ICS 点击此处添加 ICS 号
点击此处添加中国标准文献分类号

GB/T 28448. 2—20XX

信息安全技术 网络安全等级保护测评要求 第 2 部分：云计算安全扩展要求

Information security technology—

Testing and evaluation requirement for classified protection of network security Part 2: Testing and evaluation requirement of cloud computing security

点击此处添加与国际标准一致性程度的标识

（征求意见稿）

20XX－XX－XX 发布 20XX－XX－XX 实施

目　　次

前　言

本部分按照GB/T1.1-2009给出的规则起草。

GB/T 28448已经或计划发布以下部分：

——GB/T 28448.1-20XX 信息安全技术 网络安全等级保护测评要求 第1部分：通用测评要求；

——GB/T 28448.2-20XX 信息安全技术 网络安全等级保护测评要求 第2部分：云计算安全扩展测评要求；

——GB/T 28448.3-20XX 信息安全技术 网络安全等级保护测评要求 第3部分：移动互联安全扩展测评要求；

——GB/T 28448.4-20XX 信息安全技术 网络安全等级保护测评要求 第4部分：物联网安全扩展测评要求；

——GB/T 28448.5-20XX 信息安全技术 网络安全等级保护测评要求 第5部分：工业控制安全扩展测评要求；

——GB/T 28448.6-20XX 信息安全技术 网络安全等级保护测评要求 第6部分：大数据安全扩展测评要求；

本部分由全国信息安全标准化技术委员会提出。

本部分由全国信息安全标准化技术委员会归口。

本部分起草单位：国家信息中心、公安部第三研究所、北京航空航天大学、北京大学、阿里云计算有限公司、曙光信息产业股份有限公司、中科院信息工程研究所、北京天地超云科技有限公司。

本部分主要起草人：禄凯、章恒、陈永刚、任卫红、张振峰、黄河、高亚楠、邵国安、孙惠平、陈雪秀、白秀杰、陈驰、姜杨、张一鸣。

引　言

国家标准GB/T 28448—2012 《信息安全技术 信息系统安全等级保护测评要求》在开展信息安全等级保护测评工作的过程中起到了非常重要的作用，被广泛应用于各个行业和领域开展信息安全等级保护等级测评等工作，但是随着信息技术的发展，GB/T 28448—2012在时效性、易用性、可操作性上需要进一步完善。

为了适应移动互联、云计算、大数据、物联网和工业控制等新技术、新应用情况下信息安全等级保护测评工作的开展，需对GB/T 28448—2012进行修订，修订的思路和方法是针对移动互联、云计算、大数据、物联网和工业控制等新技术、新应用领域提出扩展的测评要求。

本部分只对等级保护第二级到第四级云计算系统做出要求。

在本部分文本中，黑体字表示较低等级中没有出现或增强的要求。

本部分为GB/T 28448.1在云计算系统安全领域的扩展要求，对云计算系统应用GB/T 28448时应同时使用GB/T 28448.1和GB/T 28448.2的相关要求。

信息安全技术 网络安全等级保护测评要求
第 2 部分：云计算安全扩展测评要求

1 范围

本部分规定了对不同等级的等级保护对象是否符合GB/T 22239.2-20XX所进行的测试评估活动的要求，包括对第二级等级保护对象、第三级等级保护对象和第四级等级保护对象进行安全测试评估的要求。本部分略去对第一级等级保护对象、第五级等级保护对象进行安全测评评估的要求。

本部分规定了不同等级的保护对象的云计算安全扩展测评要求，除使用本部分外，还需参考通用测评要求。

本部分适用于信息安全测评服务机构、等级保护对象的主管部门及运营使用单位对等级保护对象安全等级保护状况进行的安全测试评估。信息安全监管职能部门依法进行的信息系统安全等级保护监督检查可以参考使用。

2 规范性引用文件

下列文件对于本部分的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本部分。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本部分。

GB/T 25069-2010 信息安全技术 术语

GB17859-1999 计算机信息系统安全保护等级划分准则

GB/T 22239.1-20XX 信息安全技术 网络安全等级保护基本要求 第1部分：安全通用要求

GB/T 22240-2008 信息安全技术 信息系统安全等级保护定级指南

GB/T 28448.1-20XX 信息安全技术 网络安全等级保护测评要求 第1部分：通用测评要求

GB/T 28449-20XX 信息安全技术 信息系统安全等级保护测评过程指南

GB/T 22239.2-20XX 信息安全技术 网络安全等级保护基本要求 第2部分：云计算安全扩展要求

GB/T 25070.2-20XX 信息安全技术 网络安全等级保护安全设计技术要求 第2部分：云计算信息安全等级保护安全设计技术要求

3 术语与定义

GB/T 25069-2010、GB/T 28448.1-20XX和GB/T 22239.2-20XX界定的以及下列术语和定义适用于本部分。

3.1

访谈 interview

访谈是指测评人员通过引导等级保护对象相关人员进行有目的的（有针对性的）交流以帮助测评人员理解、澄清或取得证据的过程。

3.2

检查 examination

检查是指测评人员通过对测评对象（如制度文档、各类设备、安全配置等）进行观察、查验、分析以帮助测评人员理解、澄清或取得证据的过程。

3.3

测试 testing

测试是指测评人员使用预定的方法/工具使测评对象（各类设备或安全配置）产生特定的结果，将运行结果与预期的结果进行比对的过程。

3.4

云计算 cloud computing

一种通过网络提供计算资源服务的模式，在该模式下，用户按需动态自助供给、管理各类计算资源。

3.5

网络策略控制器 network policy controller

在网络中，把网络配置信息转化为网络设备上的转发规则集，并对这些转发规则集进行管理的核心控制系统。

3.6

云计算平台 cloud computing platform

由云服务方提供的云计算基础设施及其上的服务层软件的集合。（引自GB/T 31168-2014）

3.7

云服务方 cloud service provider

云服务的提供者，包括与云租户建立商业关系或没有商业关系的云服务提供者。

3.8

云租户 cloud tenant

租用或使用云计算资源的客户，包括计费的和不计费的云服务的机构和个人。

3.9

云服务 cloud service

由云服务方使用云计算提供的服务。（引自GB/T 31168-2014）

3.10

虚拟机监视器 hypervisor

一种运行在基础物理服务器和操作系统之间的中间软件层,可允许多个操作系统和应用共享硬件。

3.11

宿主机 host machine

运行虚拟机监视器的物理服务器。

3.12

基础设施即服务　infrastructure as a service

提供给消费者的服务是对所有计算基础设施的利用，包括处理CPU、内存、存储、网络和其它基本的计算资源，用户能够部署和运行任意软件，包括操作系统和应用程序。

3.13

软件即服务　software as a service

提供给客户的服务是运营商运行在云计算基础设施上的应用程序，用户可以在各种设备上通过客户端界面访问，如浏览器。

3.14

平台即服务　platform as a service

提供给消费者的服务是把客户采用提供的开发语言和工具（例如Java，python，.Net等）开发的或收购的应用程序部署到供应商的云计算基础设施上去。

4　等级保护测评概述

4.1　测评描述框架

云计算安全等级保护测评（以下简称等级测评）的概念性描述框架由两部分构成：单项测评和整体测评，图 1 给出了等级测评框架。

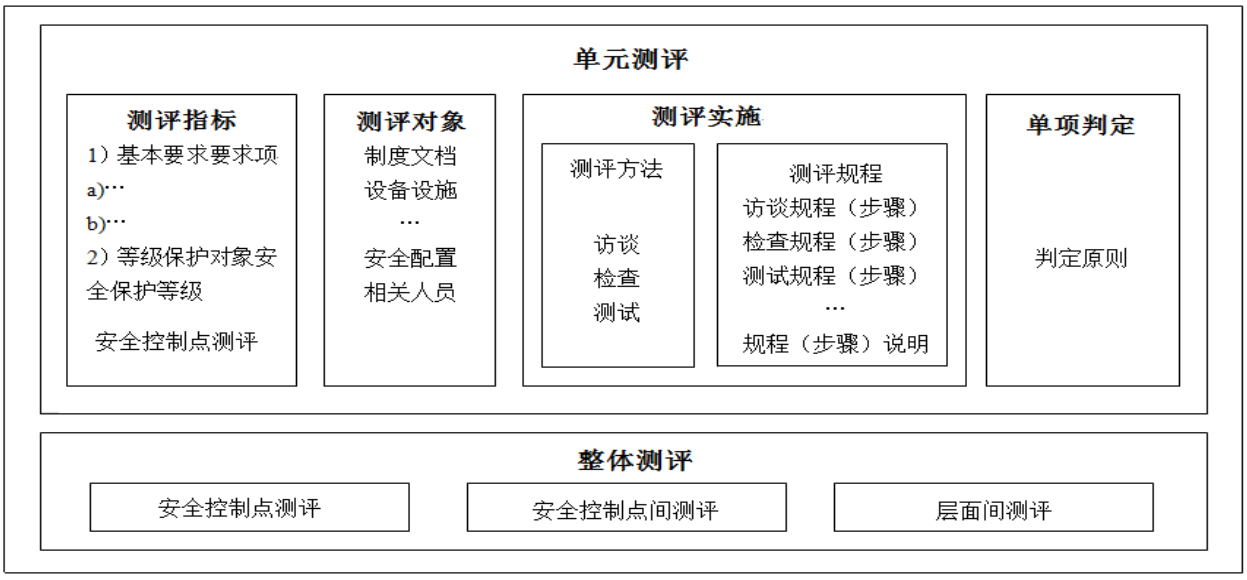

图1　测评框架

针对基本要求各安全要求项的测评称为单项测评，单项测评是等级测评工作的基本活动，支持测评结果的可重复性和可再现性。单项测评是由测评指标、测评对象、测评实施和单元判定构成。

测评指标包括《信息安全技术 信息系统安全等级保护基本要求 第2部分：云计算安全扩展基本要求》第四级目录下的要求项。

测评对象是指测评实施的对象，即测评过程中涉及到的制度文档、各类设备及其安全配置和相关人员等。对于框架来说，每一个被测安全要求项（不同级别）均有一组与之相关的预先定义的测评对象（如制度文档、各类设备设施及相关人员等）。

制度文档是指针对等级保护对象所制定的相关联的文件（如：政策、程序、计划、系统安全需求、功能规格及建筑设计）。各类设备是指安装在等级保护对象之内或边界，能起到特定保护作用的相关部件（如：硬件、软件、固件或物理设施）。相关人员或部门，是指应用上述制度、设备及安全配置的人。

测评实施是一组针对特定测评对象，采用相关测评方法，遵从一定的测评规程所形成的，用于测评人员使用的确定该要求项有效性的程序化陈述。测评实施主要由测评方法和测评规程构成。其中测评方法包括：访谈、检查和测试（说明见术语），测评人员通过这些方法试图获取证据。上述的评估方法都由一组相关属性来规范测评方法的测评力度。这些属性是：广度（覆盖面）和深度。对于每一种测评方法都标识(定义）了唯一属性，深度特性适用于访谈和检查，而覆盖面特性则适用于全部三种测评方法，具体的描述参见附录 A。上述三种测评方法（访谈、检查和测评）的测评结果都用以对安全控制的有效性进行评估。测评规程是各类测评方法操作使用的过程、步骤，测评规程实施完成后，可以获得相应的证据。

结果判定描述测评人员执行测评实施并产生各种测评输出数据后，如何依据这些测评输出数据来判定被测系统是否满足测评指标要求的原则和方法。通过测评实施所获得的所有证据都满足要求则为符合，不全满足要求则该单项要求不符合。

整体测评是在单项测评基础上，分别从安全控制点测评，控制点间和层面间三个角度分别进行测评。各部分具体描述参见第 8 章“整体测评”。

4.2 测评使用方法

本标准应与 GB/T 28448.1-20XX 配合使用，对使用云计算相关技术的平台及系统，应根据实际情况抽取出对应 GB/T 22239.1-20XX、GB/T 22239.2-20XX 中要求项的测评要求，并按照这些测评要求开发测评指导书。同时，GB/T 22239.1-20XX 中，对于云管理平台、虚拟机监视器、虚拟网络设备、虚拟安全设备等云计算环境下新增测评对象同样具有安全控制要求，应参照 GB/T 28448.1-20XX 中相应测评要求开发其测评指导书，如：对云管理平台，可参照应用和数据安全部分；对虚拟机监视器，可参照设备和计算安全部分；对虚拟网络设备、虚拟安全设备，可参照网络和通信安全部分。

本标准第 5 章到第 7 章分别描述了第二级等级保护对象、第三级等级保护对象和第四级等级保护对象所有单项测评的内容，在章节上分别对应国标 GB/T 22239.2-20XX 的第 5 章到第 7 章。在国标 GB/T 22239.2-20XX 第 5 章到第 7 章中，各章的二级目录都分为安全技术和安全管理两部分，三级目录从安全层面（如物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全）进行划分和描述，四级目录按照安全控制点进行划分和描述（如设备和计算安全层面下分为身份鉴别、访问控制、安全审计、入侵防范、资源控制、镜像和快照保护等），第五级目录是每一个安全控制点下面包括的具体安全要求项（以下简称“要求项”，这些要求项在本标准中被称为“测评指标”）。本标准中针对每一个要求项的测评就构成一个单项测评，单项测评中的每一个具体测评实施要求项（以下简称“测评要求项”）是与安全控制点下面所包括的要求项（测评指标）相对应的。在对每一要求项进行测评时，可能用到访谈、检查和测试三种测试方法，也可能用到其中一种或两种。测评实施的内容完全覆盖了 GB/T 22239.2-20X 及 GB/T25070.2-20XX 中所有要求项的测评要求，使用时应当从单项测评的测评实施中抽取出对于 GB/T 22239.1-20XX 中每一个要求项的测评要求，并按照这些测评要求开发测评指导书，以规范和指导安全等级测评活动。

测评过程中测评人员应注意对测评记录和证据的采集、处理、存储和销毁，保护其在测评期间免遭破坏、更改或遗失并保守秘密。

测评的最终输出是测评报告，测评报告应结合第 9 章的要求给出等级测评结论。

5 第二级测评要求

5.1 安全技术单项测评

5.1.1 物理和环境安全

5.1.1.1 物理位置的选择

5.1.1.1.1 测评单元（L2-PES2-01）

a) 测评指标：确保云计算服务器、承载云租户账户信息、鉴别信息、系统信息及运行关键业务和数据的物理设备均位于中国境内。

b) 测评对象：记录类文档、办公场地和机房

c) 测评实施包括以下内容：

1）应检查办公场地（放置终端计算机设备）和机房，查看云计算服务器、承载云租户账户信息、鉴别信息、系统信息及运行关键业务和数据的物理设备是否均位于中国境内；

2）应检查记录类文档、办公场地和机房，查看云计算服务器、承载云租户账户信息、鉴别信息、系统信息及运行关键业务和数据的物理设备是否位于法规、合同和协议限定的地理位置之内；

d) 单元判定：如果1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

5.1.2 网络和通信安全

5.1.2.1 网络架构

5.1.2.1.1 测评单元（L2-NCS2-01）

a) 测评指标：实现不同云租户之间的网络隔离；

b) 测评对象：网络资源隔离措施、综合网管系统或云管理平台

c) 测评实施包括以下内容：

1）应检查云租户间网络资源隔离措施；
2）应检查综合网管系统或云管理平台，查看云租户之间网络资源隔离策略是否有效；

d) 单元判定：如果1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

5.1.2.1.2 测评单元（L2-NCS2-02）

a) 测评指标：绘制与当前运行情况相符的虚拟化网络拓扑结构图；

b) 测评对象：网络设备、安全设备或管理平台

c) 测评实施：应检查网络设备、安全设备或管理平台，查看网络拓朴结构图是否与当前运行情况相符；

d) 单元判定：如果c）为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

5.1.2.1.3 测评单元（L2-NCS2-03）

a) 测评指标：保证虚拟机只能接收到目的地址包括自己地址的报文；

b) 测评对象：虚拟机、广播网段

c) 测评实施包括以下内容：

1）应检查是否采用VLAN、SDN等技术手段隔离虚拟网络中不同租户的数据传输，保证云租户不能接收到目的地址不包括自己的非广播数据包。

2）应采用抓包等方式检查虚拟交换机或交换机，查看虚拟机是否只能接收到目的地址仅包括自己地址的报文；

3）应测试不同网段的虚拟机进行广播时，是否只能接收到目的地址包括自己地址的报文；

d) 单元判定：如果1）、2）或1）、3）为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

5.1.2.2 访问控制

5.1.2.2.1 测评单元（L2-NCS2-04）

a) 测评指标：在虚拟化网络边界部署访问控制机制，并设置访问控制规则；

b) 测评对象：访问控制机制，网络边界设备或虚拟化网络边界设备

c) 测评实施包括以下内容：

1）应检查云服务方和云租户虚拟化网络边界访问控制机制，查看访问控制规则和访问控制策略等；

2）应检查云服务方的网络边界设备或虚拟化网络边界设备，查看安全保障机制、访问控制规则或访问控制策略等；

3）应检查不同租户间访问时采用的访问控制机制或设备，对于访问控制机制，应查看所采取的机制是否已被测试是安全的（如第三方测试报告），对于访问控制设备，应查看访问控制设备的访问控制策略是否合理；

4）应检查租户内不同区域间访问时采用的访问控制机制或设备，对于访问控制机制，应查看所采取的机制是否已被测试是安全的（如第三方测试报告），对于访问控制设备，应查看访问控制设备的访问控制策略是否合理；，

5）应测试虚拟化网络边界访问控制设备，查看是否可以正确拒绝违反访问控制规则的非法访问。

d) 单元判定：如果1）-5)均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

5.1.2.2.2 测评单元（L2-NCS2-05）

a) 测评指标：保证当虚拟机迁移时，访问控制策略随其迁移；

b) 测评对象：虚拟机、虚拟机迁移记录及相关配置

c) 测评实施包括以下内容：

1）应检查虚拟机迁移时访问控制策略随之迁移的措施或手段；
2）应检查虚拟机迁移记录及相关配置，查看虚拟机迁移后访问控制策略是否部署；
3）应测试虚拟机迁移，查看访问控制措施是否随其迁移；

d) 单元判定：如果1）-3)均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

5.1.2.2.3 测评单元（L2-NCS2-06）

a) 测评指标：允许云租户设置不同虚拟机之间的访问控制策略；

b) 测评对象：云服务方管理平台、云租户管理系统、虚拟化网络边界访问控制设备

c) 测评实施包括以下内容：

1）应检查云服务方的云管理平台等，查看是否允许云租户设置不同虚拟机间访问控制策略；
2）应检查云服务方的云管理平台，查看是否存在不同虚拟机间的访问控制管理模块，是否开启该访问控制功能；
3）应检查云租户的云管理系统，查看不同虚拟机间访问控制策略是否安全；
4）应测试虚拟化网络边界访问控制设备，查看是否可以正确拒绝违反虚拟机间访问控制策略的非法访问。

d) 单元判定：如果1）、2）、4)或3）、4）为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

5.1.2.3 入侵防范

5.1.2.3.1 测评单元（L3-NCS2-07）

a) 测评指标：能检测到云租户的网络攻击行为，并能记录攻击类型、攻击时间、攻击流量等；

b) 测评对象：网络入侵防范设备或国家认可的相关机制、入侵防范措施

c) 测评实施包括以下内容：

1）应检查网络入侵防范措施，查看是否有专门设备对网络入侵进行防范，查看网络入侵防范规则库的升级方式；
2）应检查网络入侵防范设备或机制，当采用网络入侵防范机制时，应查看所采取的机制是否已被测试是安全的（如第三方测试报告），查看入侵防范设备或机制的规则库是否为最新；
3）应测试网络入侵防范设备或机制，当采用网络入侵防范机制时，应查看所采取的机制是否已被测试是安全的（如第三方测试报告），验证入侵防范设备或机制对异常流量和未知威胁的监控策略是否有效（如模拟产生攻击动作，查看网络入侵防范设备的反应，是否能记录攻击类型、攻击时间、攻击流量）；
4）应通过对外攻击发生器伪造对外攻击行为，检查云租的网络攻击的日志记录，确认是否正确记录到相应攻击行为，攻击行为日志记录是否包含攻击类型、攻击时间、攻击者IP、攻击流量规模等；

d) 单元判定：如果1）-4)均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

5.1.3 设备和计算安全

5.1.3.1 身份鉴别

5.1.3.1.1 测评单元（L2- ECS2-01）

a) 测评指标：对远程执行特权命令进行限制。

b) 测评对象：安全管理员，边界网络设备、网络虚拟化设备，云管理平台

c) 测评实施包括以下内容：

1）应访谈安全管理员，询问对远程执行特权命令的限制，询问是否对远程执行特权命令进行审计；
2）应检查边界网络设备、网络虚拟化设备，查看远程执行特权命令的限制措施，查看是否对远程执行特权命令的行为进行安全审计；

d) 单元判定：如果1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

5.1.3.1.2 测评单元（L2-ECS2-02）

a) 测评指标：应在网络策略控制器和网络设备（或设备代理）之间建立身份验证机制。

b) 测评对象：网络管理员，网络策略控制器，网络设备，网络虚拟化设备

c) 测评实施包括以下内容：

1）应访谈网络管理员，询问网络控制器和网络设备（或设备代理）之间是否建立身份验证机制；
2）应检查网络策略控制器和网络设备（或设备代理）之间的身份验证机制；
3）应对主要边界网络设备、网络虚拟化设备进行渗透测试，通过使用各种渗透测试技术（如口令猜解等）对网络设备进行渗透测试，验证网络设备防护能力是否符合要求，是否在网络控制器和网络设备（或设备代理）之间建立身份验证机制。

d) 单元判定：如果1）-3）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

5.1.3.2 访问控制

5.1.3.2.1 测评单元（L2- ECS2-03）

a) 测评指标：当进行远程管理时，管理终端和云计算平台边界设备之间应建立身份验证机制。

b) 测评对象：管理终端、云平台边界设备、日志记录

c) 测评实施包括以下内容：

1）应检查云管理平台，在进行远程管理时，管理终端和云平台边界设备之间是否建立身份验证机制；

2）应检查日志记录，查看是否通过相关安全组件对运维管理人员相关行为进行记录；

d) 单元判定：如果1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

5.1.3.3 安全审计

5.1.3.3.1 测评单元（L2-ECS2-04）

a) 测评指标：根据云服务方和云租户的职责划分，实现各自控制部分审计数据的收集；

b) 测评对象：主要服务器、宿主机及虚拟机的操作系统、主要终端操作系统、主要数据库系统、审计系统

c) 测评实施包括以下内容：

1）应检查主要服务器、宿主机及虚拟机的操作系统、主要终端操作系统和主要数据库系统的安全审计策略或审计数据，查看是否根据云服务方和云租户的职责进行划分，收集各自控制的部分的审计数据；
2）应检查审计系统，查看是否根据云服务方和云租户的职责进行划分，收集各自控制的部分的审计数据；

d) 单元判定：如果1）或2）为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

5.1.3.3.2 测评单元（L2-ECS2-05）

a) 测评指标：保证云服务方对云租户系统和数据的操作可被云租户审计；

b) 测评对象：主要服务器，宿主机及虚拟机的操作系统，主要终端操作系统，主要数据库系统，审计设备、审计数据

c) 测评实施包括以下内容：

1）应检查安全审计策略，查看安全审计配置是否能够保证云服务方对云租户系统和数据的操作（如增、删、改、查等操作）可被云租户审计；
2）应检查是否支持云租户部署第三方安全审计设备，保证云服务商对云租户系统和数据的操作可被租户审计。
3）应检查云服务方与云租户收集的审计数据，查看云服务方对云租户系统和数据的操作是否可被云租户审计。

d) 单元判定：如果1）-3）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

5.1.3.3.3 测评单元（L2-ECS2-06）

a) 测评指标：保证审计数据的真实性和完整性；

b) 测评对象：主要服务器，宿主机及虚拟机的操作系统，主要终端操作系统，主要数据库系统，审计系统

c) 测评实施：应检查主要服务器、宿主机及虚拟机的操作系统、主要终端操作系统和主要数据库

系统的安全审计策略，查看是否能够通过日志覆盖周期、存储方式、日志文件/空间大小、日志文件操作权限等设置，是否实现了对审计记录的保护，使其避免受到未预期的删除、修改或覆盖等，查看是否采取措施能够保证审计数据的真实性和完整性；

d) 单元判定：如果c）为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

5.1.3.4 入侵防范

5.1.3.4.1 测评单元（L2-ECS2-07）

a) 测评指标：能够检测虚拟机对宿主机资源的异常访问；

b) 测评对象：云管理平台、虚拟机监视器

c) 测评实施包括以下内容：

1) 应检查云管理平台等，查看能否检测虚拟机对宿主机的异常访问；
2) 应测试虚拟机监视器和云管理平台，验证是否能够及时检测到虚拟机异常访问宿主机资源等行为；

d) 单元判定：如果1）-2)均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

5.1.3.4.2 测评单元（L2-ECS2-08）

a) 测评指标：能够检测虚拟机之间的资源隔离失效，并进行告警；

b) 测评对象：主要服务器、宿主机及虚拟机，操作系统，主要数据库系统，虚拟机监视器，云平台

c) 测评实施

1) 应检查主要服务器、宿主机及虚拟机，虚拟机监视器，云平台是否采取措施对不同虚拟机的CPU、内存和磁盘资源进行隔离，是否实现不同云租户自有数据库之间的隔离；是否采取措施能够检测到虚拟机之间的资源隔离失效，并进行告警；
2) 应访谈系统管理员，询问是否采取措施对不同虚拟机资源进行了安全隔离，是否采取措施能够检测到虚拟机之间的资源隔离失效，并进行告警。

d) 单元判定：如果1）-2)均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

5.1.3.5 资源控制

5.1.3.5.1 测评单元（L2-ECS2-09）

a) 测评指标：屏蔽虚拟资源故障，某个虚拟机崩溃后不影响虚拟机监视器及其他虚拟机；

b) 测评对象：资源控制相关平台、云平台

c) 测评实施包括以下内容：

1）应检查资源控制相关平台，查看所采取的屏蔽虚拟资源故障措施，查看相关虚拟机故障记录，查看是否不存在虚拟机崩溃后影响虚拟机监视器及其他虚拟机的历史；
2）应检查云平台，查看所采取的屏蔽虚拟资源故障的技术手段，查看是否能在某个虚拟机崩溃后不影响虚拟机监视器及其他虚拟机；

d) 单元判定：如果1)-2)均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

5.1.3.5.2 测评单元（L2-ECS2-10）

a) 测评指标：对物理资源和虚拟资源按照策略做统一管理调度与分配；

b) 测评对象：云平台，虚拟机，虚拟机监视器，物理资源和虚拟资源

c) 测评实施包括以下内容：

1）应检查云租户的运营管理平台或资源调度平台，查看资源调度策略，查看资源调度分配情况；
2）应检查云服务方云管理平台，查看所提供策略能否对物理资源和虚拟资源做统一管理调度与分配；

d) 单元判定：如果1)-2)均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

5.1.3.5.3 测评单元（L2-ECS2-11）

a) 测评指标：保证虚拟机仅能使用为其分配的计算资源；

b) 测评对象：云管理平台，虚拟机、计算资源

c) 测评实施包括以下内容：

1）应检查云管理平台，查看计算资源分配情况，查看资源分配的审计记录或告警记录是否不存在资源过量占用警告，或资源分配机制能否实现虚拟机仅能使用为其分配的计算资源；
2）应测试虚拟机，当访问或使用管理员未分配的计算资源时，是否可以拒绝该请求，并有相应告警信息；

d) 单元判定：如果1)-2)均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

5.1.3.6 镜像和快照保护

5.1.3.6.1 测评单元（L2-ECS2-12）

a) 测评指标：提供虚拟机镜像、快照完整性校验功能，防止虚拟机镜像被恶意篡改；

b) 测评对象：云管理平台、虚拟机监视器、虚拟机镜像文件

c) 测评实施包括以下内容：

1）应检查虚拟机监视器，查看是否有对镜像文件定期进行有效性验证的记录；

2）应检查虚拟机监视器，云管理平台是否提供有效的虚拟机镜像和快照文件管理机制，虚拟

机是否能够及时被备份和快照，以及是否准确地恢复到所需还原点。

3) 应检查虚拟机监视器，云管理平台是否对快照功能生成的镜像或快照文件进行完整性校验，是否具有严格的校验记录机制，防止虚拟机镜像或快照被恶意篡改。

d) 单元判定：如果1)-3)均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

5.1.3.6.2 测评单元（L2-ECS2-13）

a) 测评指标:采取加密或其他技术手段防止虚拟机镜像、快照中可能存在的敏感资源被非法访问；

b) 测评对象：云管理平台、虚拟机监视器、虚拟机镜像文件

c) 测评实施：应检查虚拟机监视器，云管理平台是否对虚拟机镜像或快照中的敏感资源，通过加密、访问控制、权限控制等技术手段进行保护，防止可能存在的针对快照的非法访问。

d) 单元判定：如果c）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

5.1.3.6.3 测评单元（L2-ECS2-14）

a) 测评指标：针对重要业务系统提供加固的操作系统镜像。

b) 测评对象：云管理平台、虚拟机监视器、虚拟机镜像文件

c) 测评实施：应检查虚拟机监视器，云管理平台是否对生成的虚拟机镜像进行必要的加固措施，如关闭不必要的端口、服务及进行安全加固配置。

d) 单元判定：如果c）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

5.1.4 应用和数据安全

5.1.4.1 安全审计

5.1.4.1.1 测评单元（L2-ADS2-01）

a) 测评指标：根据云服务方和云租户的职责划分，实现各自控制部分审计数据的收集；

b) 测评对象：云管理平台、审计系统、审计数据

c) 测评实施包括以下内容：

1) 应检查云管理平台或审记系统，查看是否具备安全审计功能，查看审计策略及审计数据；
2) 应检查云服务方云管理平台或审记系统，查看是否根据云服务方和云租户的职责划分，收集各自控制部分的审计数据。查看审计策略，查看云服务方和云租户各自的审计内容；

d) 单元判定：如果1)-2)均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

5.1.4.1.2 测评单元（L2-ADS2-02）

a) 测评指标：保证云服务方对云租户系统和数据的操作可被云租户审计；

b) 测评对象：审计系统、审计数据

c) 测评实施：应检查审计系统，验证云服务方对云租户系统和数据的操作可以被云租户审计；

d) 单元判定：如果c）为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

5.1.4.1.3 测评单元（L2-ADS2-03）

a) 测评指标：保证审计数据的真实性和完整性；

b) 测评对象：审计系统、审计数据

c) 测评实施：应检查审记系统或各项审计数据，验证其是否对数据进行加密和完整性保护。

d) 单元判定：如果c）为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

5.1.4.2 资源控制

5.1.4.2.1 测评单元（L2-ADS2-04）

a) 测评指标：能够对应用系统的运行状况进行监测，并在发现异常时进行告警；

b) 测评对象：主要应用系统，开发平台

c) 测评实施：应检查应用系统，查看是否能够对应用系统的运行状况进行监测，包括应用运行异常、入侵攻击发生、扫描漏洞出现，并在发现异常时进行邮件或短信等方式的及时告警；

d) 单元判定：如果c)为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

5.1.4.2.2 测评单元（L3-ADS2-05）

a) 测评指标：保证不同云租户的应用系统及开发平台之间的隔离。

b) 测评对象：主要应用系统，开发平台

c) 测评实施包括以下内容：

1）应检查云服务方为实现云租户的应用系统与开发平台隔离所采取的保障措施；
2）应检查云租户的应用系统与开发平台是否隔离。

d) 单元判定：如果1）-2)均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

5.1.4.3 接口安全

5.1.4.3.1 测评单元（L2-ADS2-06）

a) 测评指标：保证云计算服务对外接口的安全性。

b) 测评对象：云计算服务对外接口

c) 测评实施包括以下内容：

1）应检查云计算服务对外接口的安全策略，如认证、加密等。
2）应测试云计算服务对外接口是否存在安全漏洞或安全隐患，测试方法可采取渗透测试或代码审计。

d) 单元判定：如果1）-2)均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

5.1.4.4 数据完整性

5.1.4.4.1 测评单元（L2-ADS2-07）

a) 测评指标：确保虚拟机迁移过程中，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。

b) 测评对象：虚拟机

c) 测评实施包括以下内容：

1）应检查虚拟资源迁移过程中采用的数据完整性保障措施及恢复措施；
2）应检查在虚拟资源迁移过程中，是否采取加密、签名等措施保证虚拟资源数据及重要数据的完整性，并在检测到完整性受到破坏时是否采取必要的恢复措施；

d) 单元判定：如果1）-2)均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

5.1.4.5 数据备份恢复

5.1.4.5.1 测评单元（L2-ADS2-08）

a) 测评指标：提供查询云租户数据及备份存储位置的方式；

b) 测评对象：系统管理员，网络管理员，数据库管理员，安全管理员，主要主机操作系统，主要网络设备、虚拟化网络设备操作系统，主要数据库管理系统，主要应用系统，网络拓扑结构，在线存储数据，虚拟机，虚拟机监视器，云平台

c) 测评实施包括以下内容：

1）应访谈系统管理员，询问是否能为云租户提供数据及备份存储的位置的查询；
2）应检查相关技术文档，查看云服务方是否为云租户提供数据及备份存储位置查询的接口或其他技术、管理手段；

d) 单元判定：如果1）-2)均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

5.1.4.6 剩余信息保护

5.1.4.6.1 测评单元（L2-ADS2-09）

a) 测评指标：应保证虚拟机所使用的内存和存储空间回收时得到完全清除。

b) 测评对象：系统管理员、虚拟机、虚拟机监视器系统，云管理平台系统，主要操作系统技术开发手册或产品检测报告，主要数据库系统技术开发手册或产品检测报告

c) 测评实施包括以下内容：

1）应访谈系统管理员，询问资源抽象层用户的鉴别信息存储空间，在回收时的数据清除策略，查看是否达到完全清除；
2）应访谈系统管理员，虚拟机监视器和云管理平台内的文件、目录、数据库记录和虚拟资源等所在的存储空间，在回收时的数据清除策略，查看是否达到完全清除；
3）应检查主要操作系统和主要数据库系统技术开发手册或产品检测报告，查看是否明确用户的鉴别信息存储空间回收时得到完全清除；
4）应检查主要操作系统和主要数据库系统技术开发手册或产品检测报告，是否明确文件、目录和数据库记录等资源所在的存储空间回收时得到完全清除。
5）应检查虚拟机监视器和云管理平台内的文件、目录、数据库记录和虚拟资源等所在的存储空间回收时是否得到完全清除；
6）应检查虚拟机的内存和存储空间回收时，是否得到完全清除；
7）应检查在迁移或删除虚拟机后，数据以及备份数据（如镜像文件、快照文件等）是否已清理。

d) 单元判定：如果1）-7)均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

5.2 安全管理单项测评

5.2.1 安全管理机构和人员

5.2.1.1 测评单元（L2-ORS2-01）

a) 测评指标：应保证云服务方对云租户业务数据的访问或使用必须经过云租户的授权，授权必须保留相关记录。

b) 测评对象：安全管理负责人，相关规章制度和流程

c) 测评实施包括以下内容：

1）应访谈安全管理负责人，询问云服务方对云租户业务数据的访问或使用是否必须经过云租户的授权；
2）应检查是否存在相应的规章制度和流程。

d) 单元判定：如果1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

5.2.2 系统安全建设管理

5.2.2.1 测试验收

5.2.2.1.1 测评单元（L2-CMS2-01）

a) 测评指标：应验证或评估所提供的安全措施的有效性。

b) 测评对象：系统建设负责人，资质证书，安全检测报告

c) 测评实施包括以下内容：

1）应访谈系统建设负责人，询问是否对所提供的安全措施的有效性进行验证和评估。
2）应检查相关评估记录和报告，查看是否对所提供安全措施的有效性进行了验证和评估；
3）应检查云服务方的相关资质证书检查或相关安全检测报告，查看是否对所提供安全措施的有效性进行了验证和评估。

d） 单元判定：如果1）-3）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

5.2.2.2 云服务商选择

5.2.2.2.1 测评单元（L2-CMS2-02）

a） 测评指标：确保云服务商的选择符合国家的有关规定；

b） 测评对象：系统建设负责人，相关流程或规章制度，服务合同

c） 测评实施包括以下内容：

1）应访谈系统建设负责人，询问向云计算平台提供安全规划、设计、实施、维护、测评等服务的安全服务单位和云服务供应商的过程是否符合国家有关规定；
2）应检查安全服务单位和云服务提供商的资质，查看是否符合国家的有关规定；

d） 单元判定：如果1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

5.2.2.2.2 测评单元（L2-CMS2-03）

a） 测评指标：选择安全合规的云服务商，其所提供的云平台应具备与信息系统等级相应的安全保护能力；

b） 测评对象：系统建设负责人，安全责任合同书或保密协议，服务合同，云平台

c） 测评实施包括以下内容：

1）应访谈系统管理员，询问是否根据业务系统的安全保护等级选择具有相应等级安全保护能力的云平台及云服务商；
2）应检查安全责任合同书或保密协议，服务合同，查看云服务商选择是否是否安全合规，查看是否根据业务系统的安全保护等级选择具有相应等级安全保护能力的云平台及云服务商。

d） 单元判定：如果1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

5.2.2.2.3 测评单元（L2-CMS2-04）

a） 测评指标：满足服务水平协议（SLA）要求；

b） 测评对象：系统建设负责人，服务水平协议（SLA），云平台

c） 测评实施包括以下内容：

1）应检查服务水平协议（SLA），查看相关服务水平协议内容；

2）应检查云平台，查看是否满足服务水平协议（SLA）要求。

d) 单元判定：如果1）—2）为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

5.2.2.2.4 测评单元（L2-CMS2-05）

a) 测评指标：在服务水平协议（SLA）中规定云服务的各项服务内容和具体技术指标；

b) 测评对象：系统建设负责人，服务水平协议（SLA），云平台

c) 测评实施包括以下内容：

1）应检查服务水平协议（SLA），查看是否规定了云服务的各项服务内容和具体指标、服务期限、双方签字或盖章等；
2）应检查云平台，查看是否有相关服务内容，查看云平台是否符合具体技术指标。

d) 单元判定：如果c)为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

5.2.2.2.5 测评单元（L2-CMS2-06）

a) 测评指标：在服务水平协议（SLA）中规定云服务商的权限与责任，包括管理范围、职责划分、访问授权、隐私保护、行为准则、违约责任等；

b) 测评对象：系统建设负责人，服务水平协议（SLA）

c) 测评实施：应检查服务水平协议（SLA），查看在服务水平协议（SLA）中规范了安全服务商和云服务供应商的权限与责任，包括管理范围、职责划分、访问授权、隐私保护、行为准则等；

d) 单元判定：如果c）为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

5.2.2.2.6 测评单元（L2-CMS2-07）

a) 测评指标：在服务水平协议（SLA）中规定云计算所能提供的安全服务的内容，并提供安全声明；

b) 测评对象：系统建设负责人，在服务水平协议（SLA）

c) 测评实施：应检查服务水平协议（SLA），查看是否规定了云计算所能提供的安全服务的内容，并提供安全声明；

d) 单元判定：如果c)为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

5.2.2.2.7 测评单元（L3-CMS2-08）

a) 测评指标：在服务水平协议（SLA）中规定服务合约到期时，完整地返还云租户信息，并承诺相关信息均已在云计算平台上清除；

b) 测评对象：系统建设负责人，在服务水平协议（SLA），云平台

c） 测评实施包括以下内容：

1）应检查服务水平协议（SLA），查看是否规定服务合约到期时，完整地返还云租户信息，并承诺相关信息均已在云平台上清除。
2）应检查云平台，查看是否采取措施保障服务合约到期时，完整地返还云租户信息，并承诺相关信息均已在云平台上清除；

d） 单元判定：如果1)-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

5.2.2.3 供应链管理

5.2.2.3.1 测评单元（L2-CMS2-09）

a） 测评指标：确保供应商的选择符合国家的有关规定；

b） 测评对象：安全主管，供应商资质

c） 测评实施包括以下内容：

1）应访谈云服务方安全主管，询问供应商的选择是否符合国家的有关规定；
2）应检查供应商资质，查看是否符合国家的有关规定；

d） 单元判定：如果1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

5.2.2.3.2 测评单元（L2-CMS2-10）

a） 测评指标：应确保供应链安全事件信息或威胁信息能够及时传达到云租户。

b） 测评对象：安全主管

c） 测评实施：应检查安全风险评估报告和风险预案，确认对每次供应商的重要变更都进行评估与风险预案设计。

d） 单元判定：如果c）为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

6 第三级测评要求

6.1 安全技术单项测评

6.1.1 物理和环境安全

6.1.1.1 物理位置的选择

6.1.1.1.1 测评单元（L3-PES2-01）

a） 测评指标：确保云计算服务器、承载云租户账户信息、鉴别信息、系统信息及运行关键业务和数据的物理设备均位于中国境内。

b） 测评对象：记录类文档、办公场地和机房

c) 测评实施包括以下内容：

1）应检查办公场地（放置终端计算机设备）和机房，查看云计算服务器、承载云租户账户信息、鉴别信息、系统信息及运行关键业务和数据的物理设备是否均位于中国境内；
2）应检查记录类文档、办公场地和机房，查看云计算服务器、承载云租户账户信息、鉴别信息、系统信息及运行关键业务和数据的物理设备是否位于法规、合同和协议限定的地理位置之内；

d) 单元判定：如果1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

6.1.2 网络和通信安全

6.1.2.1 网络架构

6.1.2.1.1 测评单元（L3-NCS2-01）

a) 测评指标：实现不同云租户之间的网络隔离；

b) 测评对象：网络资源隔离措施、综合网管系统或云管理平台

c) 测评实施包括以下内容：

1）应检查云租户间网络资源隔离措施；
2）应检查综合网管系统或云管理平台，查看云租户之间网络资源隔离策略是否有效；

d) 单元判定：如果1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

6.1.2.1.2 测评单元（L3-NCS2-02）

a) 测评指标：绘制与当前运行情况相符的虚拟化网络拓扑结构图，并能对虚拟化网络资源、网络拓扑进行实时更新和集中监控；

b) 测评对象：综合网管系统或云管理平台，网络拓扑图，网络设备、安全设备或管理平台

c) 测评实施包括以下内容：

1）应检查云服务方综合网管系统、云管理平台或云租户管理平台，检查是否对虚拟化网络资源（如虚拟交换机、虚拟防火墙等）、虚拟网络拓扑进行实时更新和集中监控；
2）应检查网络设备、安全设备或管理平台，查看网络拓朴结构图是否与当前运行情况相符；

d) 单元判定：如果1）-2）为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

6.1.2.1.3 测评单元（L3-NCS2-03）

a) 测评指标：保证虚拟机只能接收到目的地址包括自己地址的报文；

b) 测评对象：虚拟机、广播网段

c) 测评实施包括以下内容：

1）应检查是否采用VLAN、SDN等技术手段隔离虚拟网络中不同租户的数据传输，保证云租户不能接收到目的地址不包括自己的非广播数据包。

2）应采用抓包等方式检查虚拟交换机或交换机，查看虚拟机是否只能接收到目的地址仅包括自己地址的报文；

3）应测试不同网段的虚拟机进行广播时，是否只能接收到目的地址包括自己地址的报文；

d) 单元判定：如果1）、2）或1）、3）为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

6.1.2.1.4 测评单元（L3-NCS2-04）

a) 测评指标：保证云计算平台管理流量与云租户业务流量分离；

b) 测评对象：网络架构、云管理平台

c) 测评实施包括以下内容：

1）应检查网络架构和配置策略，查看能否采用带外管理或策略配置等方式实现管理流量和业务流量分离；

2）应检查云管理平台，查看云平台管理流量与云租户业务流量是否分离，查看所采取的技术手段和流量分离手段；

3）应测试云计算平台管理流量与业务流量是否分离。

d) 单元判定：如果1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

6.1.2.1.5 测评单元（L3-NCS2-05）

a) 测评指标：能识别、监控虚拟机之间、虚拟机与物理机之间的流量；

b) 测评对象：虚拟机监视器、云管理平台

c) 测评实施：应检查虚拟机监视器、云管理平台等，查看同一宿主机内虚拟机之间、虚拟机与物理机之间流量是否能被识别、监控；查看不同宿主机的虚拟机之间、虚拟机与物理机之间流量是否能被识别、监控。

d) 单元判定：如果c）为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

6.1.2.1.6 测评单元（L3-NCS2-06）

a) 测评指标：根据承载的业务系统安全保护等级划分不同安全级别资源池，并实现资源池之间的网络隔离；

b) 测评对象：资源池、业务系统、私有云

c) 测评实施包括以下内容：

1）应查看不同安全等级的业务系统是否对应不同资源池，查看资源池隔离所采用的机制和技术，查看资源池间访问控制策略及隔离机制；

2）应测试对不同安全等级资源池间进行非法访问时，是否可以正确拒绝该非法访问；

3）当被测系统为私有云，且无资源池划分需求时，不同等级资源间访问应可追责，实现不同等级资源间网络隔离；

d) 单元判定：如果1）、2)或3） 为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

6.1.2.1.7 测评单元（L3-NCS2-07）

a) 测评指标：提供开放接口或开放性安全服务，允许云租户接入第三方安全产品或在云平台选择第三方安全产品、服务，加强云租户虚拟机之间、安全区域之间的网络安全防护能力；

b) 测评对象：系统管理员，相关接口，相关服务

c) 测评实施包括以下内容：

1）应检查接口设计文档或开放性服务技术文档，查看是否符合开放性及安全性要求；
2）如果提供开放接口，应检查内部通信网络（虚拟网络）为第三方安全产品所提供的开放接口，查看接口安全保障机制，查看接口配置或参数；
3）如果提供开放性安全产品、服务，应查看开放性安全产品及服务的服务内容和实现开放性安全服务所采用的技术手段，查看安全保障机制。

d) 单元判定：如果1）、2）或1）、3）为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

6.1.2.1.8 测评单元（L3-NCS2-08）

a) 测评指标：根据云租户的业务需求定义安全访问路径。

b) 测评对象：云平台、网络设备、安全访问路径

c) 测评实施包括以下内容：

1）应检查云服务方的云管理平台或网络设备，查看能否根据云租户业务需求定义网络安全访问路径，查看其安全策略；
2）应检查云租户的网络管理平台或网络设备，查看是否已定义安全访问路径，查看其安全策略；
3）检查云服务商管理员进行远程管理时，管理终端与管理服务器之间所建立的安全访问路径。

d) 单元判定：如果1）、3）或2）为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

6.1.2.2 访问控制

6.1.2.2.1 测评单元（L3-NCS2-09）

a) 测评指标：在虚拟化网络边界部署访问控制机制，并设置访问控制规则；

b) 测评对象：访问控制机制，网络边界设备或虚拟化网络边界设备

c) 测评实施包括以下内容：

1）应检查云服务方和云租户虚拟化网络边界访问控制机制，查看访问控制规则和访问控制策略等；
2）应检查云服务方的网络边界设备或虚拟化网络边界设备，查看安全保障机制、访问控制规则或访问控制策略等；
3）应检查不同租户间访问时采用的访问控制机制或设备，对于访问控制机制，应查看所采取的机制是否已被测试是安全的（如第三方测试报告），对于访问控制设备，应查看访问控制设备的访问控制策略是否合理；
4）应检查租户内不同区域间访问时采用的访问控制机制或设备，对于访问控制机制，应查看所采取的机制是否已被测试是安全的（如第三方测试报告），对于访问控制设备，应查看访问控制设备的访问控制策略是否合理；，
5）应测试虚拟化网络边界访问控制设备，查看是否可以正确拒绝违反访问控制规则的非法访问。

d) 单元判定：如果1）-5)均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

6.1.2.2.2 测评单元（L3-NCS2-10）

a) 测评指标：保证当虚拟机迁移时，访问控制策略随其迁移；

b) 测评对象：虚拟机、虚拟机迁移记录及相关配置

c) 测评实施包括以下内容：

1）应检查虚拟机迁移时访问控制策略随之迁移的措施或手段；
2）应检查虚拟机迁移记录及相关配置，查看虚拟机迁移后访问控制策略是否部署；
3）应测试虚拟机迁移，查看访问控制措施是否随其迁移；

d) 单元判定：如果1）-3)均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

6.1.2.2.3 测评单元（L3-NCS2-11）

a) 测评指标：允许云租户设置不同虚拟机之间的访问控制策略；

b) 测评对象：云服务方管理平台、云租户管理系统、虚拟化网络边界访问控制设备

c) 测评实施包括以下内容：

1）应检查云服务方的云管理平台等，查看是否允许云租户设置不同虚拟机间访问控制策略；
2）应检查云服务方的云管理平台，查看是否存在不同虚拟机间的访问控制管理模块，是否开启该访问控制功能；
3）应检查云租户的云管理系统，查看不同虚拟机间访问控制策略是否安全；
4）应测试虚拟化网络边界访问控制设备，查看是否可以正确拒绝违反虚拟机间访问控制策略的非法访问。

d) 单元判定：如果1）、2）、4)或3）、4）为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

6.1.2.2.4 测评单元（L3-NCS2-12）

a) 测评指标：在不同等级的网络区域边界部署访问控制机制，设置访问控制规则

b) 测评对象：边界访问控制机制或边界访问控制设备

c) 测评实施包括以下内容：

1）应检查不同安全等级网络区域边界的访问控制机制部署情况，查看访问控制规则；
2）应测试不同安全等级的网络区域间进行非法访问时，是否可以正确拒绝该非法访问；

d) 单元判定：如果1）-2)均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

6.1.2.3 入侵防范

6.1.2.3.1 测评单元（L3-NCS2-13）

a) 测评指标：能检测到云租户的网络攻击行为，并能记录攻击类型、攻击时间、攻击流量等；

b) 测评对象：网络入侵防范设备或国家认可的相关机制、入侵防范措施

c) 测评实施包括以下内容：

1）应检查网络入侵防范措施，查看是否有专门设备对网络入侵进行防范，查看网络入侵防范规则库的升级方式；
2）应检查网络入侵防范设备或机制，当采用网络入侵防范机制时，应查看所采取的机制是否已被测试是安全的（如第三方测试报告），查看入侵防范设备或机制的规则库是否为最新；
3）应测试网络入侵防范设备或机制，当采用网络入侵防范机制时，应查看所采取的机制是否已被测试是安全的（如第三方测试报告），验证入侵防范设备或机制对异常流量和未知威胁的监控策略是否有效（如模拟产生攻击动作，查看网络入侵防范设备的反应，是否能记录攻击类型、攻击时间、攻击流量）；
4）应检查系统是否具备异常流量、大规模攻击流量、高级持续性攻击的检测功能、报警功能和清洗处置功能；
5）应检查是否具有对SQL注入、跨站脚本等攻击进行检测发现并阻断的能力；
6）应具有对恶意虚拟机，如具有恶意行为、过分占用计算资源和带宽资源等的虚拟机，进行检测的能力；
7）应检查云管理平台等，查看对云租户攻击的防范措施，查看对云租户的网络攻击行为的记录情况，记录应包括攻击类型、攻击时间、攻击流量等；
8）应测试主要网络入侵防范设备或机制，验证其云租户网络攻击报警报警策略是否有效（如模拟产生攻击动作，查看网络入侵防范设备是否能实时报警）；
9）应对云平台内部发起的恶意攻击或恶意对外连接的行为进行限制，查看是否对内部行为进行监控，查看相关日志记录。
10）应通过对外攻击发生器伪造对外攻击行为，检查云租的网络攻击的日志记录，确认是否正确记录到相应攻击行为，攻击行为日志记录是否包含攻击类型、攻击时间、攻击者IP、攻击流量规模等；
11）应检查运行虚拟机监控器（VMM）和云管理平台软件的物理主机，查看其安全加固手段是否能够应对虚拟化共享带来的安全漏洞。

d) 单元判定：如果1）-11)均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保

护对象不符合或部分符合本单项测评指标要求。

6.1.2.3.2 测评单元（L3-NCS2-14）

a) 测评指标：向云租户提供互联网发布内容监测功能，便于云租户对其发布内容中的有害信息进行实时监测和告警。

b) 测评对象：安全管理员，云平台

c) 测评实施包括以下内容：

1）应检查云服务方安全服务，查看是否可为云租户提供互联网发布内容监测功能；
2）应检查相关安全组件，查看云租户能否对其发布到互联网的有害信息进行实时监测和告警；
3）应检查云租户对其发布到互联网有害信息的实时监测情况以及历史告警信息。
4）应检查云租户设置的有害信息过滤规则，查看过滤规则是否可对常见有害信息进行过滤；

d) 单元判定：如果1）-2)均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

6.1.2.4 安全审计

6.1.2.4.1 测评单元（L3-NCS2-15）

a) 测评指标：对远程执行特权命令进行审计；

b) 测评对象：边界网络设备、网络虚拟化设备、相关审计数据

c) 测评实施包括以下内容：

1）应检查审计数据，查看执行远程特权命令后是否有相关审计记录；
2）当云服务方采用第三方运维时，应检查第三方运维方是否向云服务方提供审计数据，或云服务方是否可采取措施收集相关审计数据；
3）应检查边界网络设备、网络虚拟化设备，查看远程执行特权命令的限制措施，查看是否对远程执行特权命令的行为进行安全审计；

d) 单元判定：如果1）-3)均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

6.1.2.4.2 测评单元（L3-NCS2-16）

a) 测评指标:根据云服务方和云租户的职责划分,实现各自控制部分审计数据的收集和集中审计；

b) 测评对象：审计数据收集系统或设备、云管理平台、审计数据

c) 测评实施包括以下内容：

1）应检查云服务方审计数据收集系统或设备，查看是否根据云服务方和云租户的职责划分实现各自控制部分审计数据的收集和集中审计；
2）如果云租户授权云服务方收集部分云租户控制的审计数据，应检查云服务方是否在不影响其他云租户安全的前提下将云租户审计数据提供给云租户；
3）应检查云服务方审计数据，查看是否不包括云租户控制部分的审计数据；
4）应检查云服务方和云租户云管理平台，查看集中审计结果；

5）应检查是否支持云租户部署第三方安全审计设备，实现云租户职责范围内的集中审计；

d) 单元判定：如果1）-5)均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

6.1.2.4.3 测评单元（L3-NCS2-17）

a) 测评指标：为安全审计数据的汇集提供接口，并可供第三方审计；

b) 测评对象：边界网络设备，网络虚拟化设备，审计数据汇集接口，审计数据

c) 测评实施：应检查主要边界网络设备、网络虚拟化设备、审计系统或云管理平台，查看是否为安全审计数据的汇集提供接口，并可供第三方审计；

d) 单元判定：如果c）为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

6.1.3 设备和计算安全

6.1.3.1 身份鉴别

6.1.3.1.1 测评单元（L3- ECS2-01）

a) 测评指标:当进行远程管理时,管理终端和云计算平台边界设备之间应建立双向身份验证机制。

b) 测评对象：管理终端、云平台边界设备、日志记录

c) 测评实施包括以下内容：

1）应检查云管理平台，在进行远程管理时，管理终端和云平台边界设备之间是否建立双向身份验证机制（如证书、共享密钥等），应限制访问重要物理资源及虚拟资源、安全管理中心的远程登录地址；
2）应检查日志记录，查看是否通过相关安全组件对运维管理人员相关行为进行记录和告警；

d) 单元判定：如果1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

6.1.3.1.2 测评单元（L3-ECS2-02）

a) 测评指标：应在网络策略控制器和网络设备（或设备代理）之间建立双向身份验证机制。

b) 测评对象：网络管理员，网络策略控制器，网络设备，虚拟化网络设备

c) 测评实施包括以下内容：

1）当采用SDN方式时，应检查网络策略控制器和网络设备（或设备代理）之间是否建立双向身份验证机制；
2) 当采用SDN方式时，应对网络策略控制器和网络设备（代理设备）进行渗透测试，通过使用各种渗透测试技术（如口令猜解等）对网络设备进行渗透测试，验证网络设备防护能力是否符合要求，是否在网络策略控制器和网络设备（或设备代理）之间建立双向身份验证机制。

d) 单元判定：如果1）-3)均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护

对象不符合或部分符合本单项测评指标要求。

6.1.3.2 访问控制

6.1.3.2.1 测评单元（L3-ECS2-03）

a) 测评指标：当进行远程管理时，防止远程管理设备同时直接连接其他网络；

b) 测评对象：系统管理员，云平台，数据库，运维终端，远程管理设备，云平台运维管理员，云服务运营管理员

c) 测评实施：应检查运维终端，查看是否为专用，查看当进行远程管理时，是否能够防止远程管理设备同时直接连接到其他网络资源；

d) 单元判定：如果c）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

6.1.3.2.2 测评单元（L3-ECS2-04）

a) 测评指标：确保只有在云租户授权下，云服务方或第三方才具有云租户数据的管理权限；

b) 测评对象：云平台，数据库，运维终端，远程管理设备

c) 测评实施包括以下内容：

1）应检查云服务方所采取的措施，以确保只有在云租户授权情况下才具有云租户数据的管理权限，查看该措施能否有效避免云服务方非授权管理云租户数据；

2）应测试数据库系统，验证云服务方是否不能对云租户非授权数据进行管理；

d) 单元判定：如果1）-2)均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

6.1.3.2.3 测评单元（L3-ECS2-05）

a) 测评指标：提供云计算平台管理用户权限分离机制，为网络管理员、系统管理员建立不同账户并分配相应的权限。

b) 测评对象：云管理平台、相关文档

c) 测评实施包括以下内容：

1）应检查云租户云的云管理平台，查看云平台运维管理员和云服务运营管理员的权限是否分离，查看网络管理员、系统管理员是否建立不同账户并分配相应的权限；

2）应检查云服务方的云管理平台，是否提供云平台管理用户权限分离机制，能够为网络管理、系统管理建立不同账户并分配相应的权限；

d) 单元判定：如果1）-2)均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

6.1.3.3 安全审计

6.1.3.3.1 测评单元（L3-ECS2-06）

a) 测评指标：根据云服务方和云租户的职责划分，实现各自控制部分审计数据的收集和集中审计；

b) 测评对象：系统管理员，主要服务器，宿主机及虚拟机的操作系统，主要终端操作系统，主要数据库系统，审计系统

c) 测评实施包括以下内容：

1）应检查主要服务器、宿主机及虚拟机的操作系统、主要终端操作系统和主要数据库系统的安全审计策略或审计数据，查看是否根据云服务方和云租户的职责进行划分，收集各自控制的部分的审计数据；
2）应检查审计系统，查看是否根据云服务方和云租户的职责进行划分，收集各自控制的部分的审计数据；

d) 单元判定：如果1）或2）为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

6.1.3.3.2 测评单元（L3-ECS2-07）

a) 测评指标：保证云服务方对云租户系统和数据的操作可被云租户审计；

b) 测评对象：主要服务器，宿主机及虚拟机的操作系统，主要终端操作系统，主要数据库系统，审计设备、审计数据

c) 测评实施包括以下内容：

1）应检查安全审计策略，查看安全审计配置是否能够保证云服务方对云租户系统和数据的操作（如增、删、改、查等操作）可被云租户审计；
2）应检查是否支持云租户部署第三方安全审计设备，保证云服务商对云租户系统和数据的操作可被租户审计。
3）应检查云服务方与云租户收集的审计数据，查看云服务方对云租户系统和数据的操作是否可被云租户审计。

d) 单元判定：如果1）-3）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

6.1.3.3.3 测评单元（L3-ECS2-08）

a) 测评指标：保证审计数据的真实性和完整性；

b) 测评对象：主要服务器，宿主机及虚拟机的操作系统，主要终端操作系统，主要数据库系统，审计系统

c) 测评实施：应检查主要服务器、宿主机及虚拟机的操作系统、主要终端操作系统和主要数据库系统的安全审计策略，查看是否能够通过日志覆盖周期、存储方式、日志文件/空间大小、日志文件操作权限等设置，是否实现了对审计记录的保护，使其避免受到未预期的删除、修改或覆盖等，查看是否采取措施能够保证审计数据的真实性和完整性；

d) 单元判定：如果c）为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

6.1.3.3.4 测评单元（L3-ECS2-09）

a) 测评指标：为安全审计数据的汇集提供接口，并可供第三方审计；

b) 测评对象：主要服务器，宿主机及虚拟机的操作系统，主要终端操作系统，主要数据库系统，审计系统

c) 测评实施：应检查主要服务器、宿主机及虚拟机的操作系统、主要终端操作系统和主要数据库系统的安全审计策略，是否能够进行例如日志数据等各类审计数据的集中，并设置安全可信的接口以供访问上述数据，如存在需要进行第三方集中审计的情况下，实现集中审计或第三方审计。

d) 单元判定：如果c）为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

6.1.3.4 入侵防范

6.1.3.4.1 测评单元（L3-ECS2-10）

a) 测评指标：能够检测虚拟机对宿主机资源的异常访问，并进行告警；

b) 测评对象：云管理平台、虚拟机监视器

c) 测评实施包括以下内容：

1) 应检查云管理平台等，查看能否检测虚拟机对宿主机的异常访问，并查看告警机制；
2) 应测试虚拟机监视器和云管理平台，验证是否能够及时检测到虚拟机异常访问宿主机资源等行为并进行报警，如利用虚机逃逸漏洞验证是否触发报警；

d) 单元判定：如果1）-2)均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

6.1.3.4.2 测评单元（L3-ECS2-11）

a) 测评指标：能够检测虚拟机之间的资源隔离失效，并进行告警；

b) 测评对象：主要服务器、宿主机及虚拟机，操作系统，主要数据库系统，虚拟机监视器，云平台

c) 测评实施

1) 应检查主要服务器、宿主机及虚拟机，虚拟机监视器，云平台是否采取措施对不同虚拟机的CPU、内存和磁盘资源进行隔离，是否实现不同云租户自有数据库之间的隔离；是否采取措施能够检测到虚拟机之间的资源隔离失效，并进行告警；
2) 应访谈系统管理员，询问是否采取措施对不同虚拟机资源进行了安全隔离，是否采取措施能够检测到虚拟机之间的资源隔离失效，并进行告警。

d) 单元判定：如果1）-2)均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

6.1.3.4.3 测评单元（L3-ECS2-12）

a) 测评指标：能检测到非授权新建虚拟机或者重新启用虚拟机，并进行告警；

b) 测评对象：主要服务器、宿主机及虚拟机，操作系统，主要数据库系统，虚拟机监视器，云平台

c) 测评实施：应检查主要服务器、宿主机及虚拟机，操作系统，主要数据库系统，虚拟机监视器，云平台是否能够检测到非授权新建虚拟机或者重新启用虚拟机，并进行告警。

d) 单元判定：如果c）为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

6.1.3.5 恶意代码防范

6.1.3.5.1 测评单元（L3-ECS2-13）

a) 测评指标：能够检测恶意代码感染及在虚拟机间蔓延的情况，并提出告警。

b) 测评对象：主要服务器、虚拟机监视器，宿主机及虚拟机、云平台，主要终端，防恶意代码软件或硬件，网络防恶意代码产品

c) 测评实施包括以下内容：

1）应检查主要服务器、宿主机、虚拟机、终端、虚拟机监视器、云平台是否建立恶意代码传播路径追踪机制，是否可以检测查看恶意代码的感染情况，并提出告警。
2）应检查主要服务器、宿主机、虚拟机、终端，虚拟机监视器，云平台是否能够检测恶意代码感染及在虚拟机间蔓延的情况，是否能够检测出虚拟机的恶意行为，并提出告警。

d) 单元判定：如果1）-2)均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

6.1.3.6 资源控制

6.1.3.6.1 测评单元（L3-ECS2-14）

a) 测评指标：屏蔽虚拟资源故障，某个虚拟机崩溃后不影响虚拟机监视器及其他虚拟机；

b) 测评对象：资源控制相关平台、云平台

c) 测评实施包括以下内容：

1）应检查资源控制相关平台，查看所采取的屏蔽虚拟资源故障措施，查看相关虚拟机故障记录，查看是否不存在虚拟机崩溃后影响虚拟机监视器及其他虚拟机的历史；
2）应检查云平台，查看所采取的屏蔽虚拟资源故障的技术手段，查看是否能在某个虚拟机崩溃后不影响虚拟机监视器及其他虚拟机；

d) 单元判定：如果1)-2)均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

6.1.3.6.2 测评单元（L3-ECS2-15）

a) 测评指标：对物理资源和虚拟资源按照策略做统一管理调度与分配；

b) 测评对象：云平台，虚拟机，虚拟机监视器，物理资源和虚拟资源

c) 测评实施包括以下内容：

1）应检查云租户的运营管理平台或资源调度平台，查看资源调度策略，查看资源调度分配情况；
2）应检查云服务方云管理平台，查看所提供策略能否对物理资源和虚拟资源做统一管理调度与分配；

d） 单元判定：如果1)-2)均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

6.1.3.6.3 测评单元（L3-ECS2-16）

a） 测评指标：保证虚拟机仅能使用为其分配的计算资源；

b） 测评对象：云管理平台，虚拟机、计算资源

c） 测评实施包括以下内容：

1）应检查云管理平台，查看计算资源分配情况，查看资源分配的审计记录或告警记录是否不存在资源过量占用警告，或资源分配机制能否实现虚拟机仅能使用为其分配的计算资源；
2）应测试虚拟机，当访问或使用管理员未分配的计算资源时，是否可以拒绝该请求，并有相应告警信息；

d） 单元判定：如果1)-2)均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

6.1.3.6.4 测评单元（L3-ECS2-17）

a） 测评指标：保证虚拟机仅能迁移至相同安全等级的资源池。

b） 测评对象：系统管理员、虚拟机迁移记录

c） 测评实施包括以下内容：

1）应访谈系统管理员，询问虚拟机迁移时是否仅迁移至相同安全等级的资源池。
2）应检查虚拟机迁移记录，查看是否存在虚拟机迁移至不同安全等级资源池的情况。

d） 单元判定：如果1）-2)均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

6.1.3.6.5 测评单元（L3-ECS2-18）

a） 测评指标：保证分配给虚拟机的内存空间仅供其独占访问；

b） 测评对象：云平台

c） 测评实施包括以下内容：

1）应检查云平台，采取了何种技术手段，以保证分配给虚拟机的内存空间仅供其独占访问；
2）应检查云平台，查看是否采取安全机制保障同一物理地址段被不同用户使用；

d） 单元判定：如果c）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

6.1.3.6.6 测评单元（L3-ECS2-19）

a) 测评指标：对虚拟机的网络接口的带宽进行设置，并进行监控；

b) 测评对象：云管理平台或其他安全组件

c) 测评实施包括以下内容：

1）应检查云管理平台或其他安全组件，查看是否能对虚拟机网络接口带宽进行设置，查看能否对其进行监控；
2）应检查云管理平台，查看虚拟机的网络接口带宽的配置及参数，并查看带宽监控记录；

d) 单元判定：如果1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

6.1.3.6.7 测评单元（L3-ECS2-20）

a) 测评指标：为监控信息的汇集提供接口，并实现集中监控。

b) 测评对象：云平台，监控信息汇集接口

c) 测评实施包括以下内容：

1）应检查云平台，查看是否为CPU、内存、流量和安全等监控信息的汇集提供了接口，并实现集中监控；
2）应检查CPU、内存、流量和安全等监控信息汇集接口配置或参数，查看集中监控措施和记录；

d) 单元判定：如果1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

6.1.3.7 镜像和快照保护

6.1.3.7.1 测评单元（L3-ECS2-21）

a) 测评指标：提供虚拟机镜像、快照完整性校验功能，防止虚拟机镜像被恶意篡改；

b) 测评对象：云管理平台、虚拟机监视器、虚拟机镜像文件

c) 测评实施包括以下内容：

1) 应检查虚拟机监视器，查看是否有对镜像文件定期进行有效性验证的记录；

2) 应检查虚拟机监视器，云管理平台是否提供有效的虚拟机镜像和快照文件管理机制，虚拟机是否能够及时被备份和快照，以及是否准确地恢复到所需还原点。

3) 应检查虚拟机监视器，云管理平台是否对快照功能生成的镜像或快照文件进行完整性校验，是否具有严格的校验记录机制，防止虚拟机镜像或快照被恶意篡改。

d) 单元判定：如果1)-3)均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

6.1.3.7.2 测评单元（L3-ECS2-22）

a) 测评指标:采取加密或其他技术手段防止虚拟机镜像、快照中可能存在的敏感资源被非法访问；

b) 测评对象：云管理平台、虚拟机监视器、虚拟机镜像文件

c) 测评实施：应检查虚拟机监视器，云管理平台是否对虚拟机镜像或快照中的敏感资源，通过加密、访问控制、权限控制等技术手段进行保护，防止可能存在的针对快照的非法访问。

d) 单元判定：如果c）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

6.1.3.7.3 测评单元（L3-ECS2-23）

a) 测评指标：针对重要业务系统提供加固的操作系统镜像。

b) 测评对象：云管理平台、虚拟机监视器、虚拟机镜像文件

c) 测评实施：应检查虚拟机监视器，云管理平台是否对生成的虚拟机镜像进行必要的加固措施，如关闭不必要的端口、服务及进行安全加固配置。

d) 单元判定：如果c）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

6.1.4 应用和数据安全

6.1.4.1 安全审计

6.1.4.1.1 测评单元（L3-ADS2-01）

a) 测评指标:根据云服务方和云租户的职责划分,实现各自控制部分审计数据的收集和集中审计；

b) 测评对象：云管理平台、审计系统、审计数据

c) 测评实施包括以下内容：

1）应检查云管理平台或审记系统，查看是否具备安全审计功能，查看审计策略及审计数据；
2）应检查云服务方云管理平台或审记系统，查看是否根据云服务方和云租户的职责划分，收集各自控制部分的审计数据。查看审计策略，查看云服务方和云租户各自的审计内容；
3）应检查云服务方和云租户收集的审计数据，查看是否根据云服务方和云租户的职责划分，实现了各自控制部分的集中审计。

d) 单元判定：如果1)-2)均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

6.1.4.1.2 测评单元（L3-ADS2-02）

a) 测评指标：保证云服务方对云租户系统和数据的操作可被云租户审计；

b) 测评对象：审计系统、审计数据

c) 测评实施：应检查审计系统，验证云服务方对云租户系统和数据的操作可以被云租户审计；

d) 单元判定：如果c）为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

6.1.4.1.3 测评单元（L3-ADS2-03）

a) 测评指标：保证审计数据的真实性和完整性；

b) 测评对象：审计系统、审计数据

c) 测评实施：应检查审记系统或各项审计数据，验证其是否对数据进行加密和完整性保护。

d) 单元判定：如果c）为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

6.1.4.1.4 测评单元（L3-ADS2-04）

a) 测评指标：为安全审计数据的汇集提供接口，并可供第三方审计；

b) 测评对象：主要应用系统、审计数据汇集接口

c) 测评实施：应检查主要应用系统，查看是否为安全审计数据的汇集提供接口，并能对汇集的数据进行集中审计或第三方审计；

d) 单元判定：如果c）为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

6.1.4.2 资源控制

6.1.4.2.1 测评单元（L3-ADS2-05）

a) 测评指标：能够对应用系统的运行状况进行监测，并在发现异常时进行告警；

b) 测评对象：主要应用系统，开发平台

c) 测评实施：应检查应用系统，查看是否能够对应用系统的运行状况进行监测，包括应用运行异常、入侵攻击发生、扫描漏洞出现，并在发现异常时进行邮件或短信等方式的及时告警；

d) 单元判定：如果c)为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

6.1.4.2.2 测评单元（L3-ADS2-06）

a) 测评指标：保证不同云租户的应用系统及开发平台之间的隔离。

b) 测评对象：主要应用系统，开发平台

c) 测评实施包括以下内容：

1）应检查云服务方为实现云租户的应用系统与开发平台隔离所采取的保障措施；
2）应检查云租户的应用系统与开发平台是否隔离。

d) 单元判定：如果1）-2)均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

6.1.4.3 接口安全

6.1.4.3.1 测评单元（L3-ADS2-07）

a) 测评指标：保证云计算服务对外接口的安全性。

b) 测评对象：云计算服务对外接口

c) 测评实施包括以下内容：

1）应检查云计算服务对外接口的安全策略，如认证、加密等。
2）应测试云计算服务对外接口是否存在安全漏洞或安全隐患，测试方法可采取渗透测试或代码审计。

d) 单元判定：如果1）-2)均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

6.1.4.4 数据完整性

6.1.4.4.1 测评单元（L3-ADS2-08）

a) 测评指标：确保虚拟机迁移过程中，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。

b) 测评对象：虚拟机

c) 测评实施包括以下内容：

1）应检查虚拟资源迁移过程中采用的数据完整性保障措施及恢复措施；
2）应检查在虚拟资源迁移过程中，是否采取加密、签名等措施保证虚拟资源数据及重要数据的完整性，并在检测到完整性受到破坏时是否采取必要的恢复措施；

d) 单元判定：如果1）-2)均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

6.1.4.5 数据保密性

6.1.4.5.1 测评单元（L3-ADS2-09）

a) 测评指标：确保虚拟机迁移过程中，重要数据的保密性，防止在迁移过程中的重要数据泄露；

b) 测评对象：系统管理数据（如镜像文件、快照）、鉴别信息和重要业务数据（如用户隐私数据）

c) 测评实施包括以下内容：

1）应检查虚拟机迁移过程中重要数据的保密措施，查看是否能有效防止迁移过程中重要数据的泄露；
2）应检查是否采取加密或其他保护措施实现系统管理数据（如镜像文件、快照）,鉴别信息和重要业务数据（如用户隐私数据）来保证虚拟机迁移过程中重要数据的保密性，防止迁移过程中重要数据的泄露；

d) 单元判定：如果1）-2)均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

6.1.4.5.2 测评单元（L3-ADS2-10）

a) 测评指标：支持云租户部署密钥管理解决方案，确保云租户自行实现数据的加解密过程；

b) 测评对象：系统管理数据（如镜像文件、快照），云租户数据

c） 测评实施包括以下内容：

1） 当云租户已部署密钥管理解决方案，应检查密钥管理解决方案是否能确保云租户自行实现数据的加解密过程；
2）应检查云服务方支持云租户部署密钥管理解决方案所采取的技术手段或管理措施，查看是否能确保云租户自行实现数据的加解密过程；

d） 单元判定：如果1）-2)均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

6.1.4.5.3 测评单元（L3-ADS2-11）

a） 测评指标：对网络策略控制器和网络设备（或设备代理）之间网络通信进行加密。

b） 测评对象：网络策略控制器和网络设备（代理设备）

c） 测评实施包括以下内容：

1） 应检查网络策略控制器和网络设备（代理设备），确认其是否对网络策略控制器和网络设备（代理设备）之间网络通信进行加密；
2） 应对主要网络策略控制器和网络设备（代理设备）进行渗透测试，通过使用各种渗透测试技术（如口令猜解等）对网络设备进行渗透测试，验证网络设备防护能力是否符合要求。

d） 单元判定：如果1）-2)均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

6.1.4.6 数据备份恢复

6.1.4.6.1 测评单元（L3-ADS2-12）

a） 测评指标：云租户应在本地保存其业务数据的备份；

b） 测评对象：系统管理员，网络管理员，数据库管理员，安全管理员，主要主机操作系统，主要网络设备、虚拟化网络设备操作系统，主要数据库管理系统，主要应用系统，网络拓扑结构，在线存储数据，虚拟机，虚拟机监视器，云平台

c） 测评实施包括以下内容：

1） 应访谈系统管理员，询问是否采取措施使云租户可以在本地保存其业务数据的备份
2） 应检查虚拟机，虚拟机监视器，云平台，查看是否采取备份措施保证云租户可以在本地保存其业务数据。

d） 单元判定：如果1）-2)均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

6.1.4.6.2 测评单元（L3-ADS2-13）

a） 测评指标：提供查询云租户数据及备份存储位置的方式；

b） 测评对象：系统管理员，网络管理员，数据库管理员，安全管理员，主要主机操作系统，主要网络设备、虚拟化网络设备操作系统，主要数据库管理系统，主要应用系统，网络拓扑结构，在线存储数据，虚拟机，虚拟机监视器，云平台

c） 测评实施包括以下内容：

1）应访谈系统管理员，询问是否能为云租户提供数据及备份存储的位置的查询；
2）应检查相关技术文档，查看云服务方是否为云租户提供数据及备份存储位置查询的接口或其他技术、管理手段；

d） 单元判定：如果1）-2)均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

6.1.4.6.3 测评单元（L3-ADS2-14）

a） 测评指标：保证不同云租户的审计数据隔离存放；

b） 测评对象：系统管理员，网络管理员，数据库管理员，安全管理员，主要主机操作系统，主要网络设备、虚拟化网络设备操作系统，主要数据库管理系统，主要应用系统，网络拓扑结构，在线存储数据，虚拟机，虚拟机监视器，云平台

c） 测评实施包括以下内容：

1）应访谈系统管理员，询问不同云租户的审记数据存放策略，是否隔离存放；
2）应检查是否采取云租户审计数据隔离存放措施；

d） 单元判定：如果1）-2)均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

6.1.4.6.4 测评单元（L3-ADS2-15）

a） 测评指标：为云租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。

b） 测评对象：系统管理员，网络管理员，数据库管理员，安全管理员，主要主机操作系统，主要网络设备、虚拟化网络设备操作系统，主要数据库管理系统，主要应用系统，网络拓扑结构，在线存储数据，虚拟机，虚拟机监视器，云平台

c） 测评实施包括以下内容：

1）应访谈系统管理员，询问采取了哪些技术手段保证云租户能够将业务系统及数据迁移到其他云计算平台和本地系统，询问是否协助云租户完成迁移过程；
2）应检查相关技术手段，查看是否能保障云租户将业务系统及数据迁移到其他云计算平台和本地系统，；
3）应检查云服务方是否提供措施、手段或人员协助云租户完成迁移过程。

d） 单元判定：如果1）-2)均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

6.1.4.7 剩余信息保护

6.1.4.7.1 测评单元（L3-ADS2-16）

a） 测评指标：应保证虚拟机所使用的内存和存储空间回收时得到完全清除。

b） 测评对象：系统管理员、虚拟机、虚拟机监视器系统，云管理平台系统，主要操作系统技术开

发手册或产品检测报告，主要数据库系统技术开发手册或产品检测报告

c) 测评实施包括以下内容：

1）应访谈系统管理员，询问资源抽象层用户的鉴别信息存储空间，在回收时的数据清除策略，查看是否达到完全清除；
2）应访谈系统管理员，虚拟机监视器和云管理平台内的文件、目录、数据库记录和虚拟资源等所在的存储空间，在回收时的数据清除策略，查看是否达到完全清除；
3）应检查主要操作系统和主要数据库系统技术开发手册或产品检测报告，查看是否明确用户的鉴别信息存储空间回收时得到完全清除；
4）应检查主要操作系统和主要数据库系统技术开发手册或产品检测报告，是否明确文件、目录和数据库记录等资源所在的存储空间回收时得到完全清除。
5）应检查虚拟机监视器和云管理平台内的文件、目录、数据库记录和虚拟资源等所在的存储空间回收时是否得到完全清除；
6）应检查虚拟机的内存和存储空间回收时，是否得到完全清除；
7）应检查在迁移或删除虚拟机后，数据以及备份数据（如镜像文件、快照文件等）是否已清理。

d) 单元判定：如果1）-7)均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

6.2 安全管理单项测评

6.2.1 安全管理机构和人员

6.2.1.1 授权和审批

6.2.1.1.1 测评单元（L3-ORS2-01）

a) 测评指标：应保证云服务方对云租户业务数据和隐私信息的访问或使用必须经过云租户的授权，授权必须保留相关记录。

b) 测评对象：安全管理负责人、相关规章制度和流程、授权记录

c) 测评实施包括以下内容：

1）应访谈云服务方安全管理负责人，询问云服务方对云租户业务数据和隐私信息的访问或使用是否必须经过云租户的授权；
2）应访谈云租户安全管理负责人，询问云服务方对其业务数据和隐似信息的访问授权内容，询问数据管理权限是否为云租户所有；
2）应检查云服务方相应规章制度和流程，查看云租户业务数据和隐私信息保护细则；
3）应检查授权记录，查看云服务方对云租户业务数据和隐私信息的访问或使用是否均有授权；

d) 单元判定：如果1）-2)均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

6.2.2 安全建设管理

6.2.2.1 安全方案设计

6.2.2.1.1 测评单元（L3-CMS2-01）

a) 测评指标：云计算平台应提供开放接口或开放性安全服务，允许云租户接入第三方安全产品或在云平台选择第三方安全服务，支持异构方式对云租户的网络、主机、应用、数据层的安全措施进行实施。

b) 测评对象：系统建设负责人、相关接口、系统建设文档、云平台

c) 测评实施包括以下内容：

1）应访谈系统建设负责人，询问云计算平台是否开放接口或开放性安全服务，允许第三方安全产品接入或允许云租户在云平台选择第三方安全服务。询问云计算平台是否支持异构方式对云租户的网络、主机、应用、数据层的安全措施进行实施；
2)应检查系统建设文档，查看云计算平台是否存在开放接口设计，支持第三方安全产品接入。查看接口配置信息，查看云计算平台是否支持异构方式对云租户的网络、主机、应用、数据层的安全措施进行实施；
3）应检查云平台，查看所提供第三方安全服务，查看是否支持异构方式对云租户的网络、主机、应用、数据层的安全措施进行实施。

d) 单元判定：如果1）-2)均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

6.2.2.2 测试验收

6.2.2.2.1 测评单元（L3-CMS2-02）

a) 测评指标：应验证或评估所提供的安全措施的有效性。

b) 测评对象：系统建设负责人、相关评估记录和报告、相关资质证书、相关安全检测报告

c) 测评实施包括以下内容：

1）应访谈系统建设负责人，询问是否对所提供的安全措施的有效性进行验证和评估；
2）应检查相关评估记录和报告，查看是否对所提供安全措施的有效性进行了验证和评估；
3）应检查云服务方的相关资质证书检查或相关安全检测报告，查看是否对所提供安全措施的有效性进行了验证和评估。

d) 单元判定：如果1）-3)均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

6.2.2.3 云服务商选择

6.2.2.3.1 测评单元（L3-CMS2-03）

a) 测评指标：确保云服务商的选择符合国家的有关规定；

b) 测评对象：系统建设负责人、相关流程或规章制度、服务合同

c) 测评实施包括以下内容：

1）应访谈系统建设负责人，询问为云计算平台提供安全规划、设计、实施、维护、测评等服务的安全服务单位和云服务供应商的选择是否符合国家有关规定；

2）应检查安全服务单位和云服务提供商的资质，查看是否符合国家的有关规定；

d) 单元判定：如果1）-2）为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

6.2.2.3.2 测评单元（L3-CMS2-04）

a) 测评指标：选择安全合规的云服务商，其所提供的云平台应具备与信息系统等级相应的安全保护能力；

b) 测评对象：系统建设负责人、安全责任合同书或保密协议、服务合同

c) 测评实施包括以下内容：

1）应访谈系统建设负责人，询问是否根据业务系统的安全保护等级选择具有相应等级安全保护能力的云平台及云服务商；
2）应检查安全责任合同书或保密协议，服务合同，查看云服务商选择是否是否安全合规，查看是否根据业务系统的安全保护等级选择具有相应等级安全保护能力的云平台及云服务商。单元判定

d) 单元判定：如果1）-2)均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

6.2.2.3.3 测评单元（L3-CMS2-05）

a) 测评指标：满足服务水平协议（SLA）要求；

b) 测评对象：系统建设负责人，服务水平协议（SLA），云平台

c) 测评实施包括以下内容：

1）应检查服务水平协议（SLA），查看相关服务水平协议内容；
2）应检查云平台，查看是否满足服务水平协议（SLA）要求。

d) 单元判定：如果1）—2）为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

6.2.2.3.4 测评单元（L3-CMS2-06）

a) 测评指标：在服务水平协议（SLA）中规定云服务的各项服务内容和具体技术指标；

b) 测评对象：系统建设负责人，服务水平协议（SLA），云平台

c) 测评实施包括以下内容：

1）应检查服务水平协议（SLA），查看是否规定了云服务的各项服务内容和具体指标、服务期限、双方签字或盖章等；
2）应检查云平台，查看是否有相关服务内容，查看云平台是否符合具体技术指标。

d) 单元判定：如果c)为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

6.2.2.3.5 测评单元（L3-CMS2-07）

a) 测评指标：在服务水平协议（SLA）中规定云服务商的权限与责任，包括管理范围、职责划分、访问授权、隐私保护、行为准则、违约责任等；

b) 测评对象：系统建设负责人，服务水平协议（SLA）

c) 测评实施：应检查服务水平协议（SLA），查看在服务水平协议（SLA）中规范了安全服务商和云服务供应商的权限与责任，包括管理范围、职责划分、访问授权、隐私保护、行为准则等；

d) 单元判定：如果c）为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

6.2.2.3.6 测评单元（L3-CMS2-08）

a) 测评指标：在服务水平协议（SLA）中规定云计算所能提供的安全服务的内容，并提供安全声明；

b) 测评对象：系统建设负责人，在服务水平协议（SLA）

c) 测评实施：应检查服务水平协议（SLA），查看是否规定了云计算所能提供的安全服务的内容，并提供安全声明；

d) 单元判定：如果c)为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

6.2.2.3.7 测评单元（L3-CMS2-09）

a) 测评指标：在服务水平协议（SLA）中规定服务合约到期时，完整地返还云租户信息，并承诺相关信息均已在云计算平台上清除；

b) 测评对象：系统建设负责人，在服务水平协议（SLA），云平台

c) 测评实施包括以下内容：

1）应检查服务水平协议（SLA），查看是否规定服务合约到期时，完整地返还云租户信息，并承诺相关信息均已在云平台上清除。
2）应检查云平台，查看是否采取措施保障服务合约到期时，完整地返还云租户信息，并承诺相关信息均已在云平台上清除；

d) 单元判定：如果1)-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

6.2.2.3.8 测评单元（L3-CMS2-10）

a) 测评指标：与选定的云服务商签署保密协议，要求其不得泄露云租户数据和业务系统的相关重要信息；

b) 测评对象：系统建设负责人，安全责任合同书或保密协议，服务合同

c) 测评实施：应检查安全责任合同书、保密协议或服务合同，查看其是否包含对云服务商不得泄露云租户数据和业务系统的相关重要信息的要求。

d) 单元判定：如果c)为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不

符合或部分符合本单项测评指标要求。

6.2.2.3.9 测评单元（L3-CMS2-11）

a) 测评指标：对可能接触到云租户数据的员工进行背景调查，并签署保密协议；

b) 测评对象：系统建设负责人、相应调查文件或报告

c) 测评实施包括以下内容：

1）应访谈系统建设负责人，询问是否与云服务商可接触到云租户数据的员工签订保密协议，并检查相应协议；
2）应访谈系统建设负责人，询问是否对云服务商和云服务商可接触到云租户敏感信息的员工进行过背景调查，并检查相应调查文件或报告；
3）应检查员工保密协议，并检查是否存在背景调查资料；

d) 单元判定：如果1）-3)均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

6.2.2.3.10 测评单元（L3-CMS2-12）

a) 测评指标：云服务商应接受云租户以外的第三方运行监管。

b) 测评对象：系统建设负责人、相关技术文档

c) 测评实施包括以下内容：

1）应访谈系统建设负责人，询问云服务商是否接受云租户以外的第三方运行监管；
2）应检查相关技术文档，查看是否提供运行监管接口或其他手段可接受云租户以外的第三方监管；

d) 单元判定：如果1）-2)均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

6.2.2.4 供应链管理

6.2.2.4.1 测评单元（L3-CMS2-13）

a) 测评指标：确保供应商的选择符合国家的有关规定；

b) 测评对象：云服务方安全主管、供应商资质

c) 测评实施包括以下内容：

1）应访谈云服务方安全主管，询问供应商的选择是否符合国家的有关规定；
2）应检查供应商资质，查看是否符合国家的有关规定；

d) 单元判定：如果1)-2)均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

6.2.2.4.2 测评单元（L3-CMS2-14）

a) 测评指标：确保供应链安全事件信息或威胁信息能够及时传达到云租户；

b) 测评对象：云服务方安全主管，供应商重要变更记录，安全风险评估报告和风险预案

c) 测评实施包括以下内容：

1）应访谈云服务方安全主管，询问是否供应商的重要变更是否及时传达到云租户，并且对带来的安全风险进行评估，并采取有关措施对风险进行控制；
2）应检查系统，确认供应链安全事件信息或威胁信息是否能够及时传达到云租户。

d) 单元判定：如果1）-2)均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

6.2.2.4.3 测评单元（L3-CMS2-15）

a) 测评指标：保证供应商的重要变更及时传达到云租户，并评估变更带来的安全风险，采取有关措施对风险进行控制。

b) 测评对象：云服务方安全主管，供应商重要变更记录，安全风险评估报告和风险预案

c) 测评实施：应检查安全风险评估报告和风险预案，确认对每次供应商的重要变更都进行评估与风险预案设计。

d) 单元判定：如果c)为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

6.2.3 安全运维管理

6.2.3.1 监控和审计管理

6.2.3.1.1 测评单元（L3-MMS2-01）

a) 测评指标：确保信息系统的监控活动符合关于隐私保护的相关政策法规；

b) 测评对象：系统安全负责人，云计算平台，监控活动，相关政策法规，审计数据，相关策略，安全措施

c) 测评实施包括以下内容：

1）应访谈系统安全负责人，询问云计算平台的监控活动是否符合关于隐私保护的相关政策法规；
2）应检查信息系统监控活动，查看是否符合隐私保护的相关政策法规；

d) 单元判定：如果1)-2)均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

6.2.3.1.2 测评单元（L3-MMS2-02）

a) 测评指标：确保提供给云租户的审计数据的真实性和完整性；

b) 测评对象：系统安全负责人，云计算平台，监控活动，相关政策法规，审计数据，相关策略，安全措施

c) 测评实施包括以下内容：

1）应访谈系统安全负责人，询问采取了哪些手段保证提供给云租户的审计数据是真实的和完整的；
2）应检查云平台，采用技术手段查看提供给云租户的审计数是否是真实的和完整的；

d) 单元判定：如果1）-2)均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

6.2.3.1.3 测评单元（L3-MMS2-03）

a) 测评指标：制定相关策略，对安全措施有效性进行持续监控；

b) 测评对象：系统安全负责人、云平台、相关策略

c) 测评实施包括以下内容：

1）应访谈系统安全负责人，询问制定哪些相关策略，对安全措施有效性进行持续监控；
2）应检查云平台，查看是否制定了相关策略，对安全措施有效性进行持续监控；

d) 单元判定：如果1）-2)均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

6.2.3.1.4 测评单元（L3-MMS2-04）

a) 测评指标：云服务方应将安全措施有效性的监控结果定期提供给相关云租户。

b) 测评对象：文件或邮件等形式通知

c) 测评实施：应检查文件或邮件等形式通知，查看是否已将安全措施有效性的监控结果定期提供给相关云租户；

d) 单元判定：如果c)为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

7 第四级测评要求

7.1 安全技术单项测评

7.1.1 物理和环境安全

7.1.1.1 物理位置的选择

7.1.1.1.1 测评单元（L4-PES2-01）

a) 测评指标：确保云计算服务器、承载云租户账户信息、鉴别信息、系统信息及运行关键业务和数据的物理设备均位于中国境内。

b) 测评对象：记录类文档、办公场地和机房

c) 测评实施包括以下内容：

1）应检查办公场地（放置终端计算机设备）和机房，查看云计算服务器、承载云租户账户信息、鉴别信息、系统信息及运行关键业务和数据的物理设备是否均位于中国境内；

2）应检查记录类文档、办公场地和机房，查看云计算服务器、承载云租户账户信息、鉴别信息、系统信息及运行关键业务和数据的物理设备是否位于法规、合同和协议限定的地理位置之内；；

d) 单元判定：如果1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

7.1.2 网络和通信安全

7.1.2.1 网络架构

7.1.2.1.1 测评单元（L4-NCS2-01）

a) 测评指标：实现不同云租户之间的网络隔离；

b) 测评对象：网络资源隔离措施、综合网管系统或云管理平台

c) 测评实施包括以下内容：

1）应检查云租户间网络资源隔离措施；
2）应检查综合网管系统或云管理平台，查看云租户之间网络资源隔离策略是否有效；

d) 单元判定：如果1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

7.1.2.1.2 测评单元（L4-NCS2-02）

a) 测评指标：绘制与当前运行情况相符的虚拟化网络拓扑结构图，并能对虚拟化网络资源、网络拓扑进行实时更新和集中监控；

b) 测评对象：综合网管系统或云管理平台，网络拓扑图，网络设备、安全设备或管理平台

c) 测评实施包括以下内容：

1）应检查云服务方综合网管系统、云管理平台或云租户管理平台，检查是否对虚拟化网络资源（如虚拟交换机、虚拟防火墙等）、虚拟网络拓扑进行实时更新和集中监控；
2）应检查网络设备、安全设备或管理平台，查看网络拓朴结构图是否与当前运行情况相符；

d) 单元判定：如果1）-2）为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

7.1.2.1.3 测评单元（L4-NCS2-03）

a) 测评指标：保证虚拟机只能接收到目的地址包括自己地址的报文；

b) 测评对象：虚拟机、广播网段

c) 测评实施包括以下内容：

1）应检查是否采用VLAN、SDN等技术手段隔离虚拟网络中不同租户的数据传输，保证云租户不能接收到目的地址不包括自己的非广播数据包。

2）应采用抓包等方式检查虚拟交换机或交换机，查看虚拟机是否只能接收到目的地址仅包括自己地址的报文；
3）应测试不同网段的虚拟机进行广播时，是否只能接收到目的地址包括自己地址的报文；

d) 单元判定：如果1）、2）或1）、3）为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

7.1.2.1.4 测评单元（L4-NCS2-04）

a) 测评指标：保证云计算平台管理流量与云租户业务流量分离；

b) 测评对象：网络架构、云管理平台

c) 测评实施包括以下内容：

1）应检查网络架构和配置策略，查看能否采用带外管理或策略配置等方式实现管理流量和业务流量分离；
2）应检查云管理平台，查看云平台管理流量与云租户业务流量是否分离，查看所采取的技术手段和流量分离手段；
3）应测试云计算平台管理流量与业务流量是否分离。

d) 单元判定：如果1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

7.1.2.1.5 测评单元（L4-NCS2-05）

a) 测评指标：能识别、监控虚拟机之间、虚拟机与物理机之间的流量；

b) 测评对象：虚拟机监视器、云管理平台

c) 测评实施：应检查虚拟机监视器、云管理平台等，查看同一宿主机内虚拟机之间、虚拟机与物理机之间流量是否能被识别、监控；查看不同宿主机的虚拟机之间、虚拟机与物理机之间流量是否能被识别、监控。

d) 单元判定：如果c）为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

7.1.2.1.6 测评单元（L4-NCS2-06）

a) 测评指标：根据承载的业务系统安全保护等级划分不同安全级别资源池，并实现资源池之间的网络隔离；

b) 测评对象：资源池、业务系统、私有云

c) 测评实施包括以下内容：

1）应查看不同安全等级的业务系统是否对应不同资源池，查看资源池隔离所采用的机制和技术，查看资源池间访问控制策略及隔离机制；
2）应测试对不同安全等级资源池间进行非法访问时，是否可以正确拒绝该非法访问；
3）当被测系统为私有云，且无资源池划分需求时，不同等级资源间访问应可追责，实现不同等级资源间网络隔离；

d) 单元判定：如果1）、2)或3） 为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

7.1.2.1.7 测评单元（L4-NCS2-07）

a) 测评指标：提供开放接口或开放性安全服务，允许云租户接入第三方安全产品或在云平台选择第三方安全产品、服务，加强云租户虚拟机之间、安全区域之间的网络安全防护能力；

b) 测评对象：系统管理员，相关接口，相关服务

c) 测评实施包括以下内容：

1）应检查接口设计文档或开放性服务技术文档，查看是否符合开放性及安全性要求；
2）如果提供开放接口，应检查内部通信网络（虚拟网络）为第三方安全产品所提供的开放接口，查看接口安全保障机制，查看接口配置或参数；
3）如果提供开放性安全产品、服务，应查看开放性安全产品及服务的服务内容和实现开放性安全服务所采用的技术手段，查看安全保障机制。

d) 单元判定：如果1）、2）或1）、3）为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

7.1.2.1.8 测评单元（L4-NCS2-08）

a) 测评指标：根据云租户的业务需求定义安全访问路径。

b) 测评对象：云平台、网络设备、安全访问路径

c) 测评实施包括以下内容：

1）应检查云服务方的云管理平台或网络设备，查看能否根据云租户业务需求定义网络安全访问路径，查看其安全策略；
2）应检查云租户的网络管理平台或网络设备，查看是否已定义安全访问路径，查看其安全策略；
3）检查云服务商管理员进行远程管理时，管理终端与管理服务器之间所建立的安全访问路径。

d) 单元判定：如果1）、3）或2）为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

7.1.2.1.9 测评单元（L4-NCS2-09）

a) 测评指标：保证信息系统的外部通信接口经授权后方可传输数据。

b) 测评对象：相关授权记录、外部通信接口

c) 测评实施包括以下内容：

1）应检查相关授权记录，查看信息系统的外部通信接口的数据传输是否经授权，查看授权流程；
2）应检查信息系统的外部通信接口，查看实现数据传输授权所采取的技术手段；

d) 单元判定：如果1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

7.1.2.2 访问控制

7.1.2.2.1 测评单元（L4-NCS2-10）

a) 测评指标：在虚拟化网络边界部署访问控制机制，并设置访问控制规则；

b) 测评对象：访问控制机制，网络边界设备或虚拟化网络边界设备

c) 测评实施包括以下内容：

1）应检查云服务方和云租户虚拟化网络边界访问控制机制，查看访问控制规则和访问控制策略等；
2）应检查云服务方的网络边界设备或虚拟化网络边界设备，查看安全保障机制、访问控制规则或访问控制策略等；
3）应检查不同租户间访问时采用的访问控制机制或设备，对于访问控制机制，应查看所采取的机制是否已被测试是安全的（如第三方测试报告），对于访问控制设备，应查看访问控制设备的访问控制策略是否合理；
4）应检查租户内不同区域间访问时采用的访问控制机制或设备，对于访问控制机制，应查看所采取的机制是否已被测试是安全的（如第三方测试报告），对于访问控制设备，应查看访问控制设备的访问控制策略是否合理；，
5）应测试虚拟化网络边界访问控制设备，查看是否可以正确拒绝违反访问控制规则的非法访问。

d) 单元判定：如果1）-5)均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

7.1.2.2.2 测评单元（L4-NCS2-11）

a) 测评指标：保证当虚拟机迁移时，访问控制策略随其迁移；

b) 测评对象：网络管理员，安全管理员，管理平台，虚拟化网络边界访问控制设备，虚拟机

c) 测评实施包括以下内容：

1）应访谈安全管理员，询问虚拟机迁移时，访问控制策略迁移措施和手段；
2）应检查虚拟机迁移记录及相关配置，查看虚拟机迁移后访问控制策略是否部署；
3）应测试虚拟机迁移，查看访问控制措施是否随其迁移；

d) 单元判定：如果1）-3)均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

7.1.2.2.3 测评单元（L4-NCS2-12）

a) 测评指标：允许云租户设置不同虚拟机之间的访问控制策略；

b) 测评对象：云服务方管理平台、云租户管理系统、虚拟化网络边界访问控制设备

c) 测评实施包括以下内容：

1）应检查云服务方的云管理平台等，查看是否允许云租户设置不同虚拟机间访问控制策略；

2）应检查云服务方的云管理平台，查看是否存在不同虚拟机间的访问控制管理模块，是否开启该访问控制功能；
3）应检查云租户的云管理系统，查看不同虚拟机间访问控制策略是否安全；
4）应测试虚拟化网络边界访问控制设备，查看是否可以正确拒绝违反虚拟机间访问控制策略的非法访问。

d) 单元判定：如果1）、2）、4)或3）、4）为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

7.1.2.2.4 测评单元（L4-NCS2-13）

a) 测评指标：在不同等级的网络区域边界部署访问控制机制，设置访问控制规则

b) 测评对象：边界访问控制机制或边界访问控制设备

c) 测评实施包括以下内容：

1）应检查不同安全等级网络区域边界的访问控制机制部署情况，查看访问控制规则；
2）应测试不同安全等级的网络区域间进行非法访问时，是否可以正确拒绝该非法访问；

d) 单元判定：如果1）-2)均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

7.1.2.2.5 测评单元（L4-NCS2-14）

a) 测评指标：对进出网络的流量实施有效监控。

b) 测评对象：网络边界访问控制设备，网络流量监控记录

c) 测评实施包括以下内容：

1）应检查边界网络设备、网络虚拟化设备，查看对进出网络的流量是否实施有效监控；
2）应检查进出网络流量的监控情况或监控信息，查看是否对进出网络的流量进行有效监控。

d) 单元判定：如果1)-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

7.1.2.3 入侵防范

7.1.2.3.1 测评单元（L4-NCS2-15）

a) 测评指标：能检测到并告警后及时处理云租户的网络攻击行为，并能记录攻击类型、攻击时间、攻击流量等；

b) 测评对象：网络入侵防范设备或国家认可的相关机制、入侵防范措施

c) 测评实施包括以下内容：

1）应检查网络入侵防范措施，查看是否有专门设备对网络入侵进行防范，查看网络入侵防范规则库的升级方式；
2）应检查网络入侵防范设备或机制，当采用网络入侵防范机制时，应查看所采取的机制是否已被测试是安全的（如第三方测试报告），查看入侵防范设备或机制的规则库是否为最新；

3）应测试网络入侵防范设备或机制，当采用网络入侵防范机制时，应查看所采取的机制是否已被测试是安全的（如第三方测试报告），验证入侵防范设备或机制对异常流量和未知威胁的监控策略是否有效（如模拟产生攻击动作，查看网络入侵防范设备的反应，是否能记录攻击类型、攻击时间、攻击流量）；

4）应检查系统是否具备异常流量、大规模攻击流量、高级持续性攻击的检测功能、报警功能和清洗处置功能；

5）应检查是否具有对SQL注入、跨站脚本等攻击进行检测发现、告警并及时处理的能力；

6）应具有对恶意虚拟机，如具有恶意行为、过分占用计算资源和带宽资源等的虚拟机，进行检测发现、告警并及时处理的能力；

7）应检查云管理平台等，查看对云租户攻击的防范措施，查看对云租户的网络攻击行为的记录情况，记录应包括攻击类型、攻击时间、攻击流量等；

8）应测试主要网络入侵防范设备或机制，验证其云租户网络攻击报警报警策略是否有效（如模拟产生攻击动作，查看网络入侵防范设备是否能实时报警并及时处置）；

9）应对云平台内部发起的恶意攻击或恶意对外连接的行为进行限制，查看是否对内部行为进行监控，查看相关日志记录。

10）应通过对外攻击发生器伪造对外攻击行为，检查云租的网络攻击的日志记录，确认是否正确记录到相应攻击行为，攻击行为日志记录是否包含攻击类型、攻击时间、攻击者IP、攻击流量规模等；

11）应检查运行虚拟机监控器（VMM）和云管理平台软件的物理主机，查看其安全加固手段是否能够应对虚拟化共享带来的安全漏洞。

d) 单元判定：如果1）-11)均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

7.1.2.3.2 测评单元（L4-NCS2-16）

a) 测评指标：向云租户提供互联网发布内容监测功能，便于云租户对其发布内容中的有害信息进行实时监测并告警后及时处理。

b) 测评对象：安全管理员，云平台

c) 测评实施包括以下内容：

1）应检查云服务方安全服务，查看是否可为云租户提供互联网发布内容监测功能；

2）应检查相关安全组件，查看云租户能否对其发布到互联网的有害信息进行实时监测并告警后及时处理；

3）应检查云租户对其发布到互联网有害信息的实时监测情况、历史告警信息和告警处理记录。

4）应检查云租户设置的有害信息过滤规则，查看过滤规则是否可对常见有害信息进行过滤；

d) 单元判定：如果1）-2)均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

7.1.2.4 安全审计

7.1.2.4.1 测评单元（L4-NCS2-17）

a) 测评指标：对远程执行特权命令进行审计；

b) 测评对象：边界网络设备、网络虚拟化设备、相关审计数据

c) 测评实施包括以下内容：

1）应检查审计数据，查看执行远程特权命令后是否有相关审计记录；
2）当云服务方采用第三方运维时，应检查第三方运维方是否向云服务方提供审计数据，或云服务方是否可采取措施收集相关审计数据；
3）应检查边界网络设备、网络虚拟化设备，查看远程执行特权命令的限制措施，查看是否对远程执行特权命令的行为进行安全审计；

d) 单元判定：如果1）-3)均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

7.1.2.4.2 测评单元（L4-NCS2-18）

a) 测评指标:根据云服务方和云租户的职责划分,实现各自控制部分审计数据的收集和集中审计；

b) 测评对象：审计数据收集系统或设备、云管理平台、审计数据

c) 测评实施包括以下内容：

1）应检查云服务方审计数据收集系统或设备，查看是否根据云服务方和云租户的职责划分实现各自控制部分审计数据的收集和集中审计；
2）如果云租户授权云服务方收集部分云租户控制的审计数据，应检查云服务方是否在不影响其他云租户安全的前提下将云租户审计数据提供给云租户；
3）应检查云服务方审计数据，查看是否不包括云租户控制部分的审计数据；
4）应检查云服务方和云租户云管理平台，查看集中审计结果；
5）应检查是否支持云租户部署第三方安全审计设备，实现云租户职责范围内的集中审计；

d) 单元判定：如果1）-5)均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

7.1.2.4.3 测评单元（L4-NCS2-19）

a) 测评指标：为安全审计数据的汇集提供接口，并可供第三方审计；

b) 测评对象：边界网络设备，网络虚拟化设备，审计数据汇集接口，审计数据

c) 测评实施：应检查主要边界网络设备、网络虚拟化设备、审计系统或云管理平台，查看是否为安全审计数据的汇集提供接口，并可供第三方审计；

d) 单元判定：如果c）为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

7.1.3 设备和计算安全

7.1.3.1 身份鉴别

7.1.3.1.1 测评单元（L4-ECS2-01）

a) 测评指标：应在网络策略控制器和网络设备（或设备代理）之间建立双向身份验证机制。

b) 测评对象：网络管理员，网络策略控制器和网络设备（代理设备）

c) 测评实施包括以下内容：

1）应访谈网络管理员，询问是否在网络策略控制器和网络设备（或设备代理）之间建立双向身份验证机制；
2）应检查网络策略控制器和网络设备（或设备代理）之间的身份验证机制；
3）应对主要网络策略控制器和网络设备（代理设备）进行渗透测试，通过使用各种渗透测试技术（如口令猜解等）对网络设备进行渗透测试，验证网络设备防护能力是否符合要求，是否在网络策略控制器和网络设备（或设备代理）之间建立双向身份验证机制。

d) 单元判定：如果1）-3)均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

7.1.3.2 访问控制

7.1.3.2.1 测评单元（L4-ECS2-02）

a) 测评指标：当进行远程管理时，防止远程管理设备同时直接连接其他网络；

b) 测评对象：系统管理员，云平台，数据库，运维终端，远程管理设备，云平台运维管理员，云服务运营管理员

c) 测评实施：应检查运维终端，查看是否为专用，查看当进行远程管理时，是否能够防止远程管理设备同时直接连接到其他网络资源；

d) 单元判定：如果c）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

7.1.3.2.2 测评单元（L4-ECS2-03）

a) 测评指标：确保只有在云租户授权下，云服务方或第三方才具有云租户数据的管理权限；

b) 测评对象：云平台，数据库，运维终端，远程管理设备

c) 测评实施包括以下内容：

1）应检查云服务方所采取的措施，以确保只有在云租户授权情况下才具有云租户数据的管理权限，查看该措施能否有效避免云服务方非授权管理云租户数据；
2）应测试数据库系统，验证云服务方是否不能对云租户非授权数据进行管理；

d) 单元判定：如果1）-2)均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

7.1.3.2.3 测评单元（L4-ECS2-04）

a) 测评指标：提供云计算平台管理用户权限分离机制，为网络管理员、系统管理员建立不同账户并分配相应的权限。

b) 测评对象：云管理平台、相关文档

c) 测评实施包括以下内容：

1）应检查云租户云的云管理平台，查看云平台运维管理员和云服务运营管理员的权限是否分离，查看网络管理员、系统管理员是否建立不同账户并分配相应的权限；
2）应检查云服务方的云管理平台，是否提供云平台管理用户权限分离机制，能够为网络管理、系统管理建立不同账户并分配相应的权限；

d) 单元判定：如果1）-2)均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

7.1.3.3 安全审计

7.1.3.3.1 测评单元（L4-ECS2-05）

a) 测评指标:根据云服务方和云租户的职责划分,实现各自控制部分审计数据的收集和集中审计；

b) 测评对象：系统管理员，主要服务器，宿主机及虚拟机的操作系统，主要终端操作系统，主要数据库系统，审计系统

c) 测评实施包括以下内容：

1）应检查主要服务器、宿主机及虚拟机的操作系统、主要终端操作系统和主要数据库系统的安全审计策略或审计数据，查看是否根据云服务方和云租户的职责进行划分，收集各自控制的部分的审计数据；
2）应检查审计系统，查看是否根据云服务方和云租户的职责进行划分，收集各自控制的部分的审计数据；

d) 单元判定：如果1）或2）为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

7.1.3.3.2 测评单元（L4-ECS2-06）

a) 测评指标：保证云服务方对云租户系统和数据的操作可被云租户审计；

b) 测评对象：主要服务器，宿主机及虚拟机的操作系统，主要终端操作系统，主要数据库系统，审计设备、审计数据

c) 测评实施包括以下内容：

1）应检查安全审计策略，查看安全审计配置是否能够保证云服务方对云租户系统和数据的操作（如增、删、改、查等操作）可被云租户审计；
2）应检查是否支持云租户部署第三方安全审计设备，保证云服务商对云租户系统和数据的操作可被租户审计。
3）应检查云服务方与云租户收集的审计数据，查看云服务方对云租户系统和数据的操作是否可被云租户审计。

d) 单元判定：如果1）-3）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

7.1.3.3.3 测评单元（L4-ECS2-07）

a) 测评指标：保证审计数据的真实性和完整性；

b) 测评对象：主要服务器，宿主机及虚拟机的操作系统，主要终端操作系统，主要数据库系统，审计系统

c) 测评实施：应检查主要服务器、宿主机及虚拟机的操作系统、主要终端操作系统和主要数据库系统的安全审计策略，查看是否能够通过日志覆盖周期、存储方式、日志文件/空间大小、日志文件操作权限等设置，是否实现了对审计记录的保护，使其避免受到未预期的删除、修改或覆盖等，查看是否采取措施能够保证审计数据的真实性和完整性；

d) 单元判定：如果c）为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

7.1.3.3.4 测评单元（L4-ECS2-08）

a) 测评指标：为安全审计数据的汇集提供接口，并可供第三方审计；

b) 测评对象：主要服务器，宿主机及虚拟机的操作系统，主要终端操作系统，主要数据库系统，审计系统

c) 测评实施：应检查主要服务器、宿主机及虚拟机的操作系统、主要终端操作系统和主要数据库系统的安全审计策略，是否能够进行例如日志数据等各类审计数据的集中，并设置安全可信的接口以供访问上述数据，如存在需要进行第三方集中审计的情况下，实现集中审计或第三方审计。

d) 单元判定：如果c）为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

7.1.3.4 入侵防范

7.1.3.4.1 测评单元（L4-ECS2-09）

a) 测评指标：能够检测虚拟机对宿主机资源的异常访问，并告警后及时处理；

b) 测评对象：系统管理员，主要服务器、宿主机及虚拟机，操作系统，主要数据库系统，虚拟机监视器，云平台

c) 测评实施包括以下内容：

1）应访谈系统管理员，询问能否检测虚拟机对宿主机的异常访问，并告警后及时处理；
2）应测试虚拟机监视器和云管理平台，验证是否能够及时检测到虚拟机异常访问宿主机资源等行为，并告警后及时处理。如利用虚机逃逸漏洞验证是否触发报警；

d) 单元判定：如果1）-2)均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

7.1.3.4.2 测评单元（L4-ECS2-10）

a) 测评指标：能够检测虚拟机之间的资源隔离失效，并告警后及时处理；

b) 测评对象：系统管理员，主要服务器、宿主机及虚拟机，操作系统，主要数据库系统，虚拟机监视器，云平台

c) 测评实施包括以下内容：

1）应检查主要服务器、宿主机及虚拟机，虚拟机监视器，云平台是否采取措施对不同虚拟机的CPU、内存和磁盘资源进行隔离，是否实现不同云租户自有数据库之间的隔离；是否采取措施能够检测到虚拟机之间的资源隔离失效，并告警后及时处理；
2）应访谈系统管理员，询问是否采取措施对不同虚拟机资源进行了安全隔离，是否采取措施能够检测到虚拟机之间的资源隔离失效，并告警后及时处理。

d) 单元判定：如果1）-2)均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

7.1.3.4.3 测评单元（L4-ECS2-11）

a) 测评指标：能检测到非授权新建虚拟机或者重新启用虚拟机，并告警后及时处理；

b) 测评对象：系统管理员，主要服务器、宿主机及虚拟机，操作系统，主要数据库系统，虚拟机监视器，云平台

c) 测评实施：应检查主要服务器、宿主机及虚拟机，操作系统，主要数据库系统，虚拟机监视器，云平台是否能够检测到非授权新建虚拟机或者重新启用虚拟机，并告警后及时处理。

d) 单元判定：如果c）为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

7.1.3.5 恶意代码防范

7.1.3.5.1 测评单元（L4-ECS2-12）

a) 测评指标：能够检测恶意代码感染及在虚拟机间蔓延的情况，并告警后及时处理。

b) 测评对象：主要服务器、虚拟机监视器，宿主机及虚拟机、云平台，主要终端，防恶意代码软件或硬件，网络防恶意代码产品

c) 测评实施包括以下内容：

1）应检查主要服务器、宿主机、虚拟机、终端、虚拟机监视器、云平台是否建立恶意代码传播路径追踪机制，是否可以检测查看恶意代码的感染情况，并告警后及时处理。
2）应检查主要服务器、宿主机、虚拟机、终端，虚拟机监视器，云平台是否能够检测恶意代码感染及在虚拟机间蔓延的情况，是否能够检测出虚拟机的恶意行为，并告警后及时处理。

d) 单元判定：如果1）-2)均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

7.1.3.6 资源控制

7.1.3.6.1 测评单元（L4-ECS2-13）

a) 测评指标：屏蔽虚拟资源故障，某个虚拟机崩溃后不影响虚拟机监视器及其他虚拟机；

b) 测评对象：资源控制相关平台、云平台

c) 测评实施包括以下内容：

1）应检查资源控制相关平台，查看所采取的屏蔽虚拟资源故障措施，查看相关虚拟机故障记录，查看是否不存在虚拟机崩溃后影响虚拟机监视器及其他虚拟机的历史；
2）应检查云平台，查看所采取的屏蔽虚拟资源故障的技术手段，查看是否能在某个虚拟机崩溃后不影响虚拟机监视器及其他虚拟机；

d) 单元判定：如果1)-2)均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

7.1.3.6.2 测评单元（L4-ECS2-14）

a) 测评指标：对物理资源和虚拟资源按照策略做统一管理调度与分配；

b) 测评对象：云平台，虚拟机，虚拟机监视器，物理资源和虚拟资源

c) 测评实施包括以下内容：

1）应检查云租户的运营管理平台或资源调度平台，查看资源调度策略，查看资源调度分配情况；
2）应检查云服务方云管理平台，查看所提供策略能否对物理资源和虚拟资源做统一管理调度与分配；

d) 单元判定：如果1)-2)均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

7.1.3.6.3 测评单元（L4-ECS2-15）

a) 测评指标：保证虚拟机仅能使用为其分配的计算资源；

b) 测评对象：云管理平台，虚拟机、计算资源

c) 测评实施包括以下内容：

1）应检查云管理平台，查看计算资源分配情况，查看资源分配的审计记录或告警记录是否不存在资源过量占用警告，或资源分配机制能否实现虚拟机仅能使用为其分配的计算资源；
2）应测试虚拟机，当访问或使用管理员未分配的计算资源时，是否可以拒绝该请求，并有相应告警信息；

d) 单元判定：如果1)-2)均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

7.1.3.6.4 测评单元（L4-ECS2-16）

a) 测评指标：保证虚拟机仅能迁移至相同安全等级的资源池。

b) 测评对象：系统管理员、虚拟机迁移记录

c) 测评实施包括以下内容：

1）应访谈系统管理员，询问虚拟机迁移时是否仅迁移至相同安全等级的资源池。
2）应检查虚拟机迁移记录，查看是否存在虚拟机迁移至不同安全等级资源池的情况。

d) 单元判定：如果1）-2)均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护

对象不符合或部分符合本单项测评指标要求。

7.1.3.6.5 测评单元（L4-ECS2-17）

a) 测评指标：保证分配给虚拟机的内存空间仅供其独占访问；

b) 测评对象：云平台

c) 测评实施包括以下内容：

1）应检查云平台，采取了何种技术手段，以保证分配给虚拟机的内存空间仅供其独占访问；
2）应检查云平台，查看是否采取安全机制保障同一物理地址段被不同用户使用；

d) 单元判定：如果c）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

7.1.3.6.6 测评单元（L4-ECS2-18）

a) 测评指标：对虚拟机的网络接口的带宽进行设置，并进行监控；

b) 测评对象：云管理平台或其他安全组件

c) 测评实施包括以下内容：

1）应检查云管理平台或其他安全组件，查看是否能对虚拟机网络接口带宽进行设置，查看能否对其进行监控；
2）应检查云管理平台，查看虚拟机的网络接口带宽的配置及参数，并查看带宽监控记录；

d) 单元判定：如果1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

7.1.3.6.7 测评单元（L4-ECS2-19）

a) 测评指标：为监控信息的汇集提供接口，并实现集中监控。

b) 测评对象：云平台，监控信息汇集接口

c) 测评实施包括以下内容：

1）应检查云平台，查看是否为CPU、内存、流量和安全等监控信息的汇集提供了接口，并实现集中监控；
2）应检查CPU、内存、流量和安全等监控信息汇集接口配置或参数，查看集中监控措施和记录；

d) 单元判定：如果1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

7.1.3.7 镜像和快照保护

7.1.3.7.1 测评单元（L4-ECS2-20）

a) 测评指标：提供虚拟机镜像、快照完整性校验功能，防止虚拟机镜像被恶意篡改；

b) 测评对象：云管理平台、虚拟机监视器、虚拟机镜像文件

c） 测评实施包括以下内容：

1）应检查虚拟机监视器，查看是否有对镜像文件定期进行有效性验证的记录；

2）应检查虚拟机监视器，云管理平台是否提供有效的虚拟机镜像和快照文件管理机制，虚拟机是否能够及时被备份和快照，以及是否准确地恢复到所需还原点。

3）应检查虚拟机监视器，云管理平台是否对快照功能生成的镜像或快照文件进行完整性校验，是否具有严格的校验记录机制，防止虚拟机镜像或快照被恶意篡改。

d） 单元判定：如果1)-3)均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

7.1.3.7.2 测评单元（L4-ECS2-21）

a） 测评指标:采取加密或其他技术手段防止虚拟机镜像、快照中可能存在的敏感资源被非法访问；

b） 测评对象：云管理平台、虚拟机监视器、虚拟机镜像文件

c） 测评实施：应检查虚拟机监视器，云管理平台是否对虚拟机镜像或快照中的敏感资源，通过加密、访问控制、权限控制等技术手段进行保护，防止可能存在的针对快照的非法访问。

d） 单元判定：如果c）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

7.1.3.7.3 测评单元（L4-ECS2-22）

a） 测评指标：针对重要业务系统提供加固的操作系统镜像。

b） 测评对象：云管理平台、虚拟机监视器、虚拟机镜像文件

c） 测评实施：应检查虚拟机监视器，云管理平台是否对生成的虚拟机镜像进行必要的加固措施，如关闭不必要的端口、服务及进行安全加固配置。

d） 单元判定：如果c）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

7.1.4 应用和数据安全

7.1.4.1 安全审计

7.1.4.1.1 测评单元（L4-ADS2-01）

a） 测评指标:根据云服务方和云租户的职责划分,实现各自控制部分审计数据的收集和集中审计；

b） 测评对象：云管理平台、审计系统、审计数据

c） 测评实施包括以下内容：

1）应检查云管理平台或审记系统，查看是否具备安全审计功能，查看审计策略及审计数据；

2）应检查云服务方云管理平台或审记系统，查看是否根据云服务方和云租户的职责划分，收集各自控制部分的审计数据。查看审计策略，查看云服务方和云租户各自的审计内容；

3）应检查云服务方和云租户收集的审计数据，查看是否根据云服务方和云租户的职责划分，实现了各自控制部分的集中审计。

d) 单元判定：如果1)-2)均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

7.1.4.1.2 测评单元（L4-ADS2-02）

a) 测评指标：保证云服务方对云租户系统和数据的操作可被云租户审计；

b) 测评对象：审计系统、审计数据

c) 测评实施：应检查审计系统，验证云服务方对云租户系统和数据的操作可以被云租户审计；

d) 单元判定：如果c）为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

7.1.4.1.3 测评单元（L4-ADS2-03）

a) 测评指标：保证审计数据的真实性和完整性；

b) 测评对象：审计系统、审计数据

c) 测评实施：应检查审记系统或各项审计数据，验证其是否对数据进行加密和完整性保护。

d) 单元判定：如果c）为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

7.1.4.1.4 测评单元（L4-ADS2-04）

a) 测评指标：为安全审计数据的汇集提供接口，并可供第三方审计；

b) 测评对象：主要应用系统、审计数据汇集接口

c) 测评实施：应检查主要应用系统，查看是否为安全审计数据的汇集提供接口，并能对汇集的数据进行集中审计或第三方审计；

d) 单元判定：如果c）为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

7.1.4.2 资源控制

7.1.4.2.1 测评单元（L4-ADS2-05）

a) 测评指标：能够对应用系统的运行状况进行监测，并在发现异常时进行告警并及时处理；

b) 测评对象：主要应用系统，开发平台

c) 测评实施：应检查应用系统，查看是否能够对应用系统的运行状况进行监测，包括应用运行异常、入侵攻击发生、扫描漏洞出现，并在发现异常时进行邮件或短信等方式的及时告警，并及时处理；

d) 单元判定：如果c)为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

7.1.4.2.2 测评单元（L4-ADS2-06）

a) 测评指标：保证不同云租户的应用系统及开发平台之间的隔离。

b) 测评对象：主要应用系统，开发平台

c) 测评实施包括以下内容：

1）应检查云服务方为实现云租户的应用系统与开发平台隔离所采取的保障措施；
2）应检查云租户的应用系统与开发平台是否隔离。

d) 单元判定：如果1）-2)均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

7.1.4.3 接口安全

7.1.4.3.1 测评单元（L4-ADS2-07）

a) 测评指标：保证云计算服务对外接口的安全性。

b) 测评对象：云计算服务对外接口

c) 测评实施包括以下内容：

1）应检查云计算服务对外接口的安全策略，如认证、加密等。
2）应测试云计算服务对外接口是否存在安全漏洞或安全隐患，测试方法可采取渗透测试或代码审计。

d) 单元判定：如果1）-2)均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

7.1.4.4 数据完整性

7.1.4.4.1 测评单元（L4-ADS2-08）

a) 测评指标：确保虚拟机迁移过程中，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。

b) 测评对象：虚拟机

c) 测评实施包括以下内容：

1）应检查虚拟资源迁移过程中采用的数据完整性保障措施及恢复措施；
2）应检查在虚拟资源迁移过程中，是否采取加密、签名等措施保证虚拟资源数据及重要数据的完整性，并在检测到完整性受到破坏时是否采取必要的恢复措施；

d) 单元判定：如果1）-2)均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

7.1.4.5 数据保密性

7.1.4.5.1 测评单元（L4-ADS2-09）

a) 测评指标：确保虚拟机迁移过程中，重要数据的保密性，防止在迁移过程中的重要数据泄露；

b) 测评对象：系统管理数据（如镜像文件、快照）、鉴别信息和重要业务数据（如用户隐私数据）

c) 测评实施包括以下内容：

1）应检查虚拟机迁移过程中重要数据的保密措施，查看是否能有效防止迁移过程中重要数据的泄露；

2）应检查是否采取加密或其他保护措施实现系统管理数据（如镜像文件、快照），鉴别信息和重要业务数据（如用户隐私数据）来保证虚拟机迁移过程中重要数据的保密性，防止迁移过程中重要数据的泄露；

d) 单元判定：如果1）-2)均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

7.1.4.5.2 测评单元（L4-ADS2-10）

a) 测评指标：支持云租户部署密钥管理解决方案，确保云租户自行实现数据的加解密过程；

b) 测评对象：系统管理数据（如镜像文件、快照），云租户数据

c) 测评实施包括以下内容：

1）当云租户已部署密钥管理解决方案，应检查密钥管理解决方案是否能确保云租户自行实现数据的加解密过程；

2）应检查云服务方支持云租户部署密钥管理解决方案所采取的技术手段或管理措施，查看是否能确保云租户自行实现数据的加解密过程；

d) 单元判定：如果1）-2)均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

7.1.4.5.3 测评单元（L4-ADS2-11）

a) 测评指标：对网络策略控制器和网络设备（或设备代理）之间网络通信进行加密。

b) 测评对象：网络策略控制器和网络设备（代理设备）

c) 测评实施包括以下内容：

1）应检查网络策略控制器和网络设备（代理设备），确认其是否对网络策略控制器和网络设备（代理设备）之间网络通信进行加密；

2）应对主要网络策略控制器和网络设备（代理设备）进行渗透测试，通过使用各种渗透测试技术（如口令猜解等）对网络设备进行渗透测试，验证网络设备防护能力是否符合要求。

d) 单元判定：如果1）-2)均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

7.1.4.6 数据备份恢复

7.1.4.6.1 测评单元（L4-ADS2-12）

a) 测评指标：云租户应在本地保存其业务数据的备份；

b) 测评对象：系统管理员，网络管理员，数据库管理员，安全管理员，主要主机操作系统，主要

网络设备、虚拟化网络设备操作系统，主要数据库管理系统，主要应用系统，网络拓扑结构，在线存储数据，虚拟机，虚拟机监视器，云平台

c) 测评实施包括以下内容：

1) 应访谈系统管理员，询问是否采取措施使云租户可以在本地保存其业务数据的备份
2) 应检查虚拟机，虚拟机监视器，云平台，查看是否采取备份措施保证云租户可以在本地保存其业务数据。

d) 单元判定：如果1）-2)均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

7.1.4.6.2 测评单元（L4-ADS2-13）

a) 测评指标：提供查询云租户数据及备份存储位置的方式；

b) 测评对象：系统管理员，网络管理员，数据库管理员，安全管理员，主要主机操作系统，主要网络设备、虚拟化网络设备操作系统，主要数据库管理系统，主要应用系统，网络拓扑结构，在线存储数据，虚拟机，虚拟机监视器，云平台

c) 测评实施包括以下内容：

1) 应访谈系统管理员，询问是否能为云租户提供数据及备份存储的位置的查询；
2) 应检查相关技术文档，查看云服务方是否为云租户提供数据及备份存储位置查询的接口或其他技术、管理手段；

d) 单元判定：如果1）-2)均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

7.1.4.6.3 测评单元（L4-ADS2-14）

a) 测评指标：保证不同云租户的审计数据隔离存放；

b) 测评对象：系统管理员，网络管理员，数据库管理员，安全管理员，主要主机操作系统，主要网络设备、虚拟化网络设备操作系统，主要数据库管理系统，主要应用系统，网络拓扑结构，在线存储数据，虚拟机，虚拟机监视器，云平台

c) 测评实施包括以下内容：

1) 应访谈系统管理员，询问不同云租户的审记数据存放策略，是否隔离存放；
2) 应检查是否采取云租户审计数据隔离存放措施；

d) 单元判定：如果1）-2)均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

7.1.4.6.4 测评单元（L4-ADS2-15）

a) 测评指标：为云租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。

b) 测评对象：系统管理员，网络管理员，数据库管理员，安全管理员，主要主机操作系统，主要网络设备、虚拟化网络设备操作系统，主要数据库管理系统，主要应用系统，网络拓扑结构，

在线存储数据，虚拟机，虚拟机监视器，云平台

c) 测评实施包括以下内容：

1）应访谈系统管理员，询问采取了哪些技术手段保证云租户能够将业务系统及数据迁移到其他云计算平台和本地系统，询问是否协助云租户完成迁移过程；
2）应检查相关技术手段，查看是否能保障云租户将业务系统及数据迁移到其他云计算平台和本地系统，；
3）应检查云服务方是否提供措施、手段或人员协助云租户完成迁移过程。

d) 单元判定：如果1）-2)均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

7.1.4.7 剩余信息保护

7.1.4.7.1 测评单元（L4-ADS2-16）

a) 测评指标：应保证虚拟机所使用的内存和存储空间回收时得到完全清除。

b) 测评对象：系统管理员、虚拟机、虚拟机监视器系统，云管理平台系统，主要操作系统技术开发手册或产品检测报告，主要数据库系统技术开发手册或产品检测报告

c) 测评实施包括以下内容：

1）应访谈系统管理员，询问资源抽象层用户的鉴别信息存储空间，在回收时的数据清除策略，查看是否达到完全清除；
2）应访谈系统管理员，虚拟机监视器和云管理平台内的文件、目录、数据库记录和虚拟资源等所在的存储空间，在回收时的数据清除策略，查看是否达到完全清除；
3）应检查主要操作系统和主要数据库系统技术开发手册或产品检测报告，查看是否明确用户的鉴别信息存储空间回收时得到完全清除；
4）应检查主要操作系统和主要数据库系统技术开发手册或产品检测报告，是否明确文件、目录和数据库记录等资源所在的存储空间回收时得到完全清除。
5）应检查虚拟机监视器和云管理平台内的文件、目录、数据库记录和虚拟资源等所在的存储空间回收时是否得到完全清除；
6）应检查虚拟机的内存和存储空间回收时，是否得到完全清除；
7）应检查在迁移或删除虚拟机后，数据以及备份数据（如镜像文件、快照文件等）是否已清理。

d) 单元判定：如果1）-7)均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

7.2 安全管理单项测评

7.2.1 安全管理机构和人员

7.2.1.1 测评单元（L4-ORS2-01）

a) 测评指标：应保证云服务方对云租户业务数据和隐私信息的访问或使用必须经过云租户的授权，授权必须保留相关记录。

b) 测评对象：安全管理负责人，相关规章制度和流程

c) 测评实施包括以下内容：

1）应访谈安全管理负责人，询问云服务方对云租户业务数据和隐私信息的访问或使用是否必须经过云租户的授权；
2）应检查是否存在相应的规章制度和流程。

d) 单元判定：如果1）-2)均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

7.2.2 安全建设管理

7.2.2.1 安全方案设计

7.2.2.1.1 测评单元（L4-CMS2-01）

a) 测评指标：云计算平台应提供开放接口或开放性安全服务，允许云租户接入第三方安全产品或在云平台选择第三方安全服务，支持异构方式对云租户的网络、主机、应用、数据层的安全措施进行实施。

b) 测评对象：系统建设负责人，相关接口，系统建设文档

c) 测评实施包括以下内容：

1）应访谈系统建设负责人，询问云计算平台是否开放接口或开放性安全服务，允许第三方安全产品接入或允许云租户在云平台选择第三方安全服务。询问云计算平台是否支持异构方式对云租户的网络、主机、应用、数据层的安全措施进行实施；
2）如果提供开放接口，应检查系统建设文档，查看云计算平台是否存在开放接口设计，支持第三方安全产品接入。查看云计算平台是否支持异构方式对云租户的网络、主机、应用、数据层的安全措施进行实施；
3）如果提供开放性安全服务，应检查云平台，查看所提供第三方安全服务，查看是否支持异构方式对云租户的网络、主机、应用、数据层的安全措施进行实施。

d) 单元判定：如果1）-2)均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

7.2.2.2 测试验收

7.2.2.2.1 测评单元（L4-CMS2-02）

a) 测评指标：应验证或评估所提供的安全措施的有效性。

b) 测评对象：系统建设负责人，相关评估记录和报告，相关资质证书，相关安全检测报告

c) 测评实施包括以下内容：

1）应访谈系统建设负责人，询问是否对所提供的安全措施的有效性进行验证和评估；
2）应检查相关评估记录和报告，查看是否对所提供安全措施的有效性进行了验证和评估；
3）应检查云服务方的相关资质证书检查或相关安全检测报告，查看是否对所提供安全措施的有效性进行了验证和评估。

d) 单元判定：如果1）-3)均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

7.2.2.3 云服务商选择

7.2.2.3.1 测评单元（L4-CMS2-03）

a) 测评指标：应避免选择社会化的云服务。

b) 测评对象：系统建设负责人，云平台

c) 测评实施包括以下内容：

1）应访谈系统建设负责人，询问云服务是否为非社会化的云服务；
2）应检查云平台，查看云服务是否为非社会化的云服务；

d) 单元判定：如果1)-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

7.2.2.4 供应链管理

7.2.2.4.1 测评单元（L4-CMS2-04）

a) 测评指标：确保供应商的选择符合国家的有关规定；

b) 测评对象：云服务方安全主管

c) 测评实施包括以下内容：

1）应访谈云服务方安全主管，询问供应商的选择是否符合国家的有关规定；
2）应检查供应商资质，查看是否符合国家的有关规定；

d) 单元判定：如果c)为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

7.2.2.4.2 测评单元（L4-CMS2-05）

a) 测评指标：确保供应链安全事件信息或威胁信息能够及时传达到云租户；

b) 测评对象：云服务方安全主管，供应商重要变更记录，安全风险评估报告和风险预案

c) 测评实施包括以下内容：

1）应访谈云服务方安全主管，询问是否供应商的重要变更是否及时传达到云租户，并且对带来的安全风险进行评估，并采取有关措施对风险进行控制；
2）应检查系统，确认供应链安全事件信息或威胁信息是否能够及时传达到云租户。

d) 单元判定：如果1）-2)均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

7.2.2.4.3 测评单元（L4-CMS2-06）

a) 测评指标：保证供应商的重要变更及时传达到云租户，并评估变更带来的安全风险，采取有关措施对风险进行控制。

b) 测评对象：云服务方安全主管，供应商重要变更记录，安全风险评估报告和风险预案

c) 测评实施：应检查安全风险评估报告和风险预案，确认对每次供应商的重要变更都进行评估与风险预案设计。

d) 单元判定：如果c)为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

7.2.3 安全运维管理

7.2.3.1 监控和审计管理

7.2.3.1.1 测评单元（L4-MMS2-01）

a) 测评指标：确保信息系统的监控活动符合关于隐私保护的相关政策法规；

b) 测评对象：系统安全负责人，云计算平台，监控活动，相关政策法规，审计数据，相关策略，安全措施

c) 测评实施包括以下内容：

1）应访谈系统安全负责人，询问云计算平台的监控活动是否符合关于隐私保护的相关政策法规；
2）应检查信息系统监控活动，查看是否符合隐私保护的相关政策法规；

d) 单元判定：如果1)-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

7.2.3.1.2 测评单元（L4-MMS2-02）

a) 测评指标：确保提供给云租户的审计数据的真实性和完整性；

b) 测评对象：系统安全负责人，云计算平台，监控活动，相关政策法规，审计数据，相关策略，安全措施

c) 测评实施包括以下内容：

1）应访谈系统安全负责人，询问采取了哪些手段保证提供给云租户的审计数据是真实的和完整的；
2）应检查云平台，采用技术手段查看提供给云租户的审计数是否是真实的和完整的；

d) 单元判定：如果1）-2)均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

7.2.3.1.3 测评单元（L4-MMS2-03）

a) 测评指标：制定相关策略，对安全措施有效性进行持续监控；

b) 测评对象：系统安全负责人，云计算平台，监控活动，相关政策法规，审计数据，相关策略，安全措施

c) 测评实施包括以下内容：

1）应访谈系统安全负责人，询问制定哪些相关策略，对安全措施有效性进行持续监控；
2）应检查云平台，查看是否制定了相关策略，对安全措施有效性进行持续监控；

d） 单元判定：如果1）-2)均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

7.2.3.1.4 测评单元（L4-MMS2-04）

a） 测评指标：云服务方应将安全措施有效性的监控结果定期提供给相关云租户。

b） 测评对象：系统安全负责人，云服务方，云计算平台，安全措施，监控结果

c） 测评实施：应检查云服务方，查看是否已将安全措施有效性的监控结果定期，并提供给相关云租户；

d） 单元判定：如果c)为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

8 整体测评

8.1 概述

国标 GB/T 22239.2-20XX 中的要求项，是为了对抗相应等级的威胁或具备相应等级的恢复能力而设计的，但由于安全措施的实现方式多种多样，安全技术也在不断发展，等级保护对象的运行使用单位所采用的安全措施和技术并不一定和 GB/T 22239.2-20XX 的要求项完全一致。因此，需要从等级保护对象整体上是否能够对抗相应等级威胁的角度，对单项测评中的不符合项和部分符合项进行综合分析，分析这些不符合项或部分符合项是否会影响到等级保护对象整体安全保护能力的缺失。等级保护对象的整体测评就是在单项测评的基础上，评价等级保护对象的整体安全保护能力有没有缺失，是否能够对抗相应等级的安全威胁。

等级保护对象整体测评应从安全控制点、安全控制点间和层面间等方面进行测评和综合安全分析，从而给出等级测评结论。整体测评包括安全控制点测评、安全控制点间测评和层面间测评。

安全控制点测评是指对其所有要求项的符合程度进行分析和判定。

安全控制点间安全测评是指对同一区域同一层面内的两个或者两个以上不同安全控制点间的关联进行测评分析，其目的是确定这些关联对等级保护对象整体安全保护能力的影响。

层面间安全测评是指对同一区域内的两个或者两个以上不同层面安全控制点间的关联进行测评分析，其目的是确定这些关联对等级保护对象整体安全保护能力的影响。

8.2 安全控制点测评

在单项测评完成后，如果该安全控制点下的所有要求项为符合，则该安全控制点符合，否则为不符合或部分符合。

8.3 安全控制点间测评

在单项测评完成后，如果等级保护对象的某个安全控制点中的要求项存在不符合或部分符合，应进行安全控制点间测评，应分析在同一层面内，是否存在其他安全控制点对该安全控制点具有补充作用（如物理访问控制和防盗窃、身份鉴别和访问控制等）。同时，分析是否存在其他的安全措施或技术与该要求项具有相似的安全功能。

根据测评分析结果，综合判断该安全控制点所对应的系统安全保护能力是否缺失，如果经过综合分析单项测评中的不符合项或部分符合项不造成系统整体安全保护能力的缺失，则该安全控制点的测评结论应调整为符合。

8.4 层面间测评

在单项测评完成后，如果等级保护对象的某个安全控制点中的要求项存在不符合或部分符合，应进行层面间安全测评，重点分析其他层面上功能相同或相似的安全控制点是否对该安全控制点存在补充作用（如应用和数据层加密与网络和通信层加密、设备和计算层与应用和数据层上的身份鉴别等），以及技术与管理上各层面的关联关系（如设备和计算安全与安全运维管理、应用和数据安全与安全运维管理等）。

根据测评分析结果，综合判断该安全控制点所对应的系统安全保护能力是否缺失，如果经过综合分析单项测评中的不符合项或部分符合项不造成系统整体安全保护能力的缺失，则该安全控制点的测评结论应调整为符合。

9 测评结论

9.1 各层面的测评结论

通过汇总安全控制点的测评结果，等级测评报告可以给出等级保护对象在安全技术和安全管理各个层面的等级测评结论。

在安全技术四个层面的等级测评结论中，通常物理和环境安全测评结论应重点给出等级保护对象在物理位置选择方面安全控制措施的落实情况；网络和通信安全测评结论应重点给出等级保护对象在网络架构、访问控制、远程访问和入侵防范等方面安全控制措施的落实情况；设备和计算安全测评结论应重点给出身份鉴别、访问控制、安全审计、入侵防范和资源控制等方面安全控制措施的落实情况；应用和数据安全测评结论应重点给出安全审计、资源控制、接口安全、数据完整性、数据保密性和数据备份恢复等方面的安全控制措施的落实情况。

在安全管理四个方面的等级测评结论中，通常安全管理机构和人员应重点给出授权和审批等方面的测评结论；安全建设管理可重点给出安全方案设计、测试验收、云服务商选择和供应链管理等方面的测评结论；安全运维管理可重点给出监控和审计管理等方面的测评结论。

不同等级等级保护对象在不同层面上会有不同的关注点，应反映到相应层面的等级测评结论中。

9.2 风险分析和评价

等级测评报告中应对整体测评之后单项测评结果中的不符合项或部分符合项进行风险分析和评价。

采用风险分析的方法对单项测评结果中存在的不符合项或部分符合项，分析所产生的安全问题被威胁利用的可能性，判断其被威胁利用后对业务信息安全和系统服务安全造成影响的程度，综合评价这些不符合项或部分符合项对等级保护对象造成的安全风险。

9.3 测评结论

等级测评报告应给出等级保护对象安全等级保护测评结论，确认等级保护达到相应等级保护要求的程度。

应结合各层面的测评结论和对单元测评结果的风险分析给出等级测评结论：

a) 如果单元测评结果中没有不符合项或部分符合项，则测评结论为“符合”；

b) 如果单元测评结果存在不符合项或部分符合项，但所产生的安全问题不会导致等级保护对象存

在高等级安全风险，则测评结论为“基本符合”；

c) 如果单元测评结果存在不符合项或部分符合项，且所产生的安全问题导致等级保护对象存在高等级安全风险，则测评结论为“不符合”。

附 录 A
（资料性附录）
测评力度

A.1 概述

本标准在第 5 章到第 7 章描述了第二级到第四级等级保护对象的单元测评的具体测评实施过程要求。为了便于理解、对比不同测评方法的测评力度以及不同级别等级保护对象单元测评的测评力度增强情况，分别编制表 A.1 测评方法的测评力度描述和 A.2 不同安全保护等级的等级保护对象的测评力度要求表。

A.2 测评力度描述

测评方法是测评人员依据测评内容选取的、实施特定测评操作的具体方法。本标准涉及访谈、检查和测试等三种基本测评方法。访谈、检查和测试等三种基本测评方法的测评力度可以通过其测评的深度和广度来描述，如表 A.1。

表 A.1 测评方法的测评力度

测评方法	深度	广度
访谈	访谈的深度体现在访谈过程的严格和详细程度，可以分为四种：简要的、充分的、较全面的和全面的。简要访谈只包含通用和高级的问题；充分访谈包含通用和高级的问题以及一些较为详细的问题；较全面访谈包含通用和高级的问题以及一些有难度和探索性的问题；全面访谈包含通用和高级的问题以及较多有难度和探索性的问题。	访谈的广度体现在访谈人员的构成和数量上。访谈覆盖不同类型的人员和同一类人的数量多少，体现出访谈的广度不同。
检查	检查的深度体现在检查过程的严格和详细程度，可以分为四种：简要的、充分的、较全面的和全面的。简要检查主要是对功能级上的文档、机制和活动，使用简要的评审、观察或检查以及检查列表和其他相似手段的简短测评；充分检查有详细的分析、观察和研究，除了功能级上的文档、机制和活动外，还适当需要一些总体/概要设计信息；较全面检查有详细、彻底分析、观察和研究，除了功能级上的文档、机制和活动外，还需要总体/概要和一些详细设计以及实现上的相关信息；全面检查有详细、彻底分析、观察和研究，除了功能级上的文档、机制和活动外，还需要总体/概要和详细设计以及实现上的相关信息。	检查的广度体现在检查对象的种类（文档、机制等）和数量上。检查覆盖不同类型的对象和同一类对象的数量多少，体现出对象的广度不同。
测试	测试的深度体现在执行的测试类型上：功能/性能测试和渗透测试。功能/性能测试只涉及机制的功能规范、高级设计和操作规程；渗透测试涉及机制的所有可用文档，并试图智取进入等级保护对象。	测试的广度体现在被测试的机制种类和数量上。测试覆盖不同类型的机制以及同一类型机制的数量多少，体现出对象的广度不同。

A.3 等级测评力度

测评力度是在测评过程中实施测评工作的力度，反映测评的广度和深度，体现为测评工作的实际投

入程度。测评广度越大，测评实施的范围越大，测评实施包含的测评对象就越多；测评深度越深，越需要在细节上展开，测评就越严格，因此就越需要更多的投入。投入越多，测评力度就越强，测评就越有保证。测评的广度和深度落实到访谈、检查和测试三种不同的测评方法上，能体现出测评实施过程中访谈、检查和测试的投入程度的不同。

信息安全等级保护要求不同安全保护等级的等级保护对象应具有不同的安全保护能力，满足相应等级的保护要求。为了检验不同安全保护等级的等级保护对象是否具有相应等级的安全保护能力，是否满足相应等级的保护要求，需要实施与其安全保护等级相适应的测评，付出相应的工作投入，达到应有的测评力度。第二级到第四级等级保护对象的测评力度反映在访谈、检查和测试等三种基本测评方法的测评广度和深度上，落实在不同单单项测评中具体的测评实施上。

为了进一步理解不同等级等级保护对象在测评力度上的不同，表 A.2 在表 A.1 的基础上，从测评对象数量和种类以及测评深度等方面详细分析了不同测评方法的测评力度在不同等级保护对象安全测评中的具体体现。

表 A.2 不同安全保护等级云计算平台的测评力度要求

测评力度		云计算平台安全保护等级		
		第二级	第三级	第四级
访谈	广度	测评对象在种类和数量上抽样，种类和数量都较多	测评对象在数量上抽样，在种类上基本覆盖	测评对象在数量上抽样，在种类上全部覆盖
	深度	充分	较全面	全面
检查	广度	测评对象在种类和数量上抽样，种类和数量都较多	测评对象在数量上抽样，在种类上基本覆盖	测评对象在数量上抽样，在种类上全部覆盖
	深度	充分	较全面	全面
测试	广度	测评对象在种类和数量、范围上抽样，种类和数量都较多，范围大	测评对象在数量和范围上抽样，在种类上基本覆盖	测评对象在数量、范围上抽样，在种类上基本覆盖
	深度	功能测试/性能测试	功能测试/性能测试，渗透测试	功能测试/性能测试，渗透测试

从表 A.2 可以看到，对不同等级的等级保护对象进行等级测评时，选择的测评对象的种类和数量是不同的，随着等级保护对象安全保护等级的增高，抽查的测评对象的种类和数量也随之增加。

对不同安全保护等级等级保护对象进行等级测评时，实际抽查测评对象的种类和数量，应当达到表 A.2 的要求，以满足相应等级的测评力度要求。在具体测评对象选择工作过程中，可参照遵循以下原则：

a) 完整性原则，选择的设备、措施等应能满足相应等级的测评力度要求；
b) 重要性原则，应抽查重要的服务器、数据库和网络设备等；
c) 安全性原则，应抽查对外暴露的网络边界；
d) 共享性原则，应抽查共享设备和数据交换平台/设备；
e) 代表性原则，抽查应尽量覆盖系统各种设备类型、操作系统类型、数据库系统类型和应用系统的类型。

附 录 B
（资料性附录）
测评单元编号说明

B.1 测评指标编码规则

测评单元编号为三组数据，格式为 XX-XXXX-XX，各组含义和编码规则如下：

第 1 组由两位组成，第 1 位为字母 L，第 2 位为数字，其中数字 1 为第一级，2 为第二级，3 为第三级，4 为第四级，5 为第五级。

第 2 组由 4 位组成，前 3 位为字母，第 3 位为数字。字母代表层面：PES 为物理和环境安全，NCS 为网络和通信安全，ECS 为设备和计算安全，ADS 为应用和数据安全，PSS 为安全策略和管理制度，ORS 为安全管理机构和人员，CMS 为安全建设管理，MMS 为安全运维管理。数字代表标准分册：1 为第一分册，2 为第二分册，3 为第三分册，4 为第四分册，5 为第五分册，6 为第六分册。

第 3 组由 2 位数字组成，按层面对基本要求中的要求项进行顺序编号。

示例：测评单元编号为 L1-PES1-01，代表源自基本要求第一分册的第一级物理安全层面的第一个指标。

B.2 专用缩略语

物理和环境安全为 PES（Physical and Enviornment Security）
网络和通信安全 NCS（Network and Communication Security）
设备和计算安全 ECS（Equipment and Computing Security）
应用和数据安全 ADS（Application and Data Security）
安全策略和管理制度 PSS（Policy and System Security）
安全管理机构和人员 ORS（Orgnazation and Resource Security）
安全建设管理 CMS（Costruction Management Security）
安全运维管理 MMS（Maintenance Management Security）

参 考 文 献

[1] GB/T 22239-2008 信息安全技术 信息系统安全等级保护基本要求
[2] GB/T 22240-2008 信息安全技术 信息系统安全等级保护定级指南
[3] GB/T 28448-2012 信息安全技术 信息系统安全等级保护测评要求
[4] GB/T 20269-2006 信息安全技术 信息系统安全管理要求
[5] GB/T 20270-2006 信息安全技术 网络基础安全技术要求
[6] GB/T 20271-2006 信息安全技术 信息系统通用安全技术要求
[7] GB/T 20272-2006 信息安全技术 操作系统安全技术要求
[8] GB/T 20273-2006 信息安全技术 数据库管理系统安全技术要求
[9] GB/T 20282-2006 信息安全技术 信息系统安全工程管理要求
[10] GB/T 18336-2000 信息技术 信息技术安全性评估准则
[11] NIST Special Publication 800-53 联邦信息系统推荐性安全控制措施
[12] Information technology-Security techniques - Information security management systems requirements（ISO/IEC 27001：2005）
[10] Information technology-Security techniques - Code of practice forinformation security management（ISO/IEC 17799：2005）