# **网络安全等级保护测评调研表**

**单位全称：XXX**

**项目联系人：XX X 电话：XXX 邮箱：XXX**

# **被测信息系统情况**

## 承载的业务情况

|  |
| --- |
| **被测对象** |
| **被测对象名称** | XXXX系统 | **业务信息安全等级（S）** | 第X级 |
| **系统服务安全等级（A）** | 第X级 |
| **备案编号** |  | **安全保护等级（G）** | 第X级 |
| **等级保护对象形态** | □传统IT系统 □云计算 □采用移动互联技术的系统□物联网 □工业控制系统 □大数据 □其他系统 |
| **被测对象描述** | 【填写说明：描述被测对象承载的业务、主要功能，以及采用云计算/移动互联/物联网/工业控制/大数据等技术情况，如果被测对象采用了多种新技术，则不同新技术应单独成段描述。】深圳市XXX系统，XX年投入使用，包括X台服务器、X台网络设备和X台安全设备。**深圳市XXX系统采用云计算/移动互联/物联网/工业控制/大数据技术，（若为未使用新技术，此句话不用描述**）是为深圳市XXX(系统简介)。 |

## 网络结构

【填写说明：给出被测对象的网络拓扑结构示意图，并基于示意图说明被测对象的网络结构基本情况，包括功能/安全区域划分、隔离与防护情况、关键网络和服务器设备的部署情况、功能简介、与其他系统的互联情况、边界设备、网络的管理方式和管理工具以及本地备份和灾备中心的情况等。】

XX信息系统部署在XX机房或者XX云上，通过XX防火墙、XXX数据库审计和XXX堡垒机等设备提供网络安全防护；通过XXX核心交换机实现网络通信；核心主机包括：XXX系统服务器，通过部署网络防火墙以及XXXX等设备实现较为严格的网络访问控制。具体拓扑如下：



图 2-1 深圳市XXX系统拓扑图

**备注：需注明网络出口（电信，电子资源政务中心、XXX等）**

# **系统构成**

### 2.1机房

【填写说明：以列表形式给出被测对象的部署机房。】

| **序号** | **机房名称** | **物理位置** | **重要程度** |
| --- | --- | --- | --- |
| 1 | 上梅林灾备机房 | 深圳市福田区梅坳四路深圳市信息网络中心 | 重要 |
| 2 | …… | …… | …… |

### 2.2网络设备

【填写说明：以列表形式给出被测对象中的网络设备（包括虚拟网络设备）。】

| **序号** | **设备名称** | **是否虚拟设备** | **系统及版本** | **品牌及型号** | **用途** | **重要****程度** | **备注** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | 华为交换机 | 否 | -- | 华为S9700 | 接入交换机 | 重要 | IP:192.168.1.1 |
| 2 | 交换机 | 否 | -- | 华为S5720-32X-EI-AC | 接入交换机 | 重要 | 无管理权限，由市大数据资源管理中心提供，不作为本系统资产。 |
| 3 | 交换机服务 | 否 | -- | 华为S5720-32X-EI-AC | 接入交换机 | 重要 | IP:192.168.1.1，由市政务云平台提供。 |
| 4 | 交换机服务 | 否 | -- | 华为S5720-32X-EI-AC | 接入交换机 | 重要 | 无管理权限，由市政务云平台提供，不作为本系统资产。 |
| 5 | …… | …… | …… | …… | …… | …… | …… |

### 2.3安全设备

【填写说明：以列表形式给出被测对象中的安全设备（包括虚拟安全设备）。】

| **序号** | **设备名称** | **是否虚拟设备** | **系统及版本** | **品牌及型号** | **用途** | **重要程度** | **备注** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | 华为防火墙 | 否 | -- | 华为XXX | 策略限制、访问控制 | 重要 | IP:192.168.1.1 |
| 2 | 华为防火墙 | 否 | -- | 华为XXX | 策略限制、访问控制 | 重要 | 无管理权限，由市大数据资源管理中心提供，不作为本系统资产。 |
| 3 | 华为防火墙 | 否 | -- | 华为XXX | 策略限制、访问控制 | 重要 | IP:192.168.1.1，由市政务云平台提供。 |
| 4 | 华为防火墙 | 否 | -- | 华为XXX | 策略限制、访问控制 | 重要 | 无管理权限，由市政务云平台提供，不作为本系统资产。 |
| 5 | …… | …… | …… | …… | …… | …… | …… |

### 2.4服务器/存储设备

【填写说明：以列表形式给出被测对象中的服务器和存储设备（包括虚拟设备）。此列表中仅包含具备管理权限的设备，不具备管理权限的设备不列入此表。

若采用云计算技术，必须调研宿主机、云管理服务器、云应用服务器，可不以此命名，但必须在备注中说明用途。

】

| **序号** | **设备名称** | **所属业务应用系统/平台名称** | **是否虚拟设备** | **操作系统及版本** | **数据库管理系统及版本** | **中间件及版本** | **重要程度** | **备注** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | 应用服务器1 | XX系统 | 否 | WINDOWS SERVER 2012 R2 | -- | IIS 7 | 重要 | IP:192.168.1.1 |
| 2 | 数据库服务器2 | XX平台 | 是 | Linux CentOS7.2 | ORACLE 12C | -- | 重要 | IP:192.168.1.1 |
| 3 | 计算节点KVM216 | 云平台 | 否 | EulerOS V1 | -- | -- | 重要 | IP:192.168.1.1，宿主机 |
| 4 | 监控服务器 | 云平台 | 否 | EulerOS V1 | gaussdb | NGINX | 重要 | IP:192.168.1.1 |
| 5 | 云管理服务器 | ManageOne运维面（OC） | 否 | EulerOS V1 | gaussdb | NGINX | 重要 | IP:192.168.1.1 |
| 6 | 云应用服务器 | ManageOne运营面（SC） | 否 | EulerOS V1 | gaussdb | NGINX | 重要 | IP:192.168.1.1 |
| 7 | …… | …… | …… | …… | …… | …… | …… | …… |

### 2.5终端/现场设备

【填写说明：以列表形式给出被测对象中的终端，包括业务终端、运维终端、管理终端和现场设备等，如果使用了移动终端，列出移动终端。】

| **序号** | **设备名称** | **是否虚拟设备** | **操作系统/控制软件及版本** | **设备类别/用途** | **重要程度** | **备注** |
| --- | --- | --- | --- | --- | --- | --- |
| 1 | 运维终端1 | 否 | WINDOWS 10 | 运维 | 重要 | IP:192.168.1.1 |
| 2 | …… | …… | …… | …… | …… | …… |

### 2.6系统管理软件/平台

【填写说明：以列表的形式给出被测对象中的系统管理类软件或平台，包括数据库、中间件、网管软件/平台、安管软件/平台、云计算管理软件/平台等。

若采用云计算技术，必须调研云计算安全管理系统（例如ManageOne部署面（管理侧），用来监测系统资源、备份等安全相关管理的系统）、数据库管理系统（支撑云计算平台自身的数据库）、中间件（支撑云计算平台自身的中间件）】

| **序号** | **系统管理软件/平台名称** | **所在设备名称** | **版本** | **主要功能** | **重要程度** | **备注** |
| --- | --- | --- | --- | --- | --- | --- |
| 1 | gaussdb | 监控服务器、云管理服务器、云应用服务器 | V1 | 数据库管理系统 | 重要 | -- |
| 2 | NGINX | 监控服务器、云管理服务器、云应用服务器 | V1 | 中间件 | 重要 | -- |
| 3 | 虚拟化服务平台 | 虚拟化服务器 | V1 | 虚拟化服务平台，是基于网络的虚拟化解决方案，客户可以集中管理存储池，并在不同的服务器环境中创建存储资源虚拟卷。 | 重要 | -- |
| 4 | 态势感知系统 | 云管理服务器 | V1 | 态势感知系统，用于掌控网络实况全局,采集安全数据,分析预测风险,危险预警溯源等 | 重要 | 无管理权限，由XX提供，不作为本系统资产等内容。 |
| 5 | …… | …… | …… | …… | …… | …… |

### 2.7业务应用系统/平台

【填写说明：以列表的形式给出被测对象中的业务应用系统（包括服务器端和客户端软件等应用软件）。】

| **序号** | **业务应用系统/平台名称** | **主要功能** | **业务应用软件及版本** | **开发厂商** | **重要程度** |
| --- | --- | --- | --- | --- | --- |
| 1 | ManageOne运维面（OC） | 日常运维管理，包括：运维工具箱、集群管理、工单系统、操作审计以及流程单管理等内容。 | V1 | 腾讯 | 重要 |
| 2 | ManageOne运营面（SC） | 为客户提供资源申请、资源生命周期管理，包括：虚拟机管理、物理机、弹性伸缩等内容的管理。 | V1 | 腾讯 | 重要 |
| 3 | ManageOne部署面（管理侧） | 提供自动化配置部署、可视化故障诊断、智能化容量分析、安全业务的编排和管理云化和虚拟化环境的备份软件，基于虚拟机/磁盘快照、CBT和快照比对技术等安全管理相关功能 | V1 | 腾讯 | 重要 |
| 4 | XX系统 | 简介 | V1 | 腾讯 | 重要 |
| 5 | …… | …… | …… | …… | …… |

### 2.8数据类别

【填写说明：以列表形式描述具有相近业务属性和安全需求的数据集合。】

| **序号** | **数据类别[[1]](#footnote-1)** | **所属业务应用** | **安全防护需求[[2]](#footnote-2)** |
| --- | --- | --- | --- |
| 1 | 业务数据 | XX系统 | 保密性、完整性 |
| 2 | 鉴别数据 | XX系统 | 保密性、完整性 |
| 3 | 管理信息 | XX系统 | 保密性、完整性 |
| 4 | …… | …… | …… |

【填写说明：大数据测评对象采用表- 8- b数据类别，非大数据测评对象无需填写此表】

| **序号** | **数据类别** | **数据级别** | **安全防护需求** | **所属业务应用** |
| --- | --- | --- | --- | --- |
| **数据采集** | **数据存储** | **数据处理** | **数据应用** | **数据流动** | **数据销毁** |
| 1 | 政务 | 敏感 | 保密性、完整性 | XX模块 | XX子系统 | XX模块 | XX子系统 | XX模块 | XX子系统 |
| 2 | …… | …… | …… | …… | …… | …… | …… | …… | …… |

### 2.9安全相关人员

【填写说明：以列表形式给出与被测对象安全相关的人员情况。相关人员包括（但不限于）安全主管、系统建设负责人、系统运维负责人、网络（安全）管理员、主机（安全）管理员、数据库（安全）管理员、应用（安全）管理员、软件开发人员、机房管理人员、资产管理员、业务操作员、安全审计人员、数据（安全）管理员等。】

| **序号** | **姓名** | **岗位/角色** | **联系方式** |
| --- | --- | --- | --- |
| 1 | 刘一 | 安全主管 | 13800138000 |
| 2 | 陈二 | 系统运维负责人 | 13800138001 |
| 3 | 张三 | 网络（安全）管理员 | 13800138002 |
| 4 | 李四 | 主机（安全）管理员 | 13800138003 |
| 5 | 王五 | 数据库（安全）管理员 | 13800138004 |
| 6 | 赵六 | 应用（安全）管理员 | 13800138005 |
| 7 | 孙七 | 软件开发人员 | 13800138006 |
| 8 | 周八 | 机房管理员 | 13800138007 |
| 9 | 吴九 | 资产管理员 | 13800138008 |
| 10 | 郑十 | 业务操作员 | 13800138009 |
| 11 | 刘十一 | 安全审计员 | 13800138010 |
| 12 | 陈十二 | 数据（安全）管理员 | 13800138011 |
| 13 | …… | …… | …… |

### 2.10安全管理文档

【填写说明：以列表形式给出与被测对象安全相关的文档，包括主要安全管理类文档、记录类文档和其他文档。】

| **序号** | **文档名称** | **主要内容** |
| --- | --- | --- |
| 1 | 《深圳市XXX局计算机网络保密管理办法》 | 内网计算机维修、报废、软硬件、IP管理 |
| 2 | 《关于成立深圳市XXX局信息安全管理领导小组的决定》 | 明确小组成员及成员工作职责 |
| 3 | 《深圳市XXX局信息公开保密审查制度》 | 公开保密审查流程，防止保密信息泄露 |
| 4 | 《市XXX局中心机房管理制度》 | 机房日常、设备、系统软件、计算机病毒防范管理，数据保密及数据备份，管理员职责，计算机使用和管理制度 |
| 5 | 《深圳市XXX局信息安全、网络安全突发事件的应急处置预案》 | 组织指挥体系及职责、预防和预警机制、应急响应，宣传、培训、审查、监控 |
| 6 | 《深圳市XXX局网站管理暂行办法》 | 网站日常维护和管理，网站安全、监督与考核 |

# **扫描**

### 3.1主机扫描

 采用绿盟极光对服务器、网络设备、数据库等进行主机扫描，发现服务器操作系统、数据库版本漏洞、系统补丁、弱口令等安全漏洞。

原始报告可另附。

### 3.2应用层扫描

 采用Appscan对系统进行应用层扫描，发现系统由于编码习惯，插件版本等存在的漏洞，可发现各种CGI 漏洞、SQL注入，跨站脚本，敏感信息泄漏。

 原始报告可另附。

1. 主要描述业务数据类型，如用户数据、行情数据、交易数据等，如果必要可从安全防护需求（保密、完整等）的角度进一步细分。 [↑](#footnote-ref-1)
2. 保密性和完整性等。 [↑](#footnote-ref-2)