报告编号：XXXXXXXXXXX-XXXXX-XX-XXXX-XX

网络安全等级保护
XXXXXX 等级测评报告

委托单位：_____

测评单位：_____

报告时间：_____年_____月_____日_____

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。

第三组为测评机构代码，由四位数字组成。前两位为省级行政区划数字代码的前两位或行业主管部门编号：00 为公安部，11 为北京，12 为天津，13 为河北，14 为山西，15 为内蒙古，21 为辽宁，22 为吉林，23 为黑龙江，31 为上海，32 为江苏，33 为浙江，34 为安徽，35 为福建，36 为江西，37 为山东，41 为河南，42 为湖北，43 为湖南，44 为广东，45 为广西，46 为海南，50 为重庆，51 为四川，52 为贵州，53 为云南，54 为西藏，61 为陕西，62 为甘肃，63 为青海，64 为宁夏，65 为新疆，66 为新疆兵团。90 为国防科工局，91 为国家能源局，92 为教育部。后两位为公安机关或行业主管部门推荐的测评机构顺序号。

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	第 X 级（S_XA_X）	
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			机构代码	
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	
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。针对特殊情况下的测评工作，测评机构可在以下建议内容的基础上增加特殊声明。】

本报告是 XXXXXX 的等级测评报告。

本报告是对 XXXX 进行整体安全性进行检测分析，针对等级测评过程中发现的安全问题，结合风险分析，提出科学、合理的建议。

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）都应重新进行等级测评，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）

年　　月　　日

等级测评结论

测评结论和综合得分			
被测对象名称		安全保护等级	第 X 级（S_XA_X）
被测对象描述	【填写说明：简要描述被测对象承载的业务功能等基本情况。建议不超过 400 字】		
测评工作描述	【填写说明：简要描述测评机构、什么时间进行测评等，被测对象安全技术情况和管理情况。建议不超过 400 字。】		
等级测评结论		综合得分	

云计算平台等级测评结论

【填写说明：此表只针对云租户系统的等级测评时适用，应由云计算服务商提供下表内容，可以是图片格式。如果为云计算平台测评报告，此部分删除。】

测评结论和综合得分			
被测对象名称		安全保护等级	第 X 级（S_XA_X）
等级测评报告编号			
被测对象描述	【填写说明：简要描述被测对象承载的业务功能等基本情况。建议不超过 400 字】		
测评工作描述	【填写说明：简要描述测评机构、什么时间进行测评等，被测对象安全技术情况和管理情况。建议不超过 400 字。】		
等级测评结论		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，对被测对象的安全保护状况进行说明和评价，可通过图表等方式进行多维度分析，基于综合评价结果对安全保护状况给出总括性结论。】

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，以及对主要安全问题提出针对性的整改建议。】

目录

正文表格索引

附录表格索引

插图索引

1 测评项目概述

1.1 测评目的

【填写说明：简述测评项目背景和项目目标等。】

1.2 测评依据

【填写说明：列出开展测评活动所依据的文件、标准和合同等。如果依据了行业标准的，列出行业标准。】

1.3 测评过程

【填写说明：描述等级测评工作流程、各阶段完成的关键任务和工作的时间节点等内容。】

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，描述被测对象承载的业务、主要功能，然后将定级结果填入下表。】

表 2-1 XXXXXX 定级结果

被测对象名称	安全保护等级	业务信息安全等级	系统服务安全等级

2.1.2 业务和采用的技术

【填写说明：描述被测对象采用云计算/移动互联/物联网/工业控制等技术情况，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和功能简介、与其他系统的互联情况和边界设备、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。】

图 2-1 XXXXXX 网络拓扑图

2.1.4 前次测评情况

【填写说明：简要描述前次等级测评发现的主要问题、测评结论和安全整改情况。】

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，依据业务信息安全保护等级和系统服务安全保护等级，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，以表格形式在表 2-2 中列出指标。】

表 2-2 安全通用要求指标

安全类 [1]	安全控制点 [2]	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等 10 个安全要求类别。

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

2.2.2 安全扩展要求指标

【填写说明：描述被测对象的特点，采用移动互联技术、云计算技术等的情况，或者是物联网、工业控制系统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，以表格形式在表 2-3 中列出指标。】

表 2-3 安全扩展要求指标

扩展类型	安全类	安全控制点	测评项数
云计算安全扩展要求			
移动互联安全扩展要求			
物联网安全扩展要求			
工业控制系统安全扩展要求			

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（如行业标准）或者高于《基本要求》的安全要求，其他安全要求指标权重由其提出部门给出并参与最终计分计算。】

表 2-4 其他安全要求指标

安全类	安全控制点	特殊要求描述	测评项数

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》的某些要求项可能不适用于整个系统，对于这些不适用项应在表后给出不适用原因。】

表 2-5 不适用安全要求指标

安全类	安全控制点	不适用项	不适用对象	原因说明

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 中测评对象确定原则和方法，结合资产重要程度赋值结果，描述本报告中测评对象的选择规则和方法。如果某些重要设备未被选为测评对象请说明原因。】

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
1			
2			

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	品牌型号	用途	数量（台/套）	重要程度
1							
2							

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	品牌型号	用途	数量（台/套）	重要程度
1							
2							

2.3.2.4 密码产品

表 2-9 密码产品

序号	产品名称	生产厂商	商密型号	使用的密码算法	数量	用途
1						
2						
3						

2.3.2.5 服务器/存储设备

表 2-10 服务器/存储设备

序号	设备名称	是否虚拟设备	操作系统/数据库管理系统及版本	业务应用软件及版本	数量（台/套）	重要程度
1						
2						

2.3.2.6 终端/现场设备

表 2-11 终端/现场设备

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	数量（台/套）	重要程度
1						
2						

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	所在设备名称	版本	主要功能	重要程度
1					
2					

2.3.2.8 业务应用软件/平台

表 2-13 业务应用软件/平台

序号	软件/平台名称	主要功能	开发厂商	重要程度
1				
2				

2.3.2.9 关键数据类型

表 2-14 关键数据类型

序号	数据类别	所属业务应用	安全防护需求	重要程度
1				
2				

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
1			
2			

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
1		
2		

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”以及“2.2.3 其他安全要求指标”中涉及的安全类和安全要求条款，内容包括已有安全控制措施汇总分析和主要安全问题汇总分析两个部分，单项测评结果汇总、详细结果记录及符合程度参见报告附录。

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：针对安全物理环境方面安全测评结果中存在的符合项加以汇总和分析，建议按照控制点进行详细描述，形成被测对象安全物理环境方面具备的安全

保护措施描述。】

3.1.2 主要安全问题汇总分析

【填写说明：针对安全物理环境方面存在的部分符合项或不符合项加以汇总和分析，描述主要安全问题及其关联对象，形成被测对象在安全物理环境方面的安全问题描述。全部安全问题描述参见 3.14.3 及报告附录。】

3.2 安全通信网络

3.2.1 已有安全控制措施汇总分析

【填写说明：针对安全通信网络方面安全测评结果中存在的符合项加以汇总和分析，建议按照控制点进行详细描述，形成被测对象安全通信网络方面具备的安全保护措施描述。】

3.2.2 主要安全问题汇总分析

【填写说明：针对安全通信网络方面存在的部分符合项或不符合项加以汇总和分析，并结合漏洞扫描及渗透测试等结果，描述主要安全问题及其关联对象，形成被测对象在安全通信网络方面的安全问题描述。全部安全问题描述参见 3.14.3 及报告附录。】

3.3 安全区域边界

3.3.1 已有安全控制措施汇总分析

【填写说明:针对安全区域边界方面安全测评结果中存在的符合项加以汇总和分析,建议按照控制点进行详细描述,形成被测对象安全区域边界方面具备的安全保护措施描述。】

3.3.2 主要安全问题汇总分析

【填写说明:针对安全区域边界方面存在的部分符合项或不符合项加以汇总和分析,并结合漏洞扫描及渗透测试等结果,描述主要安全问题及其关联对象,形成被测对象在安全区域边界方面的安全问题描述。全部安全问题描述参见 3.14.3 及报告附录。】

3.4 安全计算环境

3.4.1 网络设备和安全设备

3.4.1.1 已有安全控制措施汇总分析

【填写说明:针对网络设备和安全设备方面安全测评结果中存在的符合项加以汇

总和分析，建议按照控制点进行详细描述，形成被测对象网络设备和安全设备方面具备的安全保护措施描述。】

3.4.1.2 主要安全问题汇总分析

【填写说明:针对网络设备和安全设备方面存在的部分符合项或不符合项加以汇总和分析,并结合漏洞扫描及渗透测试等结果,描述主要安全问题及其关联对象,形成被测对象在网络设备和安全设备方面的安全问题描述。全部安全问题描述参见 3.14.3 及报告附录。】

3.4.2 服务器和终端

3.4.2.1 已有安全控制措施汇总分析

【填写说明:针对服务器和终端方面安全测评结果中存在的符合项加以汇总和分析，建议按照控制点进行详细描述，形成被测对象服务器和终端方面具备的安全保护措施描述。】

3.4.2.2 主要安全问题汇总分析

【填写说明:针对服务器和终端方面存在的部分符合项或不符合项加以汇总和分

析，并结合漏洞扫描及渗透测试等结果，描述主要安全问题及其关联对象，形成被测对象在服务器和终端方面的安全问题描述。全部安全问题描述参见 3.14.3 及报告附录。】

3.4.3 应用和数据

3.4.3.1 已有安全控制措施汇总分析

【填写说明：针对应用和数据方面安全测评结果中存在的符合项加以汇总和分析，建议按照控制点进行详细描述，形成被测对象应用和数据方面具备的安全保护措施描述。】

3.4.3.2 主要安全问题汇总分析

【填写说明：针对应用和数据方面存在的部分符合项或不符合项加以汇总和分析，并结合漏洞扫描及渗透测试等结果，描述主要安全问题及其关联对象，形成被测对象在应用和数据方面的安全问题描述。全部安全问题描述参见 3.14.3 及报告附录。】

3.4.4 其他系统和设备

3.4.4.1 已有安全控制措施汇总分析

【填写说明:针对其他系统和设备方面安全测评结果中存在的符合项加以汇总和分析,建议按照控制点进行详细描述,形成被测对象其他系统和设备方面具备的安全保护措施描述。】

3.4.4.2 主要安全问题汇总分析

【填写说明:针对其他系统和设备方面存在的部分符合项或不符合项加以汇总和分析,并结合漏洞扫描及渗透测试等结果,描述主要安全问题及其关联对象,形成被测对象在其他系统和设备方面的安全问题描述。全部安全问题描述参见3.14.3 及报告附录。】

3.5 安全管理中心

3.5.1 已有安全控制措施汇总分析

【填写说明:针对安全管理中心方面安全测评结果中存在的符合项加以汇总和分析,建议按照控制点进行详细描述,形成被测对象安全管理中心方面具备的安全保护措施描述。】

3.5.2 主要安全问题汇总分析

【填写说明:针对安全管理中心方面存在的部分符合项或不符合项加以汇总和分析,并结合漏洞扫描及渗透测试等结果,描述主要安全问题及其关联对象,形成被测对象在安全管理中心方面的安全问题描述。全部安全问题描述参见 3.14.3 及报告附录。】

3.6 安全管理制度

3.6.1 已有安全控制措施汇总分析

【填写说明:针对安全管理制度方面安全测评结果中存在的符合项加以汇总和分析,建议按照控制点进行详细描述,形成被测对象安全管理制度方面具备的安全保护措施描述。】

3.6.2 主要安全问题汇总分析

【填写说明:针对安全管理制度方面存在的部分符合项或不符合项加以汇总和分析,描述主要安全问题及其关联对象,形成被测对象在安全管理制度方面的安全问题描述。全部安全问题描述参见 3.14.3 及报告附录。】

3.7 安全管理机构

3.7.1 已有安全控制措施汇总分析

【填写说明:针对安全管理机构方面安全测评结果中存在的符合项加以汇总和分析,建议按照控制点进行详细描述,形成被测对象安全管理机构方面具备的安全保护措施描述。】

3.7.2 主要安全问题汇总分析

【填写说明:针对安全管理机构方面存在的部分符合项或不符合项加以汇总和分析,描述主要安全问题及其关联对象,形成被测对象在安全管理机构方面的安全问题描述。全部安全问题描述参见 3.14.3 及报告附录。】

3.8 安全管理人员

3.8.1 已有安全控制措施汇总分析

【填写说明:针对安全管理人员方面安全测评结果中存在的符合项加以汇总和分析,建议按照控制点进行详细描述,形成被测对象安全管理人员方面具备的安全保护措施描述。】

3.8.2 主要安全问题汇总分析

【填写说明：针对安全管理人员方面存在的部分符合项或不符合项加以汇总和分析，描述主要安全问题及其关联对象，形成被测对象在安全管理人员方面的安全问题描述。全部安全问题描述参见 3.14.3 及报告附录。】

3.9 安全建设管理

3.9.1 已有安全控制措施汇总分析

【填写说明：针对安全建设管理方面安全测评结果中存在的符合项加以汇总和分析，建议按照控制点进行详细描述，形成被测对象安全建设管理方面具备的安全保护措施描述。】

3.9.2 主要安全问题汇总分析

【填写说明：针对安全建设管理方面存在的部分符合项或不符合项加以汇总和分析，描述主要安全问题及其关联对象，形成被测对象在安全建设管理方面的安全问题描述。全部安全问题描述参见 3.14.3 及报告附录。】

3.10 安全运维管理

3.10.1已有安全控制措施汇总分析

【填写说明:针对安全运维管理方面安全测评结果中存在的符合项加以汇总和分析,建议按照控制点进行详细描述,形成被测对象安全运维管理方面具备的安全保护措施描述。】

3.10.2主要安全问题汇总分析

【填写说明:针对安全运维管理方面存在的部分符合项或不符合项加以汇总和分析,描述主要安全问题及其关联对象,形成被测对象在安全运维管理方面的安全问题描述。全部安全问题描述参见 3.14.3 及报告附录。】

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

【填写说明:针对其他安全要求指标方面安全测评结果中存在的符合项加以汇总和分析,建议按照控制点进行详细描述,形成被测对象其他安全要求指标方面具备的安全保护措施描述。】

3.11.2 主要安全问题汇总分析

【填写说明:针对其他安全要求指标方面存在的部分符合项或不符合项加以汇总和分析,描述主要安全问题及其关联对象,形成被测对象在其他安全要求指标方面的安全问题描述。全部安全问题描述参见 3.14.3 及报告附录。】

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,验证测试发现的安全问题对应到相应的测评项的结果记录中,详细验证测试报告参见附录。若由于用户原因无法开展验证测试,应将用户签章的“自愿放弃验证测试声明”作为报告附件。】

3.12.1 漏洞扫描问题汇总描述

【填写说明:针对漏洞扫描发现的安全问题进行汇总描述,如果漏洞扫描发现的安全问题较多,可以只描述主要的安全问题(如高风险)。全部安全问题描述参见报告附录。】

3.12.2 渗透测试问题汇总描述

【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。】

3.12.3 其他测试验证问题汇总

【填写说明：针对其他测试验证发现的安全问题进行汇总描述，详细测试验证过程记录描述参见报告附录。】

3.13 单项测评小结

3.13.1 控制点符合情况汇总

【填写说明：针对各个安全类单项测评结果，详细说明计算公式，汇总统计控制点得分和符合情况。以下段落为建议书写内容，测评机构可调整下述内容，如有特殊计算公式请说明。（附件《测评项权重赋值表》给出了测评项的权重用于得分计算，其他情况的权重赋值另行发布）】

根据附录 D 中测评项的符合程度得分，以算术平均法合并多个测评对象在同一测评项的得分，得到各测评项的多对象平均分。根据测评项权重，以加权平均合并同一安全控制点下的所有测评项的符合程度得分，并按照控制点得分计算公式得到各安全控制点的 10 分制得分。

控制点得分 $=\frac{\sum_{k=1}^{n} \text{测评项的多对象平均分}\times\text{测评项权重}}{\sum_{k=1}^{n} \text{测评项权重}}\times 10$，n 为同一控制点下的测评项数，不含不适用的控制点和测评项。

下表给出了汇总测评结果，表格以不同颜色对测评结果进行区分，不符合（安全控制点得分低于 10 分）的安全控制点采用红色标识。

表 3-1 测评结果分类统计表

序号	通用/扩展	安全类	安全控制点	安全控制点得分	符合情况		
					符合	不符合	不适用
1	安全通用要求	安全物理环境	物理位置选择				
2			物理访问控制				
3			防盗窃和防破坏				
4			防雷击				
5			防火				
6			防水和防潮				
7			防静电				
8			温湿度控制				
9			电力供应				
10			电磁防护				
安全控制点符合情况数量统计							

3.13.2 工具测试情况汇总

3.13.2.1 漏洞扫描汇总表

【填写说明：给出漏洞扫描的示意图及相关接入点说明。】

图 3-1 漏洞扫描工具接入测试示意图

1) 接入点 A 漏洞扫描结果统计

【填写说明：针对漏洞扫描结果按照下表进行汇总统计，详细漏洞扫描结果记录

描述参见报告附录。】

根据在接入点 A 对 XX 台被测设备的漏洞扫描结果，汇总统计如下表：

表 3-2 接入点 A 漏洞扫描结果统计表

序号	设备名称或 IP 地址	类型/OS	安全漏洞数量			
			低	中	高	小计
1	测评对象 1		2	0	0	2
2	测评对象 2		2	0	0	2
3	测评对象 3		2	0	0	2
4	测评对象 4		2	0	0	2
5	测评对象 n		2	0	0	2
安全漏洞数量小计			10	0	0	10

3.13.2.2 渗透测试汇总表

【填写说明：针对渗透测试结果进行汇总统计，详细渗透测试结果记录描述参见报告附录。】

3.13.3 安全问题汇总

【填写说明：针对各个安全类单项测评结果汇总统计安全问题。以下段落为建议书写内容，测评机构可调整下述内容。】

对单项测评结果中存在的不符合项进行汇总后，形成了下表中的安全问题。

表 3-3 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	安全控制点	测评项	测评项权重

4 整体测评结果分析

【填写说明：从安全控制间、区域间和验证测试等方面对单项测评的结果进行验证、分析和整体评价。具体内容参见《GB/T 28448 信息安全技术 网络安全等级保护测评要求》。】

4.1 安全控制间安全测评

4.2 区域间安全测评

4.3 整体测评结果汇总

【填写说明：根据整体测评结果汇总统计修正后的安全问题。以下段落为建议书写内容，测评机构可调整下述内容。】

根据整体测评结果，对安全问题汇总表中的安全问题进行修正，修正后的问题风险程度见表 4-1。

表 4-1 修正后的安全问题汇总表 [3]

序号	问题编号 [4]	安全问题描述	整体测评描述	修正前风险程度	修正后风险程度

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。以下段落为建议书写内容，测评机构可调整下述内容，如采用了特殊的风险分析方法请详细说明方法。】

针对等级测评结果中存在的所有安全问题，采用风险分析的方法进行危害分析和风险等级判定，得到被测对象安全问题风险分析表见表 4-2。

风险分析主要结合关联资产和关联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或损失（风险等级）。风险分析结果的判断综合了相关系统组件的重要程度、安全问题的严重程度、安全问题被关联威胁利用的可能性、所影响的相关业务应用以及发生安全事件可能的影响范围等因素。风险等级根据最大安全危害的严重程度进一步确定为

[3]该处仅列出问题严重程度有所修正的安全问题。

[4]该处编号与 3.13.3 安全问题汇总表中的问题编号一一对应。

“高”、“中”、“低”。

表 4-1 安全问题风险分析表

问题编号	安全类	问题描述	关联资产[5]	关联威胁[6]	危害分析结果	风险等级

6 等级测评结论

【填写说明：说明给出被测对象等级测评结论的方法，并最终给出本次等级测评的结论。以下段落为建议书写内容，测评机构可调整下述内容。】

本次等级测评依据下述公式给出等级测评结论，等级测评结论由综合得分和最终结论构成。

表 5-1 等级测评结论判别依据

测评结论	判别依据	综合得分计算公式
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，且系统综合得分 95 分以上（含 95 分）。	$100-\frac{\sum_{k=1}^{p}\ \sum_{i=1}^{m(k)}\text{不符合测评项权重}}{\sum_{k=1}^{p}\ \sum_{i=1}^{m(k)}\text{测评项权重}}\times 100$ p 为总测评项数，不含不适用的控制点和测评

5 如风险值和评价相同，可填写多个关联资产。

6 对于多个威胁关联同一个问题的情况，应分别填写。

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，且系统综合得分 85 分以上（含 85 分）。	项，m(k)为测评项 k 对应的测评对象数，如果存在高风险安全问题则直接判定等级测评结论为较差。
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险，且系统综合得分 75 分以上（含 75 分）。	
差	被测对象中存在安全问题，而且会导致被测对象面临高等级安全风险，或被测对象综合得分低于 75 分。	

表 5-2 安全风险汇总表

高风险问题	中风险问题	低风险问题	综合得分

【填表说明：请给出高中低安全问题数量及综合得分。】

依据 GB/T 22239《信息安全技术 网络安全等级保护基本要求》中对第 X 级系统的要求，对 XXXXXX 的安全保护状况通过综合分析评价，等级测评结论如下：

XXXXXX 中存在的不符合项不会导致系统面临高安全风险，本次测评的等级测评结论为 XXXX，综合得分为 XX。

7 安全问题整改建议

【填写说明：针对 4.4 章节汇总的安全问题提出整改建议。】

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。】

附录 A 表- 1 物理机房

序号	机房名称	物理位置	重要程度
1			
2			
3			

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	品牌型号	用途	数量（台/套）	重要程度
1							
2							
3							

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	品牌型号	用途	数量（台/套）	重要程度
1							
2							
3							

A.4 密码产品

附录 A 表-4 密码产品

序号	产品名称	生产厂商	商密型号	使用的密码算法	数量	用途
1						
2						
3						

A.5 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)。】

附录 A 表-5 服务器/存储设备

序号	设备名称	是否虚拟设备	操作系统/数据库管理系统及版本	业务应用软件及版本	数量（台/套）	重要程度
1						
2						
3						

A.6 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。】

附录 A 表-6 终端/现场设备

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	数量（台/套）	重要程度
1						
2						

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	数量（台/套）	重要程度
3						

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
1					
2					
3					

A.8 业务应用软件/平台

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

附录 A 表-8 业务应用软件/平台

序号	软件/平台名称	主要功能	开发厂商	重要程度
1				
2				
3				

A.9 关键数据类别

【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。】

附录 A 表-9 关键数据类别

序号	数据类别 [7]	所属业务应用	安全防护需求 [8]	重要程度
1				
2				
3				

A.10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、安全审计人员等。】

附录 A 表- 10 安全相关人员

序号	姓名	岗位/角色	联系方式
1			
2			
3			

A.11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。】

附录 A 表- 11 安全管理文档

序号	文档名称	主要内容
1		

[7]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。

[8] 保密性和完整性等。

序号	文档名称	主要内容
2		
3		

附录B 上次测评问题整改情况说明

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安全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和统计。】

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
1	机房 1	符合										
		不符合										
		不适用										
2	机房 2	符合										
		不符合										
		不适用										
n	机房 n	符合										
		不符合										
		不适用										

总计测评项 X 个，符合项 X 个，不符合项 X 个，不适用项 X 个

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（移动互联）
1	对象 1	符合				
		不符合				
		不适用				
2	对象 2	符合				
		不符合				
		不适用				
n	对象 n	符合				
		不符合				
		不适用				
总计测评项 X 个，符合项 X 个，不符合项 X 个，不适用项 X 个						

C.2 安全通信网络

【填写说明：针对安全通用要求和安全扩展要求的不同安全控制点对单个测评对象在安全通信网络方面的单项测评结果进行汇总和统计。】

附录 C 表- 3 安全通信网络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		
			网络架构	通信传输	可信验证
1	对象 1	符合			
		不符合			
		不适用			
2	对象 2	符合			
		不符合			
		不适用			
n	对象 n	符合			

		不符合			
		不适用			
总计测评项 X 个，符合项 X 个，不符合项 X 个，不适用项 X 个					

附录 C 表- 4 安全通信网络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		
			网络架构（云计算）	网络架构（工业控制）	通信传输（工业控制）
1	对象 1	符合			
		不符合			
		不适用			
2	对象 2	符合			
		不符合			
		不适用			
n	对象 n	符合			
		不符合			
		不适用			
总计测评项 X 个，符合项 X 个，不符合项 X 个，不适用项 X 个					

C.3 安全区域边界

【填写说明：针对安全通用要求和安全扩展要求的不同安全控制点对单个测评对象在安全区域边界方面的单项测评结果进行汇总和统计。】

附录 C 表- 5 安全区域边界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					
			边界防护	访问控制	入侵防范	恶意代码和垃圾邮件防范	安全审计	可信验证
1	对象 1	符合						
		不符合						
		不适用						

2	对象 2	符合						
		不符合						
		不适用						
n	对象 n	符合						
		不符合						
		不适用						
总计测评项 X 个，符合项 X 个，不符合项 X 个，不适用项 X 个								

附录 C 表- 6 安全区域边界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										
			访问控制（云计算）	入侵方法（云计算）	安全审计（云计算）	边界防护（移动互联）	访问控制（移动互联）	入侵防范（移动互联）	接入控制（物联网）	入侵方法（物联网）	访问控制（工业控制）	拨号使用控制（工业控制）	无线使用控制（工业控制）
1	对象 1	符合											
		不符合											
		不适用											
2	对象 2	符合											
		不符合											
		不适用											
n	对象 n	符合											
		不符合											
		不适用											
总计测评项 X 个，符合项 X 个，不符合项 X 个，不适用项 X 个													

C.4 安全计算环境

C.4.1 网络设备和安全设备

【填写说明：针对安全通用要求和安全扩展要求的不同安全控制点对单个测评对

象（网络设备和安全设备等）在安全计算环境方面的单项测评结果进行汇总和统计。】

附录 C 表- 7 安全计算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										
			身份鉴别	访问控制	安全审计	入侵防范	恶意代码防范	可信验证	数据完整性	数据保密性	数据备份恢复	剩余信息保护	个人信息保护
1	对象 1	符合											
		不符合											
		不适用											
2	对象 2	符合											
		不符合											
		不适用											
n	对象 n	符合											
		不符合											
		不适用											
总计测评项 X 个，符合项 X 个，不符合项 X 个，不适用项 X 个													

附录 C 表- 8 安全计算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												
			身份鉴别（云计算）	访问控制（云计算）	入侵防范（云计算）	镜像和快照保护（云计算）	数据完整性和保密性（云计算）	数据备份恢复（云计算）	剩余信息保护（云计算）	移动终端管控（移动互联）	移动应用管控（移动互联）	感知节点设备安全（物联网）	网关节点设备安全（物联网）	抗数据重放（物联网）	数据融合处理（物联网）	控制设备安全（工业控制）

1	对象 1	符合														
		不符合														
		不适用														
2	对象 2	符合														
		不符合														
		不适用														
n	对象 n	符合														
		不符合														
		不适用														
总计测评项 X 个，符合项 X 个，不符合项 X 个，不适用项 X 个																

C.4.2 服务器和终端

【填写说明：针对安全通用要求和安全扩展要求的不同安全控制点对单个测评对象（服务器和终端等）在安全计算环境方面的单项测评结果进行汇总和统计。】

附录 C 表- 9 安全计算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										
			身份鉴别	访问控制	安全审计	入侵防范	恶意代码防范	可信验证	数据完整性	数据保密性	数据备份恢复	剩余信息保护	个人信息保护
1	对象 1	符合											
		不符合											

		不适用											
2	对象 2	符合											
		不符合											
		不适用											
n	对象 n	符合											
		不符合											
		不适用											
总计测评项 X 个，符合项 X 个，不符合项 X 个，不适用项 X 个													

附录 C 表- 10 安全计算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													
			身份鉴别（云计算）	访问控制（云计算）	入侵防范（云计算）	镜像和快照保护（云计算）	数据完整性和保密性（云计算）	数据备份恢复（云计算）	剩余信息保护（云计算）	移动终端管控（移动互联）	移动应用管控（移动互联）	感知节点设备安全（物联网）	网关节点设备安全（物联网）	抗数据重放（物联网）	数据融合处理（物联网）	控制设备安全（工业控制）
1	对象 1	符合														
		不符合														
		不适用														
2	对象 2	符合														
		不符合														

		不适用														
n	对象 n	符合														
		不符合														
		不适用														
总计测评项 X 个，符合项 X 个，不符合项 X 个，不适用项 X 个																

C.4.3 应用和数据

【填写说明：针对安全通用要求和安全扩展要求的不同安全控制点对单个测评对象（应用和数据等）在安全计算环境方面的单项测评结果进行汇总和统计。】

附录 C 表- 11 安全计算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										
			身份鉴别	访问控制	安全审计	入侵防范	恶意代码防范	可信验证	数据完整性	数据保密性	数据备份恢复	剩余信息保护	个人信息保护
1	对象 1	符合											
		不符合											
		不适用											
2	对象 2	符合											
		不符合											
		不适用											
n	对象 n	符合											
		不符合											
		不适用											
总计测评项 X 个，符合项 X 个，不符合项 X 个，不适用项 X 个													

附录 C 表- 12 安全计算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													
			身份鉴别（云计算）	访问控制（云计算）	入侵防范（云计算）	镜像和快照保护（云计算）	数据完整性和保密性（云计算）	数据备份恢复（云计算）	剩余信息保护（云计算）	移动终端管控（移动互联）	移动应用管控（移动互联）	感知节点设备安全（物联网）	网关节点设备安全（物联网）	抗数据重放（物联网）	数据融合处理（物联网）	控制设备安全（工业控制）
1	对象1	符合														
		不符合														
		不适用														
2	对象2	符合														
		不符合														
		不适用														
n	对象n	符合														
		不符合														
		不适用														
总计测评项 X 个，符合项 X 个，不符合项 X 个，不适用项 X 个																

C.4.4 其他系统和设备

【填写说明：针对安全通用要求和安全扩展要求的不同安全控制点对单个测评对象（其他系统和设备等）在安全计算环境方面的单项测评结果进行汇总和统计。】

附录 C 表- 13 安全计算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										
			身份鉴别	访问控制	安全审计	入侵防范	恶意代码防范	可信验证	数据完整性	数据保密性	数据备份恢复	剩余信息保护	个人信息保护
1	对象 1	符合											
		不符合											
		不适用											
2	对象 2	符合											
		不符合											
		不适用											
n	对象 n	符合											
		不符合											
		不适用											
总计测评项 X 个，符合项 X 个，不符合项 X 个，不适用项 X 个													

附录 C 表- 14 安全计算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												
			身份鉴别（云计算）	访问控制（云计算）	入侵防范（云计算）	镜像和快照保护（云计算）	数据完整性和保密性（云计算）	数据备份恢复（云计算）	剩余信息保护（云计算）	移动终端管控（移动互联）	移动应用管控（移动互联）	感知节点设备安全（物联网）	网关节点设备安全（物联网）	抗数据重放（物联网）	数据融合处理（物联网）	控制设备安全（工业控制）

1	对象 1	符合														
		不符合														
		不适用														
2	对象 2	符合														
		不符合														
		不适用														
n	对象 n	符合														
		不符合														
		不适用														
总计测评项 X 个，符合项 X 个，不符合项 X 个，不适用项 X 个																

C.5 安全管理中心

【填写说明：针对安全通用要求和安全扩展要求的不同安全控制点对单个测评对象在安全管理中心方面的单项测评结果进行汇总和统计。】

附录 C 表- 15 安全管理中心单项测评结果汇总表

序号	测评对象	符合情况	安全通用要求				安全扩展要求
			系统管理	审计管理	安全管理	集中管控	集中管控（云计算）
1	对象 1	符合					
		不符合					
		不适用					
2	对象 2	符合					
		不符合					

		不适用					
n	对象 n	符合					
		不符合					
		不适用					
总计测评项 X 个，符合项 X 个，不符合项 X 个，不适用项 X 个							

C.6 全管理制度

【填写说明：针对安全通用要求和安全扩展要求的不同安全控制点对单个测评对象在安全管理制度方面的单项测评结果进行汇总和统计。】

附录 C 表- 16 安全管理制度单项测评结果汇总表

类或方面	符合情况	安全通用要求			
		安全策略	管理制度	制度和发布	评审和修订
安全管理制度	符合				
	不符合				
	不适用				
总计测评项 X 个，符合项 X 个，不符合项 X 个，不适用项 X 个					

C.7 安全管理机构

【填写说明：针对安全通用要求和安全扩展要求的不同安全控制点对单个测评对象在安全管理机构方面的单项测评结果进行汇总和统计。】

附录 C 表- 17 安全管理机构单项测评结果汇总表

类或方面	符合情况	安全通用要求				
		岗位设置	人员配备	授权和审批	沟通和合作	审核和检查
安全管理机构	符合					
	不符合					
	不适用					
总计测评项 X 个，符合项 X 个，不符合项 X 个，不适用项 X 个						

C.8 安全管理人员

【填写说明：针对安全通用要求和安全扩展要求的不同安全控制点对单个测评对象在安全管理人员方面的单项测评结果进行汇总和统计。】

附录 C 表- 18 安全管理人员单项测评结果汇总表

类或方面	符合情况	安全通用要求			
		人员录用	人员离岗	安全意识教育和培训	外部人员访问管理
安全管理人员	符合				
	不符合				
	不适用				
总计测评项 X 个，符合项 X 个，不符合项 X 个，不适用项 X 个					

C.9 安全建设管理

【填写说明：针对安全通用要求和安全扩展要求的不同安全控制点对单个测评对象在安全建设管理方面的单项测评结果进行汇总和统计。】

附录 C 表- 19 安全建设管理单项测评结果汇总表（安全通用要求部分）

类或方面	符合情况	安全通用要求									
		定级和备份	安全方案设计	产品采购和使用	自行软件开发	外包软件开发	工程实施	测试验收	系统交付	等级测评	服务供应商选择
安全建设管理	符合										
	不符合										
	不适用										
总计测评项 X 个，符合项 X 个，不符合项 X 个，不适用项 X 个											

附录 C 表- 20 安全建设管理单项测评结果汇总表（安全扩展要求部分）

类或方面		安全扩展要求

	符合情况	云服务商选择（云计算）	供应链管理（云计算）	移动应用软件采购（移动互联）	移动应用软件开发（移动互联）	产品采购和使用（工业控制）	外包软件开发（工业控制）
安全建设管理	符合						
	不符合						
	不适用						
总计测评项 X 个，符合项 X 个，不符合项 X 个，不适用项 X 个							

C.10 安全运维管理

【填写说明：针对安全通用要求和安全扩展要求的不同安全控制点对单个测评对象在安全运维管理方面的单项测评结果进行汇总和统计。】

附录 C 表- 21 安全运维管理单项测评结果汇总表（安全通用要求）

类或方面	符合情况	安全通用要求													
		环境管理	资产管理	介质管理	设备维护管理	漏洞和风险管理	网络和系统安全管理	恶意代码防范管理	配置管理	密码管理	变更管理	备份与恢复管理	安全事件处置	应急预案管理	外包运维管理
安全运维管理	符合														
	不符合														
	不适用														
总计测评项 X 个，符合项 X 个，不符合项 X 个，不适用项 X 个															

附录 C 表- 22 安全运维管理单项测评结果汇总表（安全扩展要求部分）

类或方面	符合情况	安全扩展要求					
		云计算环境管理（云计算）	配置管理（移动互联）	感知节点管理（物联网）	漏洞和风险管理（工业控制）	恶意代码防范管理（工业控制）	安全事件处置（工业控制）
	符合						

安全运维管理	不符合						
	不适用						
总计测评项 X 个，符合项 X 个，不符合项 X 个，不适用项 X 个							

C.11 密码应用安全

【填写说明：针对密码应用安全指标（未覆盖或者高于《基本要求》）的单项测评结果进行汇总和统计。】

附录 C 表- 23 密码应用安全指标单项测评结果汇总表

序号	测评对象	符合情况	密码应用安全要求指标			
1	对象 1	符合				
		不符合				
		不适用				
2	对象 2	符合				
		不符合				
		不适用				
n	对象 n	符合				
		不符合				
		不适用				
总计测评项 X 个，符合项 X 个，不符合项 X 个，不适用项 X 个						

C.12 其他安全要求指标

【填写说明：针对其他指标（未覆盖或者高于《基本要求》（或行业标准））的单项测评结果进行汇总和统计。】

附录 C 表- 24 其他指标单项测评结果汇总表

序号	测评对象	符合情况	其他安全要求指标			
1	对象 1	符合				
		不符合				
		不适用				
2	对象 2	符合				

		不符合				
		不适用				
n	对象 n	符合				
		不符合				
		不适用				
总计测评项 X 个，符合项 X 个，不符合项 X 个，不适用项 X 个						

附录D　单项测评结果记录

说明：单项测评指标只有符合、不符合、不适用。

D.1 安全物理环境

D.1.1 安全通用要求部分

[redacted]测评对象 1

[redacted]测评对象 2

D.1.2 安全扩展要求部分

[redacted]测评对象 1

[redacted]测评对象 2

D.2 安全通信网络

D.2.1 安全通用要求部分

[redacted]测评对象 1

[redacted]测评对象 2

D.2.2 安全扩展要求部分

[redacted]测评对象 1

[redacted]测评对象 2

D.3 安全区域边界

D.3.1 安全通用要求部分

[redacted]测评对象 1

[redacted]测评对象 2

D.3.2 安全扩展要求部分

[redacted]测评对象 1

[redacted]测评对象 2

D.4 安全计算环境

D.4.1 安全通用要求部分

[redacted]测评对象 1

[redacted]测评对象 2

D.4.2 安全扩展要求部分

[redacted]测评对象 1

[redacted]测评对象 2

D.5 安全管理中心

D.5.1 测评对象 1

D.5.2 测评对象 2

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.9.1 安全通用要求部分

D.9.2 安全扩展要求部分

D.10 安全运维管理

D.10.1 安全通用部分

D.10.2 安全扩展部分

D.11其他安全要求

附录E 漏洞扫描结果记录

附录F　渗透测试结果记录

附录G　测评项权重赋值表