网络安全等级保护
XXX 系统
等级测评方案

系统名称：

委托单位：

测评单位：

编制日期： 2019 年 X 月

测评文档基本信息			
文档名称	网络安全等级保护【XXX 系统】等级测评方案		
编制单位			
编 制 人			
审 阅 人			
提交日期			
测评文档确认信息			
确 认 人		日期	
单位/部门			

目 录

1 概述

1.1 项目简介

为贯彻落实国务院147号令和中办27号文件，公安部会同有关部委出台了一系列的文件以及具体工作的指导意见和规范，并在全国范围内组织完成了一系列工作。目前，信息安全等级保护工作已经进入安全建设整改阶段，公安部印发了《关于开展信息系统等级保护安全建设整改工作的指导意见》（公信安[2009]1429），明确提出："依据信息安全等级保护有关政策和标准，通过组织开展信息安全等级保护安全管理制度建设、技术措施建设和等级测评，落实等级保护制度的各项要求，力争在2012年底前完成已定级信息系统安全建设整改工作"。

为了贯彻国家对网络安全保障工作的要求，XXXX委托YYYY对ZZZZ平台进行安全等级保护测评。测评工作组将依据等级保护的相关管理规范、技术标准，实施本次安全测评工作。安全测评范围包括被测系统相关的网络设备、安全设备、服务器设备等；测评内容涵盖安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心以及信息安全管理等方面。测评完成后针对系统中存在的安全问题进行风险分析，提出整改意见，并最终形成安全等级测评报告。本测评方案仅用于指导ZZZZ平台的安全等级保护测评工作。

1.2 测评依据

1) 《中华人民共和国计算机信息系统安全保护条例》(国务院147号令)
2) 《信息安全等级保护管理办法》（公通字[2007]43号）
3) 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》）
4) GB/T 28448-2019《信息安全技术 网络安全等级保护测评要求》（以下简称《测评要求》）

2 被测信息系统情况

2.1 定级情况

本次被测系统定级结果如下：

ZZZZ 平台的安全保护等级为第三级，其中业务信息安全等级和系统服务安全等级均为第三级。

2.2 承载的业务情况

【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。】

2.3 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 [被测对象名称]网络拓扑图

2.4 被测对象资产

2.4.1.1 物理机房

【填写说明：以列表形式给出被测对象的部署机房。】

表 2-1 物理机房

序号	机房名称	物理位置	重要程度
1			
2			
3			

2.4.1.2 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）。】

表 2-2 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

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
1						
2						
3						

2.4.1.3 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）。】

表 2-3 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
1						
2						
3						

2.4.1.4 密码产品

【填写说明：以列表形式给出被测对象中使用的密码产品。】

表 2-4 密码产品

序号	产品/模块名称	生产厂商	商密型号证书编号	使用的密码算法	用途	重要程度
1						
2						
3						

2.4.1.5 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）。】

表 2-5 服务器/存储设备

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
1							
2							

2.4.1.6 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。】

表 2-6 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	重要程度
1					
2					
3					

2.4.1.7 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。】

表 2-7 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					

2.4.1.8 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（包括服务器端和客户端软件等应用软件）。】

表 2-8 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
1					
2					
3					

2.4.1.9 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。】

表 2-9 关键数据类别

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

【填写说明：当被测对象为大数据系统时，测评对象选择需要覆盖各级各类的大数据资源，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，

[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。

[2] 保密性和完整性等。

因此大数据系统测评采用表 2-10】

表 2-10 大数据数据类别

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									
2									

2.4.1.10 访谈人员

【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。】

表 2-11 安全相关人员

序号	姓名	岗位/角色	联系方式
1			
2			
3			

2.4.1.11 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。】

表 2-12 安全管理文档

序号	文档名称	主要内容
1		
2		
3		

2.5 上次测评问题整改情况说明

【填写说明：描述上次等级测评发现的主要问题、测评结论和安全整改情况。】

3 测评范围与方法

《基本要求》中对不同等级信息系统的安全功能和措施作出具体要求，信息安全等级测评要根据信息系统的等级从中选取相应等级的安全测评指标，并根据《测评要求》的要求，对信息系统实施安全测评。因此，本次测评将根据信息系统的等

级选取相应级别的测评指标。

3.1 测评指标

3.1.1 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 3-1 中列出指标。】

表 3-1 安全通用要求指标

安全类[3]	安全控制点[4]	测评项数

3.1.2 安全扩展要求指标

【填写说明：描述采用移动互联技术、云计算技术等的被测对象，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 3-2 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			
大数据安全扩展要求			

[3] 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。

[4]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。

3.1.3 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）或者高于被测对象相应等级《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 3-3 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

3.1.4 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某些测评对象，对于这些不适用项应在表后给出不适用原因。】

表 3-4 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

3.2 测评对象

3.2.1 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，赋值结果为非常重要、重要、一般，描述本报告中测评对象的选择规则和方法。当被测对象为大数据系统时，测评对象选择还应结合数据的分类分级结果，描述本报告中大数据资源相关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，请在相应表格下方通过文字描述说明原因。】

3.2.2 测评对象选择结果

3.2.2.1 物理机房

表 3-5 物理机房

序号	机房名称	物理位置	重要程度
1			
2			

3.2.2.2 网络设备

表 3-6 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
1						
2						

3.2.2.3 安全设备

表 3-7 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
1						
2						

3.2.2.4 密码产品

表 3-8 密码产品

序号	产品/模块名称	生产厂商	商密型号	使用的密码算法	用途	重要程度
1						
2						
3						

3.2.2.5 服务器/存储设备

表 3-9 服务器/存储设备

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
1							
2							

3.2.2.6 终端/现场设备

表 3-10 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	重要程度
1					
2					

3.2.2.7 系统管理软件/平台

表 3-11 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					

3.2.2.8 业务应用系统/平台

表 3-12 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
1					
2					

3.2.2.9 关键数据类别

表 3-13 关键数据类别

序号	数据类别	所属业务应用	安全防护需求
1			
2			

表 3-14 大数据数据类别

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

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									
2									

3.2.2.10 安全相关人员

表 3-145 安全相关人员

序号	姓名	岗位/角色	联系方式
1			
2			

3.2.2.11 安全管理文档

表 3-16 安全管理文档

序号	文档名称	主要内容
1		
2		

3.3 测评方法

安全测评的主要方式包括：访谈、检查和测试。

- 访谈

访谈是指测评人员通过与信息系统有关人员（个人/群体）进行交流、讨论等活动，获取相关证据表明信息系统安全保护措施是否落实的一种方法。在访谈的范围上，应基本覆盖所有的安全相关人员类型，在数量上可以抽样。

- 检查

检查是指测评人员通过对测评对象进行观察、查验、分析等活动，获取证据以证明信息系统安全等级保护措施是否得以有效实施的一种方法。在检查范围上，应基本覆盖所有的对象种类（设备、文档、机制等），数量上可以抽样。

- 测试

测试是指测评人员通过对测评对象按照预定的方法/工具使其产生特定的响应等活动，查看、分析响应输出结果，获取证据以证明信息系统安全等级保护措施是否得以有效实施的一种方法。在测试范围上，应基本覆盖不同类型的机制，在数量

上可以抽样。

4 单项测评内容

把测评指标和测评方式结合到信息系统的具体测评对象上，就构成了可以具体测评的工作单元。具体分为安全物理环境、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、安全运维管理等方面。

4.1 基础环境安全测评

把测评指标和测评方式结合到信息系统的具体测评对象上，就构成了可以具体测评的工作单元。具体分为安全物理环境、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、安全运维管理等方面。

4.1.1 安全物理环境测评

安全物理环境测评中，测评人员将以文档查阅与分析和现场观测等检查方法为主，访谈为辅来获取测评证据（如机房的温湿度情况），用于评测机房的安全保护能力。

安全物理环境测评涉及的测评对象主要为机房和相关的安全文档。

安全物理环境测评实施过程涉及 10 个方面的安全保护能力，具体测评指标描述如下表所示：

表 4-1 安全物理环境测评指标描述

序号	安全子类	测评指标描述
1	物理位置选择	通过访谈物理安全负责人，检查机房，测评机房物理场所在位置上是否具有防震、防风和防雨等多方面的安全防范能力。
2	物理访问控制	通过访谈物理安全负责人，检查机房出入口等过程，测评信息系统在物理访问控制方面的安全防范能力。
3	防盗窃和防破坏	通过访谈物理安全负责人，检查机房内的主要设备、介质和防盗报警设施等过程，测评信息系统是否采取必要的措施预防设备、介质等丢失和被破坏。
4	防雷击	通过访谈物理安全负责人，检查机房设计/验收文档，测评信息系统是否采取相应的措施预防雷击。
5	防火	通过访谈物理安全负责人，检查机房防火方面的安全管理制度，检查机房防火设备等过程，测评信息系统是否采取必要的措施防止火灾的发

序号	安全子类	测评指标描述
		生。
6	防水和防潮	通过访谈物理安全负责人，检查机房及其除潮设备等过程，测评信息系统是否采取必要措施来防止水灾和机房潮湿。
7	防静电	通过访谈物理安全负责人，检查机房等过程，测评信息系统是否采取必要措施防止静电的产生。
8	温湿度控制	通过访谈物理安全负责人，检查机房的温湿度自动调节系统，测评信息系统是否采取必要措施对机房内的温湿度进行控制。
9	电力供应	通过访谈物理安全负责人，检查机房供电线路、设备等过程，测评是否具备为信息系统提供一定电力供应的能力。
10	电磁防护	通过访谈物理安全负责人，检查主要设备等过程，测评信息系统是否具备一定的电磁防护能力。

4.1.2 安全通信网络测评

安全通信网络测评中，测评人员将以配置核查和文档查阅为主，访谈和分析为辅来获取证据(如相关措施的部署和配置情况),用于测评信息系统的网络安全保护。

安全通信网络测评涉及的测评对象主要为网络设备和安全。

安全通信网络测评实施过程涉及 3 个方面的安全保护能力，具体测评指标描述如下表所示：

表 4-2 安全通信网络测评指标描述

序号	安全子类	测评指标描述
1	网络架构	测评分析网络架构与网段划分、隔离等情况的合理性和有效性。
2	通信传输	测评通信过程中的完整性、保密性等。
3	可信验证	基于可信根对通信设备的系统引导程序、系统程序、重要配置参数和通信应用程序等 进行可信验证，并在应用程序的关键执行环节进行动态可信验证。

4.1.3 安全区域边界测评

安全区域边界测评主要涉及边界防护、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 6 个方面的安全保护能力，具体测评指标描述如下表所示：

表 4-3 安全区域边界测评指标描述

序号	安全子类	测评指标描述
1	边界防护	测评分析信息系统网络边界安全防护的状况。
2	访问控制	测评分析信息系统对网络区域边界相关的网络隔离与访问控制能力。
3	入侵防范	测评分析信息系统对攻击行为的识别和处理情况。

序号	安全子类	测评指标描述
4	恶意代码和垃圾邮件防范	测评分析信息系统网络边界和核心网段对病毒等恶意代码及垃圾邮件的防护情况。
5	安全审计	测评分析信息系统审计配置和审计记录保护情况。
6	可信验证	基于可信根对通信设备的系统引导程序、系统程序、重要配置参数和通信应用程序等 进行可信验证，并在应用程序的关键执行环节进行动态可信验证。

4.1.4 安全计算环境测评

安全计算环境测评主要涉及身份鉴别、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 11 个方面的安全保护能力，具体测评指标描述如下表所示：

表 4-4 安全计算环境测评指标描述

序号	安全子类	测评指标描述
1	身份鉴别	检查服务器的身份标识与鉴别和用户登录的配置情况。
2	访问控制	检查服务器的访问控制设置情况，包括安全策略覆盖、控制粒度以及权限设置情况等。
3	安全审计	检查服务器的安全审计的配置情况，如覆盖范围、记录的项目和内容等；检查安全审计进程和记录的保护情况。
4	入侵防范	检查服务器在运行过程中的入侵防范措施，如关闭不需要的端口和服务、最小化安装、部署入侵防范产品等。
5	恶意代码防范	检查服务器的恶意代码防范情况，如服务器是否安装统一管理的恶意代码防范软件，是否及时升级病毒库等。
6	可信验证	基于可信根对通信设备的系统引导程序、系统程序、重要配置参数和通信应用程序等 进行可信验证，并在应用程序的关键执行环节进行动态可信验证。
7	数据完整性	测评操作系统、数据库管理系统的管理数据、鉴别信息和用户数据在传输和保存过程中的完整性保护情况。
8	数据保密性	测评操作系统和数据库管理系统的管理数据、鉴别信息和用户数据在传输和保存过程中的保密性保护情况。
9	数据备份恢复	测评信息系统的安全备份情况，如重要信息的备份、硬件和线路的冗余等。
10	剩余信息保护	测评鉴别信息所在的存储空间被释放或重新分配前是否得到完全清除。
11	个人信息保护	测评是否仅采集和保存业务必需的用户个人信息；是否禁止未授权访问和使用用户个人信息。

4.1.5 安全管理中心测评

安全管理中心测评主要涉及系统管理、审计管理、安全管理、集中管控 4 个方面的安全保护能力，具体测评指标描述如下表所示：

表 4-5 安全管理中心测评指标描述

序号	安全子类	测评指标描述
1	系统管理	测评信息系统的系统管理员对系统的管理情况。
2	审计管理	测评信息系统的安全审计员对系统的审计情况。
3	安全管理	测评信息系统的安全管理员对系统的安全策略的配置情况。
4	集中管控	测评网络链路、安全设备、网络设备和服务器等设备的运行状况的集中监测、分析、报警等。

4.1.6 安全管理制度测评

安全管理制度测评主要涉及安全策略、管理制度、制定和发布、评审和修订 4 个方面的安全保护能力，具体测评指标描述如下表所示：

表 4-6 安全管理制度测评指标描述

序号	安全子类	测评指标描述
1	安全策略	测评信息安全工作的总体方针、安全策略，总体目标、范围、原则和安全框架等。
2	管理制度	测评信息系统管理制度在内容覆盖上是否全面、完善。
3	制定和发布	测评信息系统管理制度的制定和发布过程是否遵循一定的流程。
4	评审和修订	测评信息系统管理制度定期评审和修订情况。

4.1.7 安全管理机构测评

安全管理制度测评主要涉及岗位设置、人员配备、授权和审批、沟通和合作、审核和检查 5 个方面的安全保护能力，具体测评指标描述如下表所示：

表 4-7 安全管理机构测评指标描述

序号	安全子类	测评指标描述
1	岗位设置	测评信息系统安全主管部门设置情况以及各岗位设置和岗位职责情况。
2	人员配备	测评信息系统各个岗位人员配备情况。
3	授权和审批	测评信息系统对关键活动的授权和审批情况。
4	沟通与合作	测评信息系统内部部门间、与外部单位间的沟通与合作情况。
5	审核和检查	检查信息系统安全工作的审核和测评情况。

4.1.8 安全管理人员测评

安全管理人员测评主要涉及人员录用、人员离岗、安全意识教育和培训、外部人员访问管理4个方面的安全保护能力，具体测评指标描述如下表所示：

表 4-8 安全管理人员测评指标描述

序号	安全子类	测评指标描述
1	人员录用	测评信息系统录用人员时是否对人员提出要求以及是否对其进行各种审查和考核。
2	人员离岗	测评信息系统人员离岗时是否按照一定的手续办理。
3	安全意识教育和培训	测评是否对人员进行安全方面的教育和培训。
4	外部人员访问管理	测评对第三方人员访问（物理、逻辑）系统是否采取必要控制措施。

4.1.9 安全建设管理测评

安全建设管理测评主要涉及定级和备案、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10个方面的安全保护能力，具体测评指标描述如下表所示：

表 4-9 安全建设管理测评指标描述

序号	安全子类	测评指标描述
1	定级和备案	测评是否按照一定要求确定系统的安全等级并完成备案工作。
2	安全方案设计	测评系统整体的安全规划设计是否按照一定流程进行。
3	产品采购和使用	测评是否按照一定的要求进行系统的产品采购。
4	自行软件开发	测评自行开发的软件是否采取必要的措施保证开发过程的安全性。
5	外包软件开发	测评外包开发的软件是否采取必要的措施保证开发过程的安全性和日后的维护工作能够正常开展。
6	工程实施	测评系统建设的实施过程是否采取必要的措施使其在机构可控的范围内进行。
7	测试验收	测评系统运行前是否对其进行测试验收工作。
8	系统交付	测评是否采取必要的措施对系统交付过程进行有效控制。
9	等级测评	测评是否依据国家要求完成等级测评和整改工作。
10	服务供应商选择	测评是否选择符合国家有关规定的安全服务单位进行相关的安全服务工作。

4.1.10 安全运维管理测评

安全管理人员测评主要涉及环境管理、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 14 个方面的安全保护能力，具体测评指标描述如下表所示：

表 4-10 安全运维管理测评指标描述

序号	安全子类	测评指标描述
1	环境管理	测评是否采取必要的措施对机房的出入控制以及办公环境的人员行为等方面进行安全管理。
2	资产管理	测评是否采取必要的措施对系统的资产进行分类标识管理。
3	介质管理	测评是否采取必要的措施对介质存放环境、使用、维护和销毁等方面进行管理。
4	设备维护管理	测评是否采取必要的措施确保设备在使用、维护和销毁等过程安全。
5	漏洞和风险管理	测评是否采取必要的措施识别安全漏洞和隐患，对发现的安全漏洞和隐患及时进行修补。测评是否定期开展安全测评。
6	网络和系统安全管理	测评是否采取必要的措施对网络和系统的安全配置、系统账户、漏洞扫描和审计日志等方面进行有效的管理。
7	恶意代码防范管理	测评是否采取必要的措施对恶意代码进行有效管理，确保系统具有恶意代码防范能力。
8	配置管理	测评是否记录和保存系统的基本配置信息
9	密码管理	测评是否能够确保信息系统中密码算法和密钥的使用符合国家密码管理规定。
10	变更管理	测评是否采取必要的措施对系统发生的变更进行有效管理。
11	备份与恢复管理	测评是否采取必要的措施对重要业务信息，系统数据和系统软件进行备份，并确保必要时能够对这些数据有效地恢复。
12	安全事件处置	测评是否采取必要的措施对安全事件进行等级划分和对安全事件的报告、处理过程进行有效的管理。
13	应急预案管理	测评是否针对不同安全事件制定相应的应急预案，是否对应急预案展开培训、演练和审查等。
14	外包运维管理	测评外包运维服务商的选择是否符合国家的有关规定并签订相关协议。

4.2 云计算安全测评

4.2.1 安全物理环境

安全物理环境测评主要关注基础设施位置,具体测评指标描述如下表所示:

表 4-11 安全物理环境测评指标描述

序号	安全子类	测评指标描述
1	基础设施位置	查看云计算基础设施是否处于中国境内。

4.2.2 安全通信网络

安全通信网络测评主要关注网络架构,具体测评指标描述如下表所示:

表 4-12 安全通信网络测评指标描述

序号	安全子类	测评指标描述
1	网络架构	测评分析网络架构与隔离等情况的合理性和有效性，测评拓扑图与实际运行情况的一致性，网络结构是否具备灵活性。

4.2.3 安全区域边界

安全区域边界测评主要关注访问控制、入侵防范、安全审计,具体测评指标描述如下表所示:

表 4-13 安全区域边界测评指标描述

序号	安全子类	测评指标描述
1	访问控制	测评分析云租户内部网络区域边界相关的网络隔离与访问控制能力。
2	入侵防范	测评分析对外攻击和有害信息发布的检测、告警能力。
3	安全审计	测评分析云租户与云服务商的职责划分，并依此测评审计信息的完整性和可用性。

4.2.4 安全计算环境

安全计算环境测评主要关注身份鉴别、访问控制、入侵防范、镜像和快照保护、数据完整性和保密性、数据备份和恢复、剩余信息保护,具体测评指标描述如下表所示:

表 4-14 安全计算环境测评指标描述

序号	安全子类	测评指标描述
1	身份鉴别	测评虚拟机、数据系统、网络设备和安全设备的身份鉴别能力。包括口令安全策略、身份鉴别机机制等。
2	访问控制	测评虚拟机、数据库系统、网络设备和安全设备的访问控制设置情况，包括安全策略、控制粒度以及权限设置情况等。
3	入侵防范	测评分析对虚拟机在运行过程中的隔离失效、异常访问的检测、告警能力，对虚拟机的迁移范围进行限制。
4	镜像和快照保护	测评虚拟机镜像和快照完整性、保密性和安全性。

序号	安全子类	测评指标描述
5	数据完整性和保密性	测评虚拟机迁移过程的鉴别信息和用户数据在传输过程中的完整性保护情况。
6.	数据备份和恢复	测评云租户重要数据的本地备份、存储位置，应用系统的可移植性等。
7	剩余信息保护	测评虚拟机的存储空间，被释放或再分配给其他用户前得到完全清除。

4.2.5 安全管理中心

安全管理中心测评主要关注集中管控,具体测评指标描述如下表所示:

表 4-15 安全管理中心测评指标描述

序号	安全子类	测评指标描述
1	集中管控	测评网络链路、安全设备、网络设备和服务器等设备的运行状况的集中监测、分析、报警等。

4.2.6 安全建设管理

安全建设管理测评主要关注云服务商选择、供应链选择,具体测评指标描述如下表所示:

表 4-16 安全建设管理测评指标描述

序号	安全子类	测评指标描述
1	云服务商选择	测评是否选择符合有关规定的云服务商。
2	供应链选择	测评供应链安全事件信息、重要变更或威胁信息是否及时传达到云租户。

4.2.7 安全运维管理

安全建设运维管理测评主要关注云计算环境管理,具体测评指标描述如下表所示:

表 4-17 安全运维管理测评指标描述

序号	安全子类	测评指标描述
1	云计算环境管理	云计算平台的运维地点位于中国境内，境外对境内云计算平台实施运维操作应遵循国家有关规定。

4.3 移动互联安全测评

4.3.1 安全物理环境

安全物理环境测评主要关注无线接入点的物理位置,具体测评指标描述如下表所示:

表 4-18 安全物理环境测评指标描述

序号	安全子类	测评指标描述
1	无线接入点的物理位置	测评无线接入设备的安装选择合理位置，避免过度覆盖和电磁干扰。

4.3.2 安全区域边界

安全区域边界测评主要关注边界防护、访问控制、入侵防范,具体测评指标描述如下表所示:

表 4-19 安全区域边界测评指标描述

序号	安全子类	测评指标描述
1	边界防护	测评有线网络与无线网络边界之间的访问和数据流是否是通过无线接入网关设备。
2	访问控制	测评无线接入设备是否开启接入认证功能,并支持采用认证服务器认证或国家密码管理局批准的密码模块进行认证。
3	入侵防范	测评分析无线接入设备对攻击行为的识别和处理情况。

4.3.3 安全计算环境

安全计算环境测评主要关注移动终端管控、移动应用管控,具体测评指标描述如下表所示:

表 4-20 安全计算环境测评指标描述

序号	安全子类	测评指标描述
1	移动终端管控	测评移动终端安装、注册并运行终端管理客户端软件,移动终端并接受管理服务端的设备生命周期及设备远程控制。
2	移动应用管控	测评应用软件安装是否只允许指定证书签名的应用软件安装和运行,是否具有白名单功能。

4.3.4 安全建设管理

安全建设管理测评主要关注移动应用软件采购、移动应用软件开发,具体测评指标描述如下表所示:

表 4-21 安全建设管理测评指标描述

序号	安全子类	测评指标描述
1	移动应用软件采购	测评移动终端软件是否来自可靠分发渠道或者使用可靠证书签名,应用软件是否由指定开发者开发。
2	移动应用软件开发	测评是否对业务应用软件开发者进行资格审查,签名证书的合法性。

4.3.5 安全运维管理

安全运维管理测评主要配置管理,具体测评指标描述如下表所示:

表 4-22 安全运维管理测评指标描述

序号	安全子类	测评指标描述
1	配置管理	应建立合法无线接入设备和合法移动终端配置库,用于对非法无线接入设备和非法移动终端的识别。

4.4 大数据安全测评

4.4.1 安全物理环境

安全物理环境测评主要关注承载大数据的机房物理位置,具体测评指标描述如下表所示:

表 4-23 安全物理环境测评指标描述

序号	测评指标描述
1	测评承载大数据存储、处理和分析的设备机房是否位于中国境内。

4.4.2 安全通信网络

安全网络测评主要关注大数据平台与应用的级别以及流量是否区分,具体测评指标描述如下表所示:

表 4-24 安全区域边界测评指标描述

序号	测评指标描述
1	测评大数据平台承载能力，是否不低于承载的大数据应用。
2	测评大数据平台是否将管理流量与业务流量分离。

4.4.3 安全计算环境

安全计算环境测评主要关注大数据在数据生命周期的各个过程的安全防护情况,具体测评指标描述如下表所示:

表 4-25 安全计算环境测评指标描述

序号	测评指标描述
1	测评大数据平台是否对数据采集、数据导入、导出过程采取身份鉴别措施。
2	测评大数据平台是否能对不同客户的大数据应用实施标识和鉴别。
3	测评大数据平台是否具备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；
4	测评大数据平台应是否对其提供的辅助工具或服务组件实施了有效管理。
5	测评大数据平台是否能够屏蔽计算、内存、存储资源故障。
6	测评大数据平台是否能够具有静态脱敏的提供静态脱敏和去标识化措施。
7	测评对外提供服务的大数据平台对大数据应用的使用是否经过授权。
8	测评大数据平台数据分类分级情况及保护措施。
9	测评大数据平台是否具备细粒度授权访问控制管理能力。
10	测评大数据平台在数据采集、存储、处理、分析等各个环节，是否进行了分类分级处置。
11	测评涉及重要数据接口、重要服务接口的调用是否实施了访问控制。
12	测评在数据清洗和转换过程中是否对重要数据进行保护，避免数据失真。
13	测评溯源数据能否重现相应过程，溯源数据是否合规审计要求。
14	测评大数据平台是否对不同大数据应用的审计数据隔离存放，是否提供不同客户审计数据收集汇总和集中分析的能力。

4.4.4 安全建设管理

安全建设管理测评主要关注大数据平台承载能力和权责问题,具体测评指标描述如下表所示:

表 4-26 安全建设管理测评指标描述

序号	测评指标描述
1	测评大数据平台服务是否为其所承载的大数据应用提供相应等级的安全保护能力。
2	测评是否以书面方式约定大数据平台提供者的权限与责任、各项服务内容和具体技术指标等，尤其是安全服务内容。
3	测评是或否明确了约束数据交换、共享的接收方对数据的保护责任，并确保接收方有足够或相当的安全防护能力。

4.4.5 安全运维管理

安全运维管理测评主要测评数据全生命周期的运维管理措施及规范,具体测评指标描述如下表所示:

表 4-27 安全运维管理测评指标描述

序号	测评指标描述
1	测评是否建立数字资产安全管理策略，对数据全生命周期的操作规范、保护措施、管理人员职责等进行规定。
2	测评是否制定并执行数据分类分级保护策略，针对不同类别级别的数据制定不同的安全保护措施。
3	测评是否在数据分类分级的基础上，划分了重要数字资产范围，明确重要数据进行自动脱敏或去标识的使用场景和业务处理流程。
4	测评是否定期评审数据的类别和级别，如需要变更数据的类别或级别，应依据变更审批流程执行变更。

5 工具测试

5.1 测评工具

主要使用到的测评工具具体描述如下表：

表 5-1 测试工具列表

序号	工具用途分类	具体描述
1	系统层漏洞检测	系统层漏洞扫描工具。
2	应用层漏洞检测	应用系统漏洞扫描工具。
3	渗透测试工具集	包含缓冲区溢出利用、口令破解、注入验证等等。

5.2 风险和规避措施

5.2.1 操作系统和常见应用漏洞扫描

在使用扫描器对目标系统扫描的过程中，可能会出现以下的风险：

1) 占用带宽（风险不高）。

2) 进程、系统崩溃。由于目标系统的多样性及脆弱性，或是目标系统上某些特殊服务本身存在的缺陷，对扫描器发送的探测包或者渗透测试工具发出的测试数据不能正常响应，可能会出现系统崩溃或程序进程的崩溃。

3) 登录界面锁死。扫描器可以对某些常用应用程序（系统登录、FTP，Telnet，SNMP，SSH，WebLogic）的登录口令进行弱口令猜测验证，如果目标系统对登录失败次数进行了限制，尝试登录次数超过限定次数系统可能会锁死登录界面。

风险规避方法：

1) 根据目标系统的网络、应用状况，调整扫描测试时间段，采取避峰扫描；

2) 对扫描器扫描策略进行配置，适当调整扫描器的并发任务数和扫描的强度，可使减少扫描器工作时占用的带宽，降低对目标系统影响；

3) 根据目标系统及目标系统上运行的应用程序，通过与测评委托方相关人员协商，定制针对本系统测试的扫描插件、端口等配置，尽量合理设置扫描强度，降低目标系统或进程崩溃的风险；

4) 如目标系统对登录某些相关程序的尝试次数进行了限制，在进行扫描时，可屏蔽暴力猜解功能，以避免登录界面锁死的情况发生。

5.2.2 WEB 应用漏洞扫描

在使用 WEB 应用漏洞扫描器对目标系统扫描的过程中，可能会存在以下的风险：

1) 占用带宽（风险不高）。

2) 登录界面锁死。WEB 应用漏洞扫描会对登录页面进行弱口令猜测，猜测过程可能会造成应用系统某些帐号锁死。

风险规避方法：

1) 根据目标系统的网络、应用状况，调整扫描测试时间段，采取避峰扫描；

2) 如目标系统对登录某些相关程序的尝试次数进行了限制，在进行扫描时，可屏蔽暴力猜解功能，以避免登录界面锁死的情况发生。

5.3 工具测试接入点说明

为了发挥测评工具的作用，达到测评的目的，各种测评工具需要接入到被测评的信息系统网络多处，并需要配置恰当的网络 IP 地址。因此，本节重点就测试工具的接入情况进行说明。

针对 ZZZZ 平台的网络结构情况，需要在系统及其边界中设置？个测试工具接入点（接入点 A 至接入点？）对 ZZZZ 平台进行扫描测试。如图所示。“接入点”标

注表示进行工具测试时，需要从该网络设备上接入，对应的箭头路线表示工具测试数据的主要流向示意：

图 5-1 接入测试示意图

5.3.1 在接入点进行探测

在接入点 A-M 点接入测试工具，探测目标系统的服务器以及扫描路径途径的网络设备，测试网络设备和服务器对该点暴露出的安全漏洞情况。扫描的网络设备、服务器设备列表如下所示：

表 5-2 接入点 A-M 扫描的网络设备和服务器设备

序号	设备名称	操作系统/版本/补丁	IP
1			
2			

根据扫描探测结果，在接入点使用测试工具集，试图利用安全漏洞获取网络设备和服务器的操作权限。

5.4 渗透测试说明

渗透测试是漏洞扫描测试的一种有效补充，漏洞扫描毕竟存在一定的局限性，比如某些应用层漏洞 SQL 注入漏洞等，由于发现这些漏洞需要一些手动的测试，才能取得更好的效果。

在扫描发现漏洞之后，根据目标服务器的具体情况，判断漏洞验证的风险程度，如条件合适，在最大程度不影响目标系统正常运行的情况下，对漏洞扫描发现的漏洞进行验证、取证。

渗透测试验证过程仅限于验证漏洞的可用性，而不对目标系统做任何的添加、修改等操作。

6 系统整体测评内容

信息系统的安全控制集成到信息系统后，会在层面内、层面间和区域间产生连接、交互、依赖、协同等相互关联关系，使信息系统的整体安全功能与信息系统的结构密切相关，在整体上呈现出一种集成特性。这些集成特性在安全控制的工作单元中是没有完全体现。因此，在安全控制测评的基础上，有必要对集成系统和运行

环境进行整体测评。

6.1 安全控制间安全测评

安全控制间安全测评主要指从信息系统的物理布局、网络拓扑、业务逻辑（业务数据流）、系统实现和集成方式等基础上，结合不同控制点间可能面临的威胁、可能暴露的脆弱性等，综合判定各安全控制间整体安全情况是否有效等。

6.2 区域/层面间安全测评

区域间的安全测评主要考虑互连互通（包括物理上和逻辑上的互连互通等）的不同区域之间存在的安全功能增强、补充和削弱等关联作用，特别是有数据交换的两个不同区域。层面间的安全测评主要考虑同一区域内的不同层面之间存在的功能增强、补充和削弱等关联作用。例如，网络通信层面、安全计算环境层面与安全管理的系统运维管理之间关系密切，应关注他们之间的关联互补作用。

7 配合资源要求

1) 人员配合要求

表 7-1 配合人员列表

配合人员	具体工作说明
总体协调人	能够进行各种工作的跨部门组织协调的人员
网络管理人员	对系统的网络架构、网络设备、安全设备、管理平台部署情况较为熟悉的人员，现场配合检查组中网络组人员完成网络方面的测评和调研工作。
系统管理人员	对系统中的各类主机的操作系统、数据库系统、各类数据备份等情况较为熟悉的人员，现场配合检查组中主机组人员完成主机和部分数据测评工作。
应用系统开发/运维人员	负责各类应用系统情况、熟悉各类应用在系统中实际部署情况的人员，现场配合检查组中应用组人员完成应用的检查工作。
机房管理人员	负责机房管理的人员，现场配合检查组中管理组完成物理安全测评工作。
安全文档维护人员	对所有相关的文档进行整理和管理的人员，现场配合检查组中管理组完成管理测评工作。

2) 扫描测试配合要求

表 7-2 扫描测试配合要求列表

配合项目	要求说明

配合人员	网络管理员，提供： 1 对于每个接入点，2 个可用以太网电口以及对应的合法 IP 地址； 2 监控网络设备的运行状态。
	主机及业务应用管理员，负责在漏洞扫描期间监控相关主机以及业务应用的运行状态。
安全权限	如接入测评设备时需出入机房，则需要测评人员在测评实施期间出入机房的许可。
	针对 WEB 扫描，需要能够访问目标应用所有应用页面的用户权限。

3) 文档资料配合要求

表 7-3 文档资料配合要求列表

文档名称	具体说明
各类管理制度文档	管理制度、工作单
其他文档	应用系统设计、开发文档

4) 现场工作环境配合要求

- 相对独立的办公环境，可以容纳 6-8 人左右；
- 提供一个保险柜，用于保存工作中的各类过程文档，以防止丢失；
- 提供一台打印机和打印纸，以便文档的输出。