环境； 2) 登录 SMMS 系统，下发基于特定 IP+特定传输层协议（TCP/UDP）端口的违法信息过滤指令； 3) 通过公网终端访问 IRCS 业务节点内应用资源（客户站点或测试参考站）； 4) 查看 ISMS 系统上报的违法信息过滤记录； 5) 下发基于域名、URL、关键词的违法信息过滤指令，重复步骤（3）、步骤（4）
预期结果： <ol style="list-style-type: none"> 1) 在步骤（2）、步骤（5）中，成功下发违法信息监测指令； 2) 在步骤（3）中，无法访问符合违法信息监测规则的资源，其他访问不受影响； 3) 在步骤（4）中，ISMS 系统上报违法信息过滤记录信息完整、准确； 4) 对于关键字过滤指令，在指令生效后生成的首次过滤记录应当留存页面快照并上报
判定原则： <p>应符合预期结果要求，否则为不合格</p>

测试编号：72
测试项目：规则优先级与冲突校验测试
测试目的：验证 ISMS 系统对规则优先级的冲突校验功能
测试环境：现网环境
测试步骤： <ol style="list-style-type: none"> 1) 确认评测环境，登录 ISMS 系统； 2) ISMS 创建并下发基于域名的违法信息监测指令； 3) 通过公网终端进行访问验证； 4) ISMS 创建并下发步骤（2）中监测域名的违法信息过滤指令； 5) 通过公网终端进行访问验证； 6) 删除违法信息监测指令； 7) ISMS 创建并下发步骤（4）中过滤域名的免过滤网站指令； 8) 通过公网终端进行访问验证
预期结果： <ol style="list-style-type: none"> 1) 在步骤（3）中，可以正常访问存在于监测规则中的网站； 2) 在步骤（5）中，无法正常访问同时存在于监测规则和过滤规则中的网站； 3) 在步骤（8）中，可以正常访问同时存在于免过滤网站列表和违法信息过滤规则中的网站
判定原则： <p>应符合预期结果要求，否则为不合格</p>
备注： <ol style="list-style-type: none"> 1) 如果 ISMS 系统实现了规则冲突提醒功能并阻止冲突规则下发，核实规则之间的逻辑后则对此项不作要求； 2) 测试方法不仅限于测试步骤中的举例，可以从更多方面的角度验证规则优先级与冲突校验

测试编号：73
测试项目：指令及结果可见性管理测试
测试目的：验证 ISMS 系统对系统指令管理的功能
测试环境：现网环境
测试步骤： <ol style="list-style-type: none"> 1) 确认评测环境； 2) 登录 SMMS 系统，向 ISMS 系统下发管理指令，限制 ISMS 查看相关指令及执行结果； 3) 登录 ISMS 系统，查看 SMMS 下发指令和执行数据； 4) 登录 SMMS 系统，向 ISMS 系统下发管理指令，允许 ISMS 查看相关指令及执行结果； 5) 登录 ISMS 系统，查看 SMMS 下发指令和执行数据
预期结果： <ol style="list-style-type: none"> 1) 在步骤（2）、步骤（4）中，指令和数据下发成功； 2) 在步骤（3）中，在 ISMS 系统中无法查看 SMMS 下发的指令和执行情况； 3) 在步骤（5）中，在 SMMS 系统中可以查看 SMMS 下发的指令和执行情况
判定原则： <p>应符合预期结果要求，否则为不合格</p>

7.14 访问日志查询与上报

测试编号：74
测试项目：访问日志查询和上报测试
测试目的：验证 ISMS 系统按照查询条件上报访问日志查询结果的功能
测试环境：现网环境
测试步骤： <ol style="list-style-type: none"> 1) 确认评测环境； 2) 通过公网终端访问 IRCS 业务节点内应用资源（客户站点或测试参考站），形成访问日志； 3) 登录 SMMS，下发基于源 IP 地址、源端口、查询时间段的访问日志查询指令； 4) 登录 SMMS，下发基于目的 IP 地址、目的端口、查询时间段的访问日志查询指令； 5) 登录 SMMS，下发基于源 IP 地址、查询时间段的访问日志查询指令； 6) 登录 SMMS，对于浏览类访问日志，下发基于用户访问 URL、查询时间段的查询指令
预期结果： <ol style="list-style-type: none"> 1) 在步骤（3）中，ISMS 完整上报符合源 IP 地址、源端口、查询时间段条件的全部日志记录信息； 2) 在步骤（4）中，ISMS 完整上报符合目的 IP 地址、目的端口、查询时间段条件的全部日志记录信息； 3) 在步骤（5）中，ISMS 完整上报符合源 IP 地址、查询时间段条件的全部日志记录信息； 4) 在步骤（6）中，对于浏览类访问日志，ISMS 完整上报符合访问 URL、查询时间段条件的全部日志记录信息
判定原则： <p>应符合预期结果要求，否则为不合格</p>

7.15 性能要求测试

测试编号：75
测试项目：信息安全规则容量测试
测试目的：验证 ISMS 系统的规则容量
测试环境：现网环境
测试步骤： <ol style="list-style-type: none"> 1) 确认评测环境； 2) 登录 SMMS 系统，向 ISMS 系统下发违法信息监测（或处置）规则； 3) 通过公网终端访问 IRCS 业务节点内应用资源（客户站点或测试参考站），对规则有效性进行验证； 4) 查看违法信息监测（或处置）规则的执行结果
预期结果： <ol style="list-style-type: none"> 1) 步骤（2）中，规则下发正常； 2) 步骤（3）、步骤（4）中，规则执行正常； 3) ISMS 系统支持由 SMMS 系统下发的违法信息监测（或过滤）规则不少于 5 万条，其中特定域名、特定 URL、特定关键词的规则至少各 1 万条
判定原则： <p>应符合预期结果要求，否则为不合格</p>
备注： <ol style="list-style-type: none"> 1) 单个违法信息监测（或处置）指令最多携带 100 条规则，规则之间为逻辑“与”关系；

2) 如果在现网环境条件下进行测试时,不便下发指令,则需要在 IRCS 业务节点内搭建临时性测试参考靶站来配合完成该项测试

测试编号: 76

测试项目: 信息安全规则匹配准确率测试

测试目的: 验证 ISMS 的规则匹配准确率

测试环境: 现网环境

测试步骤:

- 1) 确认评测环境;
- 2) 登录 SMMS 系统,向 ISMS 系统下发 5 万条违法信息监测、过滤规则;
- 3) 在正常业务流量背景下,通过公网终端访问在监测规则列表的应用资源(客户站点或测试参考站)至少 1 万次;
- 4) 计算违法信息监测规则匹配的准确率;
- 5) 在正常业务流量背景下,通过公网终端访问在过滤规则列表的应用资源(客户站点或测试参考站)至少 1 万次;计算违法信息过滤规则匹配的准确率

预期结果:

- 1) 在步骤(2)中,生效的规则不少于 6 万条,其中特定域名、特定 URL、特定关键词的监测、过滤规则至少各 1 万条;
- 2) 在步骤(4)中,对于匹配监测规则的访问,准确比例不低于 95%、漏判和错判总比例不高于 5%;
- 3) 在步骤(7)中,对于匹配过滤规则的访问,准确比例不低于 95%、漏判和错判总比例不高于 5%

判定原则:

应符合预期结果要求,否则为不合格

备注:

- 1) 准确比例=系统有效监测识别(或成功过滤)的访问量/实际匹配监测(或过滤)规则的访问总量 $\times 100\%$;
- 2) 漏判和错判总比例=(系统未有效监测识别(或未成功过滤)的访问量+系统监测识别(或过滤)的无关访问量)/实际匹配监测(或过滤)规则的访问总量 $\times 100\%$

测试编号: 77

测试项目: 信息安全记录查询响应时间测试

测试目的: 验证 ISMS 的信息安全记录上报时间

测试环境: 现网环境

测试步骤:

- 1) 确认评测环境;
- 2) 登录 ISMS 系统,确认违法违规网站监测(和处置)功能状态;
- 3) 访问属于违法网站列表中的违法网站、访问属于未备案状态的网站(无备案记录的网站);
- 4) 登录 SMMS 系统,下发违法违规网站监测(和处置)查询指令;
- 5) 查看 ISMS 上报违法违规网站监测(和处置)记录信息,并验证正确性

预期结果:

- 1) 在步骤(2)中,系统违法违规网站监测(和处置)功能状态正常;
- 2) 在步骤(5)中,完整的查询数据在 10min 内上报至 SMMS 系统

判定原则： 应符合预期结果要求，否则为不合格

测试编号：78
测试项目：基础数据查询响应时间测试
测试目的：验证 ISMS 基础数据查询结果的上报时间
测试环境：现网环境
测试步骤： 1) 确认评测环境； 2) 登录 SMMS 系统，下发基础数据信息查询指令； 3) 查看 ISMS 上报基础数据信息，并验证正确性，计算数据获取时间； 4) 登录 SMMS 系统，下发基础数据异常监测信息查询指令； 5) 查看 ISMS 上报基础数据信息，并验证正确性，计算数据获取时间
预期结果： 在步骤（3）、步骤（5）中，完整的查询数据 15min 内上报至 SMMS，且基础数据信息与 ISMS 系统本地信息一致
判定原则： 应符合预期结果要求，否则为不合格

测试编号：79
测试项目：异常状态监测错漏率测试
测试目的：验证 ISMS 系统上报基础数据异常监测记录的错漏率
测试环境：现网环境
测试步骤： 1) 确认评测环境； 2) 登录 ISMS 系统； 3) 根据实际测试环境，模拟 N 个异常的基础数据（IP）； 4) 在正常业务流量背景下，通过公网终端进行访问； 5) 登录 SMMS 系统，下发异常监测记录查询指令，根据上报记录情况计算基础数据异常监测错漏率
预期结果： 在步骤（5）中，要求 ISMS 上报的基础数据监测异常记录错漏比例应不高于 1%
判定原则： 应符合预期结果要求，否则为不合格
备注： 如果在现网环境条件下进行测试时，不便模拟基础数据异常情况，则需要在 IRCS 业务节点内搭建临时性测试参考靶站来配合完成该项测试

测试编号：80
测试项目：访问日志记录入库时间测试
测试目的：验证通过 SMMS 系统查询访问日志入库时间
测试环境：现网环境
测试步骤： 1) 确认评测环境； 2) 登录 ISMS 系统，确认访问日志功能正常； 3) 在正常业务流量背景下，通过公网终端访问 IRCS 业务节点内应用资源（客户站点或测试参考站）至少 1 万次； 4) 在访问行为发生 2h 时，登录 SMMS 系统，下发访问日志查询指令，根据 ISMS 反馈结果计算访问日志入库时间，验证访问结果
预期结果： 1) 在步骤（2）中，系统功能正常； 2) 在步骤（4），访问行为发生 2h 内可有效查询访问日志（访问日志入库时间不大于 2h），且访问日志的数量及相关记录内容与 ISMS 系统内访问日志内容一致
判定原则： 应符合预期结果要求，否则为不合格

测试编号：81
测试项目：访问日志查询响应时间测试
测试目的：验证 SMMS 系统查询访问日志的响应时间
测试环境：现网环境
测试步骤： 1) 确认评测环境； 2) 登录 SMMS 系统，通过指令查询访问日志； 3) 基于 IP、URL 和时间的组合条件查询 ISMS 系统访问日志记录，计算访问日志查询响应时间； 4) 查看 ISMS 上报访问日志信息，并验证正确性
预期结果： 1) 在步骤（3）中，完整的查询数据 10min 内上报至 SMMS 系统； 2) 在步骤（4）中，访问日志查询上报的结果完整、正确，内容与 ISMS 系统本地记录一致
判定原则： 应符合预期结果要求，否则为不合格
备注： 如匹配查询条件的日志记录总量大于 1 万条，则应在响应时间内（10min）至少完成前 1 万条匹配记录（按时间由近到远排序）的回显和上报

测试编号：82
测试项目：访问日志记录错漏率测试
测试目的：验证 ISMS 系统上报访问日志记录的错漏率
测试环境：现网环境

测试步骤:
1) 确认评测环境; 2) 登录 ISMS 系统, 确认访问日志功能正常; 3) 在正常业务流量背景下, 通过公网终端访问 IRCS 业务节点内应用资源 (客户站点或测试参考站) 至少 1 万次; 4) 登录 SMMS 系统, 下发访问日志查询指令, 根据 ISMS 系统上报的日志情况, 计算访问日志记录错漏率
预期结果:
在步骤 (4) 中, ISMS 系统上报至 SMMS 系统的访问日志记录错漏比例不高于 1%
判定原则:
应符合预期结果要求, 否则为不合格
备注:
访问日志记录错漏比例 = (1 - 访问行为发生 2h 后查询到的有效日志记录数 / 访问总量) × 100%

测试编号: 83
测试项目: 活跃资源监测记录错漏率测试
测试目的: 验证 ISMS 上报系统监测活跃资源的错漏率
测试环境: 现网环境
测试步骤:
1) 确认评测环境; 2) 在正常业务流量背景下, 通过公网终端访问特定 IP+端口 (或 IP+端口列表) 不少于 5000 次、特定域名 (或特定域名列表) 不少于 5000 次; 3) 登录 SMMS 系统, 下发 ISMS 系统活跃资源监测记录查询指令, 通过 ISMS 上报的活跃资源监测记录计算活跃资源监测记录访问量错漏率
预期结果:
在步骤 (4) 中, 要求 ISMS 系统上报活跃资源监测记录访问量的错漏比例应不高于 1%
判定原则:
应符合预期结果要求, 否则为不合格
备注:
活跃资源监测错漏率 = (1 - 活跃资源访问量监测结果 / 实际访问总量) × 100%

测试编号: 84
测试项目: ISMS 系统活动状态上报测试
测试目的: 验证 ISMS 定时向 SMMS 上报系统活动状态的功能
测试环境: 现网环境
测试步骤:
1) 确认评测环境; 2) 登录 ISMS 系统, 确认系统活动状态上报功能; 3) 登录 SMMS 系统, 在 SMMS 端查看 ISMS 系统上报的系统活动状态信息
预期结果:
在步骤 (3) 中, 成功查询 ISMS 系统上报的活动状态信息, 内容正确

判定原则： 应符合预期结果要求，否则为不合格
备注： 如果 SMMS 系统支持 ISMS 活动状态历史记录的查看功能，则可以通过该功能验证 ISMS 的稳定性

7.16 安全性要求测试

测试编号：85
测试项目：时钟同步测试
测试目的：验证 ISMS 系统时间同步功能
测试环境：现网环境
测试步骤： 1) 确认评测环境； 2) 登录 ISMS 系统，查看系统时钟同步设置； 3) 登录 SMMS 系统，查验系统各类数据、日志记录的时间戳
预期结果： 在步骤（3）中，ISMS 系统上报的各类数据、日志记录的时间戳与国家标准时间误差不超过 1s
判定原则： 应符合预期结果要求，否则为不合格

8 ISMS 接口测试

8.1 消息流程测试

测试编号：1
测试项目：ircs_command 消息接收测试
测试目的：验证系统接收正确 ircs_command 消息的功能
测试环境：测试环境
测试过程： 1) 按照测试环境图配置环境； 2) 通过 ircs_command 消息向被测系统发送正常管理指令； 3) 通过 ircs_command 消息向被测系统发送正常查询指令
预期结果： 被测系统能正常接收步骤（2）、步骤（3）中 ircs_command 消息
判定原则： 应符合预期结果要求，否则为不合格

测试编号：2
测试项目：ircs_command 响应消息发送测试
测试目的：验证系统对正确 ircs_command 消息及参数进行处理和响应的功能
测试环境：测试环境

测试过程： <ol style="list-style-type: none"> 1) 按照测试环境图配置环境； 2) 通过 ircs_command 消息向被测系统发送正常管理指令； 3) 通过 ircs_command 消息向被测系统发送正常查询指令
预期结果： <p>步骤 2)、步骤 3) 中受测系统能在同一会话中响应指令接收情况</p>
判定原则： <p>应符合预期结果要求，否则为不合格</p>

测试编号：3
测试项目：ircs_commandack 消息发送测试
测试目的：验证系统生成和发送 ircs_commandack 消息的功能
测试环境：测试环境
测试过程： <ol style="list-style-type: none"> 1) 按照测试环境图配置环境； 2) 通过 ircs_command 消息向被测系统发送正常管理指令，触发 ircs_commandack 消息
预期结果： <p>受测系统能在约定时间内发送 ircs_commandack 消息</p>
判定原则： <p>应符合预期结果要求，否则为不合格</p>

测试编号：4
测试项目：ircs_commandack 响应消息接收测试
测试目的：验证系统接收正确 ircs_commandack 响应消息的功能
测试环境：测试环境
测试过程： <ol style="list-style-type: none"> 1) 按照测试环境图配置环境； 2) 通过 ircs_command 消息向被测系统发送正常管理指令，触发 ircs_commandack 消息
预期结果： <p>受测系统能在发送 ircs_commandack 消息的同一会话中接收响应消息</p>
判定原则： <p>应符合预期结果要求，否则为不合格</p>

测试编号：5
测试项目：file_load 消息发送测试
测试目的：验证系统对 file_load 消息及参数构造和发送的功能
测试环境：测试环境
测试过程：

1) 按照测试环境图配置环境; 2) 触发 file_load 消息
预期结果: 被测系统能在约定时间内发送 file_load 消息
判定原则: 应符合预期结果要求, 否则为不合格

8.2 接口方法测试

测试编号: 6
测试项目: ircs_command 认证测试
测试目的: 验证系统 ircs_command 认证方法的功能
测试环境: 测试环境
测试过程: 1) 按照测试环境图配置环境; 2) 通过 ircs_command 消息向被测系统发送管理指令和查询指令
预期结果: 1) 被测系统能正常认证步骤 (2) 中 ircs_command 消息, 并在同一会话中响应指令接收情况; 2) 响应消息符合 YD/T 3214 《互联网资源协作服务信息安全管理系统接口规范》要求
判定原则: 应符合预期结果要求, 否则为不合格

测试编号: 7
测试项目: ircs_command 压缩测试
测试目的: 验证系统 ircs_command 压缩方法的功能
测试环境: 测试环境
测试过程: 1) 按照测试环境图配置环境; 2) 配置 ircs_command 压缩格式为无压缩; 3) 通过 ircs_command 消息向被测系统发送管理指令和查询指令; 4) 配置 ircs_command 压缩格式为 zip 压缩; 5) 重复步骤 (3)
预期结果: 1) 被测系统能正常校验步骤 (3)、步骤 (5) 中 ircs_command 消息, 并在同一会话中响应指令接收情况; 2) 响应消息符合 YD/T 3214 《互联网资源协作服务信息安全管理系统接口规范》要求
判定原则: 应符合预期结果要求, 否则为不合格
备注: 企业根据实际对接情况选择其中一种 ircs_command 的压缩格式测试即可

测试编号：8
测试项目：ircs_command 哈希测试
测试目的：验证系统 ircs_command 哈希方法的功能
测试环境：测试环境
测试过程： <ol style="list-style-type: none"> 1) 按照测试环境图配置环境； 2) 配置 ircs_command 哈希方式为无 hash； 3) 通过 ircs_command 消息向被测系统发送管理指令和查询指令； 4) 配置 ircs_command 哈希方式为 MD5； 5) 重复步骤（3）； 6) 配置 ircs_command 哈希方式为 SHA-1； 7) 重复步骤（3）
预期结果： <ol style="list-style-type: none"> 1) 被测系统能正常校验步骤（3）、步骤（5）、步骤（7）中 ircs_command 消息，并在同一会话中响应指令接收情况； 2) 响应消息符合 YD/T 3214《互联网资源协作服务信息安全管理系统接口规范》要求
判定原则： <p>应符合预期结果要求，否则为不合格</p>
备注： <p>企业根据实际对接情况选择其中一种 ircs_command 的哈希格式测试即可</p>

测试编号：9
测试项目：ircs_command 加密测试
测试目的：验证系统 ircs_command 加密方法的功能
测试环境：测试环境
测试过程： <ol style="list-style-type: none"> 1) 按照测试环境图配置环境； 2) 配置 ircs_command 加密方式为无加密； 3) 通过 ircs_command 消息向被测系统发送管理指令和查询指令； 4) 配置 ircs_command 加密方式为 AES； 5) 重复步骤（3）
预期结果： <ol style="list-style-type: none"> 1) 被测系统能正常校验步骤（3）、步骤（5）中 ircs_command 消息，并在同一会话中响应指令接收情况； 2) 响应消息符合 YD/T 3214《互联网资源协作服务信息安全管理系统接口规范》要求
判定原则： <p>应符合预期结果要求，否则为不合格</p>
备注： <p>企业根据实际对接情况选择其中一种 ircs_command 的加密方法测试即可</p>

测试编号：10
测试项目：ircs_commandack 认证测试
测试目的：验证系统 ircs_commandack 认证方法的功能
测试环境：测试环境
测试过程： <ol style="list-style-type: none"> 1) 按照测试环境图配置环境； 2) 通过 ircs_command 消息向被测系统发送管理指令，触发 ircs_commandack 消息
预期结果： <ol style="list-style-type: none"> 1) 步骤（2）后被测系统在约定时间内发送的 ircs_commandack 消息可正常认证； 2) ircs_commandack 消息符合 YD/T 3214《互联网资源协作服务信息安全管理系统接口规范》要求
判定原则： <p>应符合预期结果要求，否则为不合格</p>

测试编号：11
测试项目：ircs_commandack 哈希测试
测试目的：验证系统 ircs_commandack 哈希方法的功能
测试环境：测试环境
测试过程： <ol style="list-style-type: none"> 1) 按照测试环境图配置环境； 2) 配置 ircs_commandack 哈希方式是无 hash； 3) 通过 ircs_command 消息向被测系统发送管理指令，触发 ircs_commandack 消息； 4) 配置 ircs_commandack 哈希方式为 MD5； 5) 重复步骤（3）； 6) 配置 ircs_commandack 哈希方式为 SHA-1； 7) 重复步骤（3）
预期结果： <ol style="list-style-type: none"> 1) 步骤（3）、步骤（5）、步骤（7）后被测系统在约定时间内发送的 ircs_commandack 消息可正常校验； 2) ircs_commandack 消息符合 YD/T 3214《互联网资源协作服务信息安全管理系统接口规范》要求
判定原则： <p>应符合预期结果要求，否则为不合格</p>
备注： <p>企业根据实际对接情况选择其中一种 ircs_commandack 的哈希格式测试即可</p>

测试编号：12
测试项目：file_load 路径测试
测试目的：验证系统 file_load 路径
测试环境：测试环境
测试过程：

1) 按照测试环境图配置环境; 2) 通过 ircs_command 消息向被测系统发送各类型管理指令和查询指令, 触发 file_load 消息
预期结果: 1) 步骤 (2) 后被测系统能在约定时间内发送 file_load 消息; 2) file_load 存放文件路径符合 YD/T 3214 《互联网资源协作服务信息安全管理系统接口规范》要求
判定原则: 应符合预期结果要求, 否则为不合格

测试编号: 13
测试项目: file_load 压缩测试
测试目的: 验证系统 file_load 压缩方法的功能
测试环境: 测试环境
测试过程: 1) 按照测试环境图配置环境; 2) 配置 file_load 压缩格式为无压缩; 3) 通过 ircs_command 消息向被测系统发送管理指令和查询指令, 触发 file_load 消息; 4) 配置 file_load 压缩格式为 zip 压缩; 5) 重复步骤 (3)
预期结果: 1) 步骤 (3)、步骤 (5) 后被测系统在约定时间内发送 file_load 消息可正常校验; 2) file_load 消息符合 YD/T 3214 《互联网资源协作服务信息安全管理系统接口规范》要求
判定原则: 应符合预期结果要求, 否则为不合格
备注: 企业根据实际对接情况选择其中一种 file_load 的压缩方法测试即可

测试编号: 14
测试项目: file_load 哈希测试
测试目的: 验证系统 file_load 哈希方法的功能
测试环境: 测试环境
测试过程: 1) 按照测试环境图配置环境; 2) 配置 file_load 哈希格式为无 hash; 3) 通过 ircs_command 消息向被测系统发送管理指令和查询指令, 触发 file_load 消息; 4) 配置 file_load 哈希格式为 MD5; 5) 重复步骤 (3); 6) 配置 file_load 哈希格式为 SHA-1; 7) 重复步骤 (3)
预期结果:

1) 步骤（3）、步骤（5）后受测系统在约定时间内发送 file_load 消息可正常校验； 2) file_load 消息符合 YD/T 3214《互联网资源协作服务信息安全管理系统接口规范》要求
判定原则： 应符合预期结果要求，否则为不合格
备注： 企业根据实际对接情况选择其中一种 file_load 的哈希格式测试即可

测试编号：15
测试项目：file_load 加密测试
测试目的：验证系统 file_load 加密方法的功能
测试环境：测试环境
测试过程： 1) 按照测试环境图配置环境； 2) 配置 file_load 加密格式为无加密； 3) 通过 ircs_command 消息向受测系统发送管理指令和查询指令，触发 file_load 消息； 4) 配置 file_load 机密格式为 AES； 5) 重复步骤（3）
预期结果： 1) 步骤（3）、步骤（5）后受测系统在约定时间内发送 file_load 消息可正常校验； 2) file_load 消息符合 YD/T 3214《互联网资源协作服务信息安全管理系统接口规范》要求
判定原则： 应符合预期结果要求，否则为不合格
备注： 企业根据实际对接情况选择其中一种 file_load 的加密方法测试即可

8.3 健壮性测试

测试编号：16
测试项目：消息参数长度错误处理测试
测试目的：验证系统对各类参数长度存在错误的 ircs_command 消息进行处理的能力
测试环境：测试环境
测试过程： 1) 按照测试环境图 1 配置环境； 2) 配置参数长度存在错误的 ircs_command 消息； 3) 通过错误 ircs_command 消息向受测系统发送管理指令和查询指令
预期结果： 受测系统在步骤（3）中丢弃错误消息或回应消息错误提示信息
判定原则： 应符合预期结果要求，否则为不合格

测试编号：17
测试项目：消息参数内容错误处理测试
测试目的：验证系统各类参数内容存在错误的 ircs_command 消息进行处理的能力
测试环境：测试环境
测试过程： <ol style="list-style-type: none"> 1) 按照测试环境图 1 配置环境； 2) 配置参数内容存在错误的 ircs_command 消息； 3) 通过错误 ircs_command 消息向被测系统发送管理指令和查询指令
预期结果： <p>被测系统在步骤（3）中丢弃错误消息或回应消息错误提示信息</p>
判定原则： <p>应符合预期结果要求，否则为不合格</p>

测试编号：18
测试项目：消息响应超时处理测试
测试目的：验证系统对 ircs_commandack 响应消息超时的处理能力
测试环境：测试环境
测试过程： <ol style="list-style-type: none"> 1) 按照测试环境图配置环境； 2) 配置不响应被测系统 ircs_commandack 消息； 3) 通过 ircs_command 消息向被测系统发送正常管理指令，触发 ircs_commandack 消息
预期结果： <ol style="list-style-type: none"> 1) 被测系统在步骤（3）后，重新发送 ircs_commandack 消息； 2) ircs_commandack 消息符合 YD/T 3214《互联网资源协作服务信息安全管理系统接口规范》要求
判定原则： <p>应符合预期结果要求，否则为不合格</p>

测试编号：19
测试项目：重放消息处理测试
测试目的：验证系统接收到重放 ircs_command 消息的处理能力
测试环境：测试环境
测试过程： <ol style="list-style-type: none"> 1) 按照测试环境图配置环境； 2) 以重放的方式通过 ircs_command 消息向被测系统发送正常管理指令和查询指令
预期结果： <p>被测系统在步骤（2）中仅接受和处理一个 ircs_command 消息，丢弃其他重放消息或回应消息错误提示信息</p>
判定原则： <p>应符合预期结果要求，否则为不合格</p>

测试编号：20
测试项目：指令节点类型错误处理测试
测试目的：验证系统对接收到存在错误的指令进行处理的能力
测试环境：测试环境
测试过程： <ol style="list-style-type: none"> 1) 按照测试环境图配置环境； 2) 配置指令节点（和子节点）类型存在错误的 ircs_command 消息； 3) 通过错误 ircs_command 消息向被测系统发送管理指令和查询指令
预期结果： <p>被测系统在步骤（3）中丢弃错误消息或回应消息错误提示信息</p>
判定原则： <p>应符合预期结果要求，否则为不合格</p>

测试编号：21
测试项目：指令节点长度错误处理测试
测试目的：验证系统对接收到存在错误的指令进行处理的能力
测试环境：测试环境
测试过程： <ol style="list-style-type: none"> 1) 按照测试环境图配置环境； 2) 配置指令节点（和子节点）长度存在错误的 ircs_command 消息； 3) 通过错误 ircs_command 消息向被测系统发送管理指令和查询指令
预期结果： <p>被测系统在步骤（3）中丢弃错误消息或回应消息错误提示信息</p>
判定原则： <p>应符合预期结果要求，否则为不合格</p>

测试编号：22
测试项目：指令节点次序错误处理测试
测试目的：验证系统对接收到存在错误的指令进行处理的能力
测试环境：测试环境
测试过程： <ol style="list-style-type: none"> 1) 按照测试环境图配置环境； 2) 配置指令节点（和子节点）次序存在错误的 ircs_command 消息； 3) 通过错误 ircs_command 消息向被测系统发送管理指令和查询指令
预期结果： <p>被测系统在步骤（3）中丢弃错误消息或回应消息错误提示信息</p>
判定原则： <p>应符合预期结果要求，否则为不合格</p>

测试编号：23
测试项目：指令节点构成错误处理测试
测试目的：验证系统对接收到存在错误的指令进行处理的能力
测试环境：测试环境
测试过程： <ol style="list-style-type: none"> 1) 按照测试环境图配置环境； 2) 配置指令节点（和子节点）构成存在错误的 ircs_command 消息； 3) 通过错误 ircs_command 消息向被测系统发送管理指令和查询指令
预期结果： <p>被测系统在步骤（3）中丢弃错误消息或回应消息错误提示信息</p>
判定原则： <p>应符合预期结果要求，否则为不合格</p>

测试编号：24
测试项目：指令节点内容错误处理测试
测试目的：验证系统对接收到存在错误的指令进行处理的能力
测试环境：测试环境
测试过程： <ol style="list-style-type: none"> 1) 按照测试环境图配置环境； 2) 配置指令节点（和子节点）内容存在错误的 ircs_command 消息； 3) 通过错误 ircs_command 消息向被测系统发送管理指令和查询指令
预期结果： <p>被测系统在步骤（3）中丢弃错误消息或回应消息错误提示信息</p>
判定原则： <p>应符合预期结果要求，否则为不合格</p>