报告编号：XXXXXXXXXXX-XXXXX-XX-XXXX-XX

网络安全等级保护
[被测对象名称]等级测评报告

被测单位：_____

测评单位：_____

报告时间：_____年_____月_____

说明：

一、每个备案系统单独出具测评报告。

二、测评报告编号为四组数据。各组含义和编码规则如下:

第一组为系统备案表编号，由 2 段 16 位数字组成，可以从公安机关颁发的系统备案证明（或备案回执）上获得。第 1 段即备案证明编号的前 11 位（前 6 位为受理备案公安机关代码，后 5 位为受理备案的公安机关给出的备案单位的顺序编号)；第 2 段即备案证明编号的后 5 位（系统编号)。

第二组为年份，由 2 位数字组成。例如 09 代表 2009 年。

第三组为机构代码，由网络安全等级测评与检测评估机构服务认证证书编号最后四位数字组成。

第四组为本年度系统测评次数，由两位构成。例如 02 表示该系统本年度测评 2 次。

网络安全等级测评基本信息表

被测对象				
被测对象名称		安全保护等级		
备案证明编号				
被测单位				
单位名称				
单位地址			邮政编码	
联系人	姓名		职务/职称	
	所属部门		办公电话	
	移动电话		电子邮件	
测评单位				
单位名称	公安部信息安全等级保护评估中心		机构代码	SC202127130010001
单位地址	北京市海淀区阜成路 58 号新洲商务大厦 7 层		邮政编码	100142
联系人	姓名	张宇翔	职务/职称	副主任
	所属部门	评估中心	办公电话	010-51607592
	移动电话	——	电子邮件	zhang_yuxiang@cspec.org.cn
审核批准	编制人	（签字）	编制日期	
	审核人	（签字）	审核日期	
	批准人	（签字）	批准日期	

声明

【填写说明：声明是测评机构对测评报告的有效性前提、测评结论的适用范围以及使用方式等有关事项的陈述，测评机构可参考以下建议书写内容编制。】

本报告是[被测对象名称]的等级测评报告。

本报告测评结论的有效性建立在被测评单位提供相关证据的真实性基础之上。

本报告中给出的测评结论仅对被测对象当时的安全状态有效。当测评工作完成后，由于被测对象发生变更而涉及到的系统构成组件（或子系统）本报告不再适用。

本报告中给出的测评结论不能作为对被测对象内部部署的相关系统构成组件（或产品）的测评结论。

在任何情况下，若需引用本报告中的测评结果或结论都应保持其原有的意义，不得对相关内容擅自进行增加、修改和伪造或掩盖事实。

单位名称（加盖单位公章或等级测评业务专用章）

年　　月

等级测评结论

【填写说明：表项“第 *z* 级（S*x*A*y*）”中，“第 *z* 级”表示被测对象的安全保护等级，“*z*”的取值为（一、二、三、四或五）；“S*x*”和“A*y*”分别表示被测对象的业务信息和系统服务安全保护等级，*x* 和 *y* 的取值为（1、2、3、4 或 5），如第三级（S3A3）。如果被测对象由独立定级的云计算平台或大数据平台提供平台支撑，或者自身为独立定级的云计算平台或大数据平台，则需填写等级测评结论扩展表（云计算安全）或等级测评结论扩展表（大数据安全），否则删除等级测评结论扩展表。】

<table>
<tr><th colspan="4">测评结论和综合得分</th></tr>
<tr><td>被测对象名称</td><td></td><td>安全保护等级</td><td>第 z 级（SxAy）</td></tr>
<tr><td>扩展要求
应用情况</td><td colspan="3">☐云计算 ☐移动互联 ☐物联网
☐工业控制系统 ☐大数据</td></tr>
<tr><td>被测对象描述</td><td colspan="3">【填写说明：简要描述被测对象承载的业务功能等基本情况，以及被测对象安全技术情况和安全管理情况，建议不超过 400 字】</td></tr>
<tr><td>安全状况描述</td><td colspan="3">【填写说明：根据实际测评情况简要描述被测对象的整体安全状况，包括最主要的中高风险安全问题及数量和等级结论，建议不超过 400 字】</td></tr>
<tr><td>等级测评结论</td><td>【填写说明：除填写测评结论外，还需加盖测评机构单位公章或等级测评业务专用章】</td><td>综合得分</td><td></td></tr>
</table>

等级测评结论扩展表（云计算安全）

【填写说明】

1、“被测对象云计算形态”用于明确被测对象是云计算平台还是云服务客户业务应用系统，此处为单选。“被测对象采用的云计算服务模式”用于描述被测对象所采用的云计算服务模式，此处为单选。当云计算形态为云服务客户业务应用系统时，“云计算平台名称”填写该被测对象所使用的云计算平台名称。

2、“云计算平台服务能力描述”给出了当前服务模式下云计算平台为云服务客户提供的服务能力符合情况，以及云计算平台的等级测评结论和综合得分。需要注意的是，表中以第四级为例给出了云计算安全扩展主要要求，测评机构应根据被测对象安全保护等级情况，参照表中内容给出相应等级的云计算安全扩展主要要求。

3、如果云服务客户业务应用系统同时部署在不同模式的云计算平台上时，可以使用多个使用等级测评结论扩展表（云计算安全）来展示。

【说明结束】

<table>
<tr><th colspan="4">等级测评结论扩展表（云计算安全）</th></tr>
<tr><td>被测对象
云计算形态</td><td colspan="3">☐云计算平台
☐云服务客户业务应用系统（平台报告编号：_____）
【填写说明：填写该云服务客户业务应用系统在当前服务模式下所使用的云计算平台的等级测评报告编号。】</td></tr>
<tr><td>云计算平台
名称</td><td></td><td>被测对象采用的
云计算服务模式</td><td>☐ IaaS
☐ PaaS
☐ SaaS</td></tr>
<tr><th colspan="4">云计算平台服务能力描述</th></tr>
<tr><th colspan="3">云计算安全扩展主要要求</th><th>符合情况</th></tr>
</table>

网络架构	b)应实现不同云服务客户虚拟网络之间的隔离；	
	c)应具有根据云服务客户业务需求提供通信传输、边界防护、入侵防范等安全机制的能力；	
	e)应提供开放接口或开放性安全服务，允许云服务客户接入第三方安全产品或在云计算平台选择第三方安全服务；	
	f)应提供对虚拟资源的主体和客体设置安全标记的能力,保证云服务客户可以依据安全标记和强制访问控制规则确定主体对客体的访问；	
	g) 应提供通信协议转换或通信协议隔离等的数据交换方式，保证云服务客户可以根据业务需求自主选择边界数据交换方式；	
入侵防范	a)应能检测到云服务客户发起的网络攻击行为，并能记录攻击类型、攻击时间、攻击流量等；	
安全审计	b)应保证云服务商对云服务客户系统和数据的操作可被云服务客户审计。	
数据完整性和保密性	c)应使用校验技术或密码技术保证虚拟机迁移过程中重要数据的完整性，并在检测到完整性受到破坏时采取必要的恢复措施；	
	d)应支持云服务客户部署密钥管理解决方案，保证云服务客户自行实现数据的加解密过程。	
数据备份恢复	b)应提供查询云服务客户数据及备份存储位置的能力；	
	d)应为云服务客户将业务系统及数据迁移到其他云计算平台和本地系统提供技术手段，并协助完成迁移过程。	
剩余信息保护	b)云服务客户删除业务应用数据时，云计算平台应将云存储中所有副本删除。	
云服务商选择	a)应选择安全合规的云服务商，其所提供的云计算平台应为其所承载的业务应用系统提供相应等级的安全保护能力；	
	b)应在服务水平协议中规定云服务的各项服务内容和具体技术指标；	
供应链管理	b)应将供应链安全事件信息或安全威胁信息及时传达到云服务客户；	
云计算平台等级测评结论		云计算平台综合得分

等级测评结论扩展表（大数据安全）

【填写说明】

1、“被测对象大数据形态”用于明确被测对象的大数据形态是否包括大数据平台、大数据应用或大数据资源，此处为多选。当大数据形态为大数据应用或大数据资源时，“大数据平台名称”填写承载大数据业务所使用的大数据平台名称。

2、“大数据平台服务能力描述”给出了大数据平台的服务能力符合情况，以及大数据平台的等级测评结论和综合得分。需要注意的是，表中以第四级为例给出了大数据安全扩展主要要求，测评机构应根据被测对象安全保护等级情况，参照表中内容给出相应等级的大数据安全扩展主要要求。

【说明结束】

等级测评结论扩展表（大数据安全）		
被测对象大数据形态	☐大数据平台 ☐大数据应用（平台报告编号：_____） ☐大数据资源（平台报告编号：_____） 【填写说明：当大数据资源或大数据应用采用大数据平台提供方提供平台支撑时，平台报告编号为该大数据平台的等级测评报告编号。】	
大数据平台名称		
大数据平台服务能力描述		
大数据安全扩展主要要求		符合情况
数据隔离	b) 应保证大数据平台的管理流量与系统业务流量分离。	
	g) 对外提供服务的大数据平台，平台或第三方只有在大数据应用授权下才可以对大数据应用的数据资源进行访问、使用和管理；	
	n) 大数据平台应保证不同客户大数据应用的审计数据隔离存放；	
静态脱敏和	f) 大数据平台应提供静态脱敏和去标识化的工具或服务组件	

去标识化	技术；	
安全审计	n) 大数据平台应提供不同客户审计数据收集汇总和集中分析的能力；	
访问控制	i) 大数据平台应提供设置数据安全标记功能，基于安全标记的授权和访问控制措施，满足细粒度授权访问控制管理能力要求；	
数据分类分级的标识	h) 大数据平台应提供数据分类分级安全管理功能，供大数据应用针对不同类别级别的数据采取不同的安全保护措施；	
	j) 大数据平台应在数据采集、存储、处理、分析等各个环节，支持对数据进行分类分级处置，并保证安全保护策略保持一致；	
	o) 大数据平台应具备对不同类别、不同级别数据全生命周期区分处置的能力。	
数据溯源	m) 应跟踪和记录数据采集、处理、分析和挖掘等过程，保证溯源数据能重现相应过程，溯源数据满足合规审计要求；	
资源管理	c) 大数据平台应为大数据应用提供集中管控其计算和存储资源使用状况的能力；	
	e) 大数据平台应屏蔽计算、内存、存储资源故障，保障业务正常运行；	
大数据平台等级测评结论		**大数据平台综合得分**

总体评价

【填写说明：根据被测对象测评结果和测评过程中了解的相关信息，从安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心、安全管理制度、安全管理机构、安全人员管理、安全建设管理和安全运维管理十个安全类分别评价描述被测对象的安全保护状况，并给出被测对象的等级测评结论。】

主要安全问题及整改建议

【填写说明：描述被测对象存在的主要安全问题，并针对主要安全问题提出整改建议。测评机构可参考以下示例编制。】

经过单项测评结果判定和整体测评发现，[被测对象名称]存在的主要问题及整改建议如下：

一、安全物理环境方面

（1）问题 1 描述

整改建议：整改建议描述

（2）问题 2 和问题 3 描述

整改建议：整改建议描述

二、安全通信网络方面

三、安全区域边界方面

四、安全计算环境方面

五、安全管理中心方面

六、安全管理制度方面

七、安全管理机构方面

八、安全人员管理方面

九、安全建设管理方面

十、安全运维管理方面

目录

1 测评项目概述

【格式说明】

（1） 正文：华文仿宋和 Times New Roman，小四，1.5 倍行距。

（2） 标题：中文第一级标题为三号黑体加粗，其他标题为四号黑体加粗，西文为 Times New Roman。

（3） 表格：华文仿宋和 Times New Roman，五号，单倍行距。

（4） 页眉页脚：华文仿宋和 Times New Roman，加粗，小五，单倍行距。

（5） 注意首页不同，不使用 Word 兼容格式，容易造成格式混乱。

（6） 全文段前段后为 0（包括所有标题）。

（7） 全文页码序号分为 2 部分，正文和前面一部分。

（8） 表格和插图有题注。

（9） 所有正文中涉及数字序号为（1），不是半括号 1）。

（10） 全文页眉页脚格式正确。报告完成后检查最后一页的页码，更新目录。

1.1 测评目的

【填写说明：简述测评项目背景、委托单位和项目目标等内容。】

1.2 测评依据

【填写说明：分类列出开展测评活动所依据的标准、文件和合同等。下面列出了等级测评过程中主要依据的标准，测评机构可根据实际情况进行补充。如果标准编号的年份发生变化，以最新年份为准。】

测评过程中主要依据的标准：

（1） GB 17859—1999 《计算机信息系统 安全保护等级划分准则》

（2） GB/T 22239—2019 《信息安全技术 网络安全等级保护基本要求》（以下简称《基本要求》）

（3） GB/T 28448—2019 《信息安全技术 网络安全等级保护测评要求》

（4） GB/T 28449—2018 《信息安全技术 网络安全等级保护测评过程指南》

（5） GB/T 20984—2007 《信息安全技术 信息安全风险评估规范》

1.3 测评过程

【填写说明：应根据实际测评情况描述等级测评工作流程、各阶段完成的关键任务和工作时间节点等内容。】

1.4 报告分发范围

【填写说明：说明等级测评报告正本的份数与分发范围。】

2 被测对象描述

2.1 被测对象概述

2.1.1 定级结果

【填写说明：被测对象应为已定级备案的对象，并将被测对象的定级结果填入下表。】

表 2-1 定级结果

被测对象名称	安全保护等级	业务信息安全保护等级	系统服务安全保护等级

2.1.2 业务和采用的技术

【填写说明：描述被测对象承载的业务和主要功能，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。】

2.1.3 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，包括安全区域划分、隔离与防护情况、关键网络和服务器设备部署情况、与其他系统互联情况，以及网络管理方式和管理工具、本地备份和灾备中心情况等。】

2.2 测评指标

2.2.1 安全通用要求指标

【填写说明：根据被测对象的安全保护等级，选择《基本要求》中对应级别的安全通用要求作为等级测评的指标，以表格形式在下表中列出。】

表 2-2 安全通用要求指标

安全类[1]	控制点[2]	测评项数

2.2.2 安全扩展要求指标

【填写说明：描述采用移动互联技术、云计算技术的被测对象，以及物联网、工业控制系统、大数据等特殊类型的被测对象，选择《基本要求》中对应级别的安全扩展要求作为等级测评的指标，以表格形式在下表中列出。】

表 2-3 安全扩展要求指标

扩展类型	安全类	控制点	测评项数
云计算安全扩展要求			
……			

2.2.3 其他安全要求指标

【填写说明：结合被测评单位要求、被测对象的实际安全需求，以及安全最佳实践经验，以列表形式给出《基本要求》未覆盖或者高于被测对象安全保护等级的安全要求，如行业标准等。】

表 2-4 其他安全要求指标

安全类	控制点	测评项数

[1] 安全类对应《基本要求》中的安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心、安全管理制度、安全管理机构、安全管理人员、安全建设管理和安全运维管理。

[2] 控制点是对安全类的进一步细化，对应《基本要求》目录级别中安全类的下一级目录。

2.2.4 不适用安全要求指标

【填写说明：鉴于被测对象的复杂性和特殊性，《基本要求》中的某些要求项可能不适用于所有测评对象，对于这些不适用项应在下表中给出不适用原因。如果单个要求项不适用某个测评对象，应在该测评对象的测评结果记录中说明不适用原因，不用在下表中列出。】

表 2-5 不适用安全要求指标

安全类	控制点	不适用项	不适用原因

2.3 测评对象

2.3.1 测评对象选择方法

【填写说明：依据 GB/T 28449—2018 中测评对象确定原则和方法，结合资产重要程度赋值结果（重要程度赋值为关键、重要和一般），描述本报告中测评对象的选择方法和结果。】

2.3.2 测评对象选择结果

2.3.2.1 物理机房

表 2-6 物理机房

序号	机房名称	物理位置	重要程度

2.3.2.2 网络设备

表 2-7 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

2.3.2.3 安全设备

表 2-8 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

2.3.2.4 服务器

表 2-9 服务器

序号	设备名称	所属业务应用系统/平台	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

2.3.2.5 终端设备

表 2-10 终端设备

序号	设备名称	是否虚拟设备	操作系统及版本	用途	重要程度

2.3.2.6 其他系统或设备

表 2-11 其他系统或设备

序号	设备名称	是否虚拟设备	系统及版本	设备类别/用途	重要程度

2.3.2.7 系统管理软件/平台

表 2-12 系统管理软件/平台

序号	系统管理软件/平台名称	主要功能	版本	所在设备名称	重要程度

2.3.2.8 业务应用系统/平台

表 2-13 业务应用系统/平台

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

2.3.2.9 数据资源

【填写说明:测评对象选择需要覆盖各级各类的数据,并重点关注重要业务数据、个人敏感信息和鉴别数据等。】

表 2-14-a 数据资源

序号	数据类别	所属业务应用	安全防护需求	重要程度

【填写说明：当被测对象为大数据平台/应用/资源时，测评对象选择需要覆盖各级各类的数据，并重点关注重要业务数据、个人敏感信息、鉴别数据、溯源数据等，因此大数据安全测评时采用下表。】

表 2-14-b 数据资源

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

2.3.2.10 安全相关人员

表 2-15 安全相关人员

序号	姓名	岗位/角色	联系方式	所属单位

2.3.2.11 安全管理文档

表 2-16 安全管理文档

序号	文档名称	主要内容

3 单项测评结果分析

【填写说明：以下段落为建议书写内容，测评机构可根据情况进行调整。】

单项测评内容包括“2.2.1 安全通用要求指标”、“2.2.2 安全扩展要求指标”和“2.2.3 其他安全要求指标”中涉及的安全类，由已有安全控制措施汇总分析和主要安全问题汇总分析两部分构成，单项测评结果汇总、单项测评结果记录参见报告附录。

3.1 安全物理环境

3.1.1 已有安全控制措施汇总分析

【填写说明：针对测评结果中存在的符合项进行汇总和分析，建议按照控制点对被测对象采用的安全保护措施及其达到的效果等进行详细描述。】

3.1.2 主要安全问题汇总分析

【填写说明：针对测评结果中存在的部分符合项和不符合项进行汇总和分析，描述主要安全问题及其关联对象，形成被测对象的主要安全问题描述。全部安全问题描述参见 3.13.2。】

3.2 安全通信网络

3.2.1 已有安全控制措施汇总分析

3.2.2 主要安全问题汇总分析

3.3 安全区域边界

3.3.1 已有安全控制措施汇总分析

3.3.2 主要安全问题汇总分析

3.4 安全计算环境

3.4.1 网络设备

【填写说明：网络设备、安全设备、服务器、终端、系统管理软件/平台和业务应用系统等所涉及的鉴别数据和重要配置数据分别在对应测评对象中汇总测评证据，包括数据完整性、数据保密性和备份恢复。】

3.4.1.1 已有安全控制措施汇总分析

3.4.1.2 主要安全问题汇总分析

3.4.2 安全设备

3.4.2.1 已有安全控制措施汇总分析

3.4.2.2 主要安全问题汇总分析

3.4.3 服务器和终端

3.4.3.1 已有安全控制措施汇总分析

3.4.3.2 主要安全问题汇总分析

3.4.4 系统管理软件/平台

3.4.4.1 已有安全控制措施汇总分析

3.4.4.2 主要安全问题汇总分析

3.4.5 业务应用系统/平台

3.4.5.1 已有安全控制措施汇总分析

3.4.5.2 主要安全问题汇总分析

3.4.6 数据资源

【填写说明：数据一般包括鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要个人信息和大数据资源等，这些数据分布在不同的测评对象上，应针

对不同类型数据分别从不同测评对象上汇总测评证据。本节只汇总应用系统涉及的重要业务数据、重要个人信息和大数据资源的测评证据，包括数据完整性、数据保密性、剩余信息保护、数据备份恢复和个人信息保护等。网络设备、安全设备、服务器、终端、系统管理软件/平台和业务应用系统等所涉及的鉴别数据和重要配置数据分别在对应测评对象中汇总测评证据，包括数据完整性、数据保密性和数据备份恢复。重要审计数据在安全管理中心进行汇总测评证据，包括数据完整性。】

3.4.6.1 已有安全控制措施汇总分析

3.4.6.2 主要安全问题汇总分析

3.4.7 其他系统或设备

3.4.7.1 已有安全控制措施汇总分析

3.4.7.2 主要安全问题汇总分析

3.5 安全管理中心

【填写说明：数据一般包括鉴别数据、重要业务数据、重要审计数据、重要配置数据和重要个人信息及大数据等，这些数据分布在不同的测评对象上，应针对不

同类型数据分别从不同测评对象上汇总测评证据。重要审计数据在安全管理中心进行汇总测评证据，包括数据完整性。】

3.5.1 已有安全控制措施汇总分析

3.5.2 主要安全问题汇总分析

3.6 安全管理制度

3.6.1 已有安全控制措施汇总分析

3.6.2 主要安全问题汇总分析

3.7 安全管理机构

3.7.1 已有安全控制措施汇总分析

3.7.2 主要安全问题汇总分析

3.8 安全管理人员

3.8.1 已有安全控制措施汇总分析

3.8.2 主要安全问题汇总分析

3.9 安全建设管理

3.9.1 已有安全控制措施汇总分析

3.9.2 主要安全问题汇总分析

3.10 安全运维管理

3.10.1 已有安全控制措施汇总分析

3.10.2 主要安全问题汇总分析

3.11 其他安全要求指标

3.11.1 已有安全控制措施汇总分析

3.11.2 主要安全问题汇总分析

3.12 验证测试

【填写说明：验证测试包括漏洞扫描、渗透测试等。本章节仅列出验证测试的汇总类结果，详细验证测试结果参见报告附录。】

3.12.1 漏洞扫描

3.12.1.1 漏洞扫描结果统计

【填写说明：描述漏洞扫描工具的名称及其系统版本和规则库版本，给出漏洞扫描工具接入示意图和相关接入点说明。】

（1）接入点 X 漏洞扫描结果统计

【填写说明：按照下表对漏洞扫描结果进行汇总，详细漏洞扫描结果记录描述参见报告附录。】

接入点 X 的漏洞扫描结果汇总如下表所示。

表 3-1 接入点 X 漏洞扫描结果汇总表

序号	设备名称	系统及版本	安全漏洞数量			
			高	中	低	小计

3.12.1.2 漏洞扫描问题描述

【填写说明：针对系统漏洞扫描或 Web 漏洞扫描结果进行分析，汇总被测对象存在的安全漏洞。严重程度结果为“高”、“中”或“低”。如果被测对象存在的安全漏洞较多，可只描述主要的安全漏洞（如高危安全漏洞）。全部安全漏洞描述参见报告附录。】

通过对漏洞扫描结果进行分析，[被测对象名称]存在的主要安全漏洞汇总如下表所示。

表 3-2 主要安全漏洞汇总表

序号	安全漏洞名称	关联资产/域名	严重程度

3.12.2渗透测试

【本次测评若果未对网络设备、安全设备、服务器操作系统和应用系统等进行渗透测试，请提供特殊说明材料，以图片方式提供，说明文件需要有签字、盖章和日期。】

3.12.2.1 渗透测试过程说明

【填写说明：简要描述渗透测试的工具、方法和过程等。】

3.12.2.2 渗透测试问题描述

【填写说明：针对渗透测试发现的安全问题进行汇总描述，详细渗透测试过程记录描述参见报告附录。严重程度结果为“高”、“中”或“低”。】

通过渗透测试发现，[被测对象名称]存在的安全问题汇总如下表所示。

表 3-3 渗透测试结果汇总表

序号	安全问题	关联资产/域名	严重程度

3.13 单项测评小结

3.13.1 控制点符合情况汇总

【填写说明：根据单项测评结果汇总控制点符合情况，符合情况填写“√”。】

根据单项测评结果汇总控制点符合情况如下表所示。

表 3-4 控制点符合情况汇总表

序号	通用/扩展	安全类	控制点	控制点符合情况		
				符合	部分符合	不符合
控制点符合情况数量统计						

3.13.2 安全问题汇总

【填写说明：根据单项测评结果汇总安全问题，各安全类中同一安全问题所关联的测评对象应进行合并。下表可根据实际情况设置为纵向或横向。】

针对单项测评结果中存在的部分符合项和不符合项进行汇总，形成安全问题如下表所示。

表 3-5 安全问题汇总表

问题编号	安全问题	测评对象	通用/扩展	安全类	控制点	测评项
T1	中心机房未部署防盗报警系统。	中心机房	安全通用要求	安全物理环境	防盗窃和防破坏	c)应设置机房防盗报警系统或设置有专人值守的视频监控系统
T2	安全问题 2					测评项 b
T3	安全问题 3					
T4	安全问题 4					测评项 c

4 整体测评

【填写说明：从安全控制点间、区域间对单项测评结果进行分析和整体评价。】

4.1 安全控制点间安全测评

4.2 区域间安全测评

4.3 整体测评结果汇总

【填写说明：根据整体测评结果填写下表，表中问题编号与 3.13.2 安全问题汇总表中的问题编号一一对应。】

经整体测评后安全问题严重程度变化情况如下表所示。

表 4-1 整体测评结果汇总表

问题编号	安全问题	测评对象	整体测评描述	严重程度变化
T1	中心机房未部署防盗报警系统。	中心机房	中心机房只有一个出入口，安排 24 小时专人值守机房的出入口。通过专人值守可以及时发现并阻止设备被盗窃。	☐升高 ☑降低
T2				☐升高 ☐降低
T3				☐升高 ☐降低

5 安全问题风险分析

【填写说明：采用风险分析方法分析安全问题可能带来的影响和风险等级，验证测试发现的相关安全问题如不能对应到具体测评项上，应在表中单独列出。下表

可根据实际情况设置为纵向或横向。】

针对等级测评结果中存在的所有安全问题，结合关联资产和威胁分别分析安全问题可能产生的危害结果，找出可能对系统、单位、社会及国家造成的最大安全危害（损失），并根据最大安全危害（损失）的严重程度进一步确定安全问题的风险等级，结果为“高”、“中”或“低”。最大安全危害（损失）结果应结合安全问题所影响业务的重要程度、相关系统组件的重要程度、安全问题严重程度以及安全事件影响范围等进行综合分析。

表 5-1 安全问题风险分析

序号	安全类	安全问题	关联资产[3]	关联威胁	危害分析结果	风险等级

6 等级测评结论

【填写说明：说明等级测评结论确定的方法，并最终给出被测对象的等级测评结论。】

等级测评结论由安全问题风险分析结果和综合得分共同确定，判定依据如下表所示。

表 6-1 等级测评结论判定依据

等级测评结论	判定依据
优	被测对象中存在安全问题，但不会导致被测对象面临中、高等级安全风险，且综合得分 90 分以上（含 90 分）。
良	被测对象中存在安全问题，但不会导致被测对象面临高等级安全风险，且综合得分 80 分以上（含 80 分）。
中	被测对象中存在安全问题，但不会导致被测对象面临高等级安全风

[3] 如风险值和评价相同，可填写多个关联资产。

等级测评结论	判定依据
	险，且综合得分 70 分以上（含 70 分）。
差	被测对象中存在安全问题，且会导致被测对象面临高等级安全风险，或综合得分低于 70 分。

综合得分计算方法如下：

设 M 为被测对象的综合得分，$M=V_t+V_m$，V_t 和 V_m 根据下列公式计算。

$$V_t=\begin{cases}100\cdot y-\sum_{k=1}^{t}f(\omega_k)\cdot(1-x_k)\cdot S, & V_t>0\\ 0, & V_t\le 0\end{cases}$$

$$V_m=\begin{cases}100\cdot(1-y)-\sum_{k=1}^{m}f(\omega_k)\cdot(1-x_k)\cdot S, & V_m>0\\ 0, & V_m\le 0\end{cases}$$

$$0\le x_k\le 1,\quad S=100\cdot\frac{1}{n},\quad f(\omega_k)=\begin{cases}1, & \omega_k=\text{一般}\\ 2, & \omega_k=\text{重要}\\ 3, & \omega_k=\text{关键}\end{cases}$$

其中，y 为关注系数，取值在 0 至 1 之间，由等级保护工作管理部门给出，默认值为 0.5。n 为被测对象涉及的总测评项数（不含不适用项，下同），t 为技术方面对应的总测评项数，V_t 为技术方面的得分，m 为管理方面对应的总测评项数，V_m 为管理方面的得分，ω_k 为测评项 k 的重要程度(分为一般、重要和关键)，x_k 为测评项 k 的得分，如果测评项 k 涉及多测评对象，则 x_k 取值为多测评对象得分的算术平均值。

x_k 的得分计算如下：

测评项 k 涉及对象 / 测评项 k 定性判定	只涉及单个对象	涉及多个对象
符合	1	1
部分符合	0.5	计算测评对象平均分，取值在 0 至 1 之间。
不符合	0	0

注：当测评项 k 涉及多个对象时，针对每个对象的得分取值为 1、0.5 和 0。

根据第 5 章安全问题风险分析结果统计高、中、低风险安全问题的数量，利用综合得分计算公式计算出被测对象的综合得分，并将相关结果填入下表。

表 6-2 安全问题统计和综合得分

被测对象名称	安全问题数量			综合得分
	高风险	中风险	低风险	

依据 GB/T 22239—2019《信息安全技术 网络安全等级保护基本要求》和 GB/T 28448—2019《信息安全技术 网络安全等级保护测评要求》的第[一/二/三/四]级要求，经对[被测对象名称]的安全保护状况进行综合分析评价后，等级测评结论如下：

【填写说明：下面分别给出等级测评结论为优、良、中、差的四个编写样例，供测评机构参考。】

[被测对象名称]本次等级测评的综合得分为 92，且不存在中、高等级安全风险，等级测评结论为优。

[被测对象名称]本次等级测评的综合得分为 86，且存在中等级安全风险，等级测评结论为良。

[被测对象名称]本次等级测评的综合得分为 75，且不存在高等级安全风险，等级测评结论为中。

[被测对象名称]本次等级测评的综合得分为 65，且不存在高等级安全风险，等级测评结论为差。

[被测对象名称]本次等级测评的综合得分为 85，但存在高等级安全风险，等级测评结论为差。

7 安全问题整改建议

【填写说明：针对 5 章列出的所有安全问题提出整改建议。下表可根据实际情况设置为纵向或横向。】

表 7-1 安全问题整改建议

序号	安全类	安全问题	关联资产	整改建议

【正文结束】

附录A 被测对象资产

A.1 物理机房

【填写说明：以列表形式给出被测对象的部署机房，包括云服务客户业务系统所涉及多个物理机房。】

附录 A 表-1 物理机房

序号	机房名称	物理位置	重要程度	备注

A.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）。】

附录 A 表-2 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

注：同类型设备在备注中填写设备数量，但确定为测评对象的设备必须单独列出，且设备名称应唯一。

A.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）。】

附录 A 表-3 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

注：同类型设备在备注中填写设备数量，但确定为测评对象的设备必须单独列出，且设备名

称应唯一。

A.4 服务器

【填写说明：以列表形式给出被测对象中的服务器（包括虚拟设备）。】

附录 A 表-4 服务器

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

注：同类型设备在备注中填写设备数量，但确定为测评对象的设备必须单独列出，且设备名称应唯一。

A.5 终端设备

【填写说明：以列表形式给出被测对象中的终端设备，包括业务终端、运维终端、管理终端等。】

附录 A 表-5 终端设备

序号	设备名称	是否虚拟设备	操作系统及版本	用途	重要程度	备注

注：同类型设备在备注中填写设备数量，但确定为测评对象的设备必须单独列出，且设备名称应唯一。

A.6 其他系统或设备

【填写说明：以列表形式给出被测对象中的其他系统或设备，如移动互联的移动终端、物联网的感知终端、工业控制系统的控制设备等。】

附录 A 表-6 其他系统或设备

序号	设备名称	是否虚拟设备	系统及版本	设备类别/用途	重要程度	备注

注：同类型设备在备注中填写设备数量，但确定为测评对象的设备必须单独列出，且设备名称应唯一。

A.7 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。】

附录 A 表-7 系统管理软件/平台

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

注：同类型软件/平台在备注中填写设备数量，但确定为测评对象的设备必须单独列出。

A.8 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/平台。】

附录 A 表-8 业务应用系统/平台

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	备注

A.9 数据资源

【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。数据资

源一般包括鉴别数据、重要业务数据、重要审计数据、重要配置数据和重要个人信息等。安全防护需求一般从保密性、完整性等方面进行分析。】

附录 A 表-9-a 数据资源

序号	数据类别	所属业务应用	安全防护需求	重要程度

【填写说明：大数据测评对象采用表- 9- b 数据资源，否则不用保留下表。】

附录 A 表-9-b 数据资源

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

A.10 密码产品

【填写说明：密码产品仅作为资产列出，不作为测评对象。】

附录 A 表- 10 密码产品

序号	产品/模块名称	生产厂商	商密型号	密码算法	用途	重要程度

A.11 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及所属单位，包括安全主管、网络管理员、系统管理员、应用管理员、数据管理员、审计管理员、机房管理员、资产管理员等。】

附录 A 表-11 安全相关人员

序号	姓名	岗位/角色	联系方式	所属单位

A.12 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，主要包括安全管理制度类文档、记录类文档和其他文档。】

附录 A 表-12 安全管理文档

序号	文档名称	主要内容

附录B 上次测评问题整改情况说明

【填写说明：描述被测对象上次等级测评结论及存在的所有安全问题。针对这些安全问题，核查被测单位安全整改情况，并进行整改情况说明。如果因为标准变动、部署环境变化等原因导致无法核查被测单位安全整改情况，则应在情况说明中阐述原因。如本次测评为被测对象的首次测评，则删除下表并进行文字说明。】

附录 B 表-1 上次测评问题整改情况

序号	安全问题	整改结果	情况说明
		□已整改 □未整改	
		□已整改 □未整改	

附录C 单项测评结果汇总

C.1 安全物理环境

【填写说明：针对安全通用要求和安全扩展要求的不同控制点对单个测评对象在安全物理环境方面的单项测评结果进行汇总，测评机构应按照以下表格编制。安全扩展要求部分表格中只需列出被测对象所涉及的安全扩展要求。如果被测对象不涉及所有安全扩展要求，则可删除安全扩展要求表格，以下各节要求类同。表格可根据实际情况设置为纵向或横向。】

附录 C 表-1 安全物理环境单项测评结果汇总表（安全通用要求部分）

序号	测评对象	符合情况	安全通用要求									
			物理位置选择	物理访问控制	防盗窃和防破坏	防雷击	防火	防水和防潮	防静电	温湿度控制	电力供应	电磁防护
		符合										
		部分符合										
		不符合										
		不适用										

附录 C 表-2 安全物理环境单项测评结果汇总表（安全扩展要求部分）

序号	测评对象	符合情况	安全扩展要求				
			基础设施位置（云计算）	无线接入点的物理位置（移动互联）	感知节点设备物理防护（物联网）	室外控制设备物理防护（工业控制）	安全物理环境（大数据）
		符合					
		部分符合					
		不符合					
		不适用					

C.2 安全通信网络

C.3 安全区域边界

C.4 安全计算环境

C.4.1 网络设备

【填写说明：网络设备、安全设备、服务器、终端、系统管理软件/平台和业务应用系统等所涉及的鉴别数据和重要配置数据分别在对应测评对象中汇总测评证据，包括数据完整性、数据保密性和备份恢复。】

C.4.2 安全设备

C.4.3 服务器和终端

C.4.4 系统管理软件/平台

C.4.5 业务应用系统/平台

C.4.6 数据资源

【填写说明：数据一般包括鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要个人信息和大数据资源等，这些数据分布在不同的测评对象上，应针对不同类型数据分别从不同测评对象上汇总测评证据。本节只汇总应用系统涉及的重要业务数据、重要个人信息和大数据资源的测评证据，包括数据完整性、数据保密性、剩余信息保护、数据备份恢复和个人信息保护等。】

C.4.7 其他系统或设备

C.5 安全管理中心

C.6 安全管理制度

C.7 安全管理机构

C.8 安全管理人员

C.9 安全建设管理

C.10 安全运维管理

C.11 其他安全要求指标

附录D 单项测评结果记录

D.1 安全物理环境

D.1.1 安全通用要求部分

D.1.1.1 测评对象 1

【填写说明：以下为单项测评结果记录表编写示例，测评机构可根据实际情况调整，但至少应包含下表中内容，以下各节要求类同。】

控制点	测评项	结果记录	符合情况
物理位置的选择	a）机房场地应选择在具有防震、防风和防雨等能力的建筑内。	1）机房所在建筑物具有建筑物抗震设防审批文档； 2）机房的设计/验收文档中包含对机房具有防震、防风和防雨等能力的设计要求或验收结论； 3）机房没有窗户，机房的屋顶、墙壁等不存在雨水渗漏的情况； 4）机房的屋顶、墙体和地面等不存在破损开裂的情况。	符合

D.1.1.2 测评对象 2

D.1.2 安全扩展要求部分

D.1.2.1 测评对象 1

D.1.2.2 测评对象 2

D.2 安全通信网络

D.3 安全区域边界

D.4 安全计算环境

【填写说明：如果选择的测评对象数量较少，可不按照网络设备、安全设备、服务器和终端、其他系统或设备、系统管理软件/平台、业务应用系统/平台等分类描述，直接列出每个测评对象即可。数据进一步按照鉴别数据、重要业务数据、重要审计数据、重要配置数据和重要个人信息单独描述】

D.4.1 安全通用要求部分

D.4.1.1 网络设备

D.4.1.2 安全设备

D.4.1.3 服务器和终端

D.4.1.4 其他系统或设备

D.4.1.5 系统管理软件/平台

D.4.1.6 业务应用系统/平台

D.4.1.7 数据资源

D.4.2 安全扩展要求部分

D.4.2.1 网络设备

D.5 安全管理中心

D.6 安全管理制度

D.7 安全管理机构

D.8 安全管理人员

D.9 安全建设管理

D.10 安全运维管理

D.11 其他安全要求

附录E 漏洞扫描结果记录

【填写说明：对网络设备、安全设备、服务器操作系统、数据库管理系统和应用系统等的进行洞扫描发现的安全漏洞，主要安全漏洞见下表。】

附录 E 表-1 漏洞扫描主要安全漏洞

序号	危险程度	漏洞名称	影响 IP
1	中	Apache HTTP Server mod_SSL 空指针间接引用漏洞(CVE-2017-3169)	
2			1
3			

附录F 渗透测试结果记录

【填写说明：填写详细的渗透测试过程记录，过程记录中至少包含必要的截图、漏洞名称、漏洞位置、风险等级、漏洞说明及危害等。】

F.1 XX 安全问题 1

F.2 XX 安全漏洞 2

附录G 威胁列表

【填写说明：建议测评机构依据最新版本 GB/T 20984 制定威胁列表，以下为参考示例。】

附录 G 表-1 威胁列表

序号	威胁分(子)类	威胁描述
1	恶意攻击	利用工具和技术对信息系统进行攻击和入侵。
2	软硬件故障	对业务实施或系统运行产生影响的设备硬件故障、通讯链路中断、系统本身或软件缺陷造等问题。
3	管理不到位	由于制度缺失、不完善等原因导致安全管理无法落实或者不到位。
4	无作为或操作失误	应该执行而没有执行相应的操作，或者无意执行了错误的操作。
5	敏感信息泄露	敏感信息泄露给不应了解的他人。
6	物理环境影响	对信息系统正常运行造成影响的物理环境问题和自然灾害。
7	越权或滥用	越权访问本来无权访问的资源，或者滥用自己的权限破坏信息系统。
8	物理攻击	通过物理的接触造成对软件、硬件和数据的破坏。
9	篡改	非法修改信息，破坏信息的完整性使系统的安全性降低或信息不可用。

序号	威胁分(子)类	威胁描述
10	抵赖	否认所做的操作。

附录H　云计算平台测评及整改情况

【填写说明：本附录仅适用于被测对象为云服务客户业务应用系统，且由独立定级的云计算平台提供平台支撑，否则删除。本附录内容由云服务商提供，主要包括两部分：一是云计算平台等级测评报告中的等级测评结论表、等级测评结论扩展表、总体评价、主要安全问题及整改建议；二是云服务商针对这些主要安全问题的整改情况说明；三是如果云租户部署在多个云平台上，提供多个云平台材料。】

附录I　大数据平台测评及整改情况

【填写说明：本附录仅适用于被测对象为大数据应用/资源，且由独立定级的大数据平台提供平台支撑，否则删除。本附录内容由大数据平台提供方提供，主要包括两部分：一是大数据平台等级测评报告中的等级测评结论表、等级测评结论扩展表、总体评价、主要安全问题及整改建议；二是大数据平台提供方针对这些主要安全问题的整改情况说明。】