ICS 35.040
CCS L80

团 体 标 准

T/CIIA 059—2025

政务云平台大规模云租户网络安全等级保护测评实施指南

Testing and evaluation implementation guide for cybersecurity classified protection of large-scale cloud tenants on government cloud platform

2025－08－29 发布　　2025－08－29 实施

中国信息协会　　发 布

目　　次

前　言

为规范政务云平台大规模云租户网络安全等级保护工作，落实网络安全等级保护相关要求，根据国家标准GB/T 22239-2019《信息安全技术 网络安全等级保护基本要求》和公安部文件《关于落实网络安全保护重点措施 深入实施网络安全等级保护制度的指导意见》（公网安〔2022〕1058号），针对政务云平台大规模云租户的具体情况，特制定《政务云平台大规模云租户网络安全等级保护测评实施指南》。本文件中大规模云租户指在同一个政务云平台上承载多个信息系统的租户或租户集合体。其测评工作量与规模特性密切相关，采用本指南提出的测评实施模式可有效提升测评效率；承载系统数量越多，效率提升效益通常越显著。政务云租户均可参考本指南开展等级测评工作，以优化测评流程、提升资源效能。

本文件按照GB/T 1.1—2020《标准化工作导则 第1部分：标准化文件的结构和起草规则》的规定起草。

本文件由中国信息协会提出并归口。

本文件起草单位：国家信息中心、广西壮族自治区公安厅、安徽省公安厅网安总队、新疆维吾尔自治区公安厅、上海市公安局、北海市公安局、合肥市公安局、安庆市公安局、新疆维吾尔自治区信息中心、广西壮族自治区信息中心、安徽省大数据中心、北海市信息中心、上海市总工会、北海市互联网信息安全中心、上海市信息安全测评认证中心、中检集团天帷网络安全技术（合肥）有限公司。

本文件主要起草人：禄凯、陈永刚、赵佳璐、李格菲、赵帅、尚庆军、刘云飞、葛晓囡、赵云程、肖劲华、房锟、杨波、任仁、唐珂、阿依登·塔布斯、王昱镔、郭晓栋、严毅恒、朱斌、韦宇星、朱典、武建双、朱建树、许观就、白荣华、吴新民、周礼昊、罗杰、李菁、刘洋、王雅莉等。

引　言

随着数字政府建设的深入推进，政务云租户规模持续扩大，通过规范政务云平台大规模云租户测评流程，明确测评实施关键任务，规范各方职责边界，可保障测评工作高质量、高效率完成。《计算机信息系统安全保护等级划分准则》（GB 17859-1999）、《信息安全技术 网络安全等级保护基本要求》（GB/T 22239-2019）、《信息安全技术 网络安全等级保护测评过程指南》（GB/T 28449-2018）等标准，是政务云平台大规模云租户网络安全等级保护遵从的基本标准。本文件是针对政务云平台大规模云租户现状、技术特点和安全防护要求，对政务云平台大规模云租户等级保护测评实施过程做的细化和扩展，本文件未提到部分均按《信息安全技术 网络安全等级保护测评过程指南》（GB/T 28449-2018）执行。

政务云平台大规模云租户
网络安全等级保护测评实施指南

1. 范围

本文件规定了政务云平台大规模云租户网络安全等级保护测评流程和测评实施关键任务，上述政务云平台应已按属地公安机关相关要求通过本年度等级测评。

本文件适用于指导政务云平台大规模云租户网络安全等级保护工作的实施，也可为其他类型云平台大规模云租户等级测评提供参考。

本文件中的云计算服务模式为IaaS模式，PaaS和SaaS可参考。

2. 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB 17859 计算机信息系统安全保护等级划分准则

GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求

GB/T 25069-2022 信息安全技术 术语

GB/T 28448-2019 信息安全技术 网络安全等级保护测评要求

GB/T 28449-2018 信息安全技术 网络安全等级保护测评过程指南

GB/T 31168-2023 信息安全技术 云计算服务安全能力要求

GB/T 38249-2019 信息安全技术 政府网站云计算服务安全指南

GW 0013-2017 国家电子政务外网标准 政务云安全要求

3. 术语和定义

GB 17859-1999、GB/T 22239-2019、GB/T 25069-2022、GB/T 28448-2019和GW 0013-2017界定的术语和定义适用于本文件。

3.1

政务云 government cloud

用于承载各级政务部门开展公共服务、社会管理的业务信息系统和数据,并满足跨部门业务协同、数据共享与交换等的需要，提供IaaS、PaaS和SaaS服务的云计算服务。

[来源：GW 0013-2017，3.1，有修改]

3.2

云租户 cloud tenant

在政务云中，云租户指使用政务云的各级政务部门，即使用云计算基础设施开展电子政务业务和处理、存储数据的组织(或机构)及相关事业单位。

[来源：GW 0013-2017，3.2，有修改]

3.3

云服务方 cloud service party

在政务云中，云服务方指为各级政务部门提供计算、存储、网络及安全等各类云计算基础设施资源、相关软件和服务的提供商，并负责执行云服务方业务运营和相关管理工作。

[来源：GW 0013-2017，3.3，有修改]

3.4

政务云管理单位 government cloud management unit

是政务云的行政监管单位，负责政务云平台的规划、应用、监督、管理及对云服务方的考核，审核云服务客户的政务云平台使用需求。

[来源：GW 0013-2017，3.4，有修改]

3.5

云管理平台 cloud management platform

为整个云计算基础设施提供资源管理和服务管理，能够对存储/计算/网络/系统等基础设施资源进行管理。

[来源：GW 0013-2017，3.5，有修改]

3.6

首测阶段 initial assessment phase

首测阶段是等级测评的首次系统性评估过程，测评机构依据《信息安全技术 网络安全等级保护基本要求》（GB/T 22239）及相关标准，通过访谈、核查和测试等手段，对被测系统的安全保护状况进行全面检查，识别其与相应等级安全保护要求的符合性差距，形成问题清单并提出整改建议。

3.7

复测阶段 re-assessment phase

复测阶段是测评机构针对首测阶段发现的部分符合项/不符合项，验证被测单位整改措施有效性的过程。

4. 大规模政务云租户等级测评概述

4.1 角色和责任

政务云平台大规模云租户网络安全等级保护测评过程中涉及的各类角色和职责如下：

a）政务云管理单位

负责依照国家网络安全等级保护的管理规范和技术标准，统筹本行业、本部门或者本地区政务云的建设、使用、运维、运营、监督工作；负责审核政务云租户的政务云平台使用需求。

b）政务云租户

负责开展网络安全等级保护定级、评审、备案、整改、测评工作。

c）政务云服务方

包括政务云建设单位和运营单位。政务云建设单位负责政务云的统筹建设、统一纳管、互联互通、集约共享；配合政务云租户的政务信息系统向政务云迁移、部署或调整；负责政务云日常运行的安全管理和监测。政务云运营单位负责为各级政务部门提供算力和存储资源、网络链路、密码资源、安全保护的运营；负责政务云自身运行保障，保障政务云安全可靠稳定运行。

d）测评机构

负责根据主管、运营或使用单位的委托，协助其按照国家网络安全等级保护的管理规范和技术标准，对已经完成等级保护建设的信息系统进行等级测评。

4.2 大规模政务云租户等级测评总体流程

a）测评准备活动

政务云管理单位负责统筹协调，测评机构负责具体实施，云服务方及云租户进行配合，共同确定测评范围、明确责任主体、确定测评流程。

b）方案编制活动

测评机构整理测评准备活动中获取的定级对象相关资料，根据各租户系统情况及数量，估算现场测评工作量、确定测评项目组数量及成员，编制具体测评计划，形成测评方案。测评方案经过内部评审通过后，提交测评委托单位签字认可。

c）现场测评活动

测评机构负责测评实施，云服务方及云租户进行配合，对各租户系统进行等级测评，并提出目前存在的问题及整改建议。现场测评结束后召开测评现场结束会，对发现的问题进行汇总、分析。针对高风险问题由各云租户进行整改后，再由测评机构进行复测。

d）报告编制活动

测评机构对测评结果进行汇总分析，形成等级测评结论，编制测评报告，并将评审通过后的等级测评报告按照分发范围进行分发。

5. 测评实施过程

5.1 测评准备活动

5.1.1 工作流程

测评准备活动的目标是顺利启动测评项目，收集定级对象相关资料，准备测评所需资料，为编制测评方案打下良好的基础。

测评准备活动包括工作启动、信息收集和分析两项关键任务。

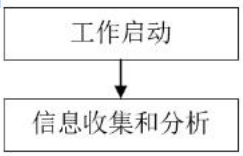

图1 测评准备活动的关键工作流程

5.1.2 关键任务

5.1.2.1 工作启动

a）测评机构

1）组建等级测评项目组并编制项目计划书。

2）指出测评委托单位应提供的基本资料。

2）协助政务云管理单位组织云租户和云服务方召开项目启动会，并介绍大规模政务云租户测评流程和方法。

b）政务云管理单位

负责统筹协调获取所有测评委托单位及定级对象的基本情况，从基本资料、人员、计划安排方面为整个测评项目的实施做好充分准备。

5.1.2.2 信息收集和分析

a）测评机构

准备被测定级对象基本情况调查表，并提交给测评委托单位。

b）政务云租户和政务云服务方

负责配合测评机构填写测评调研表。

5.2 方案编制活动

5.2.1 工作流程

方案编制活动的目标是整理测评准备活动中获取的定级对象相关资料，为现场测评活动提供最基本的文档和指导方案。

方案编制活动包括测评对象确定、工具测试方法确定、测评方案编制三项关键任务。

图2 方案编制活动的关键工作流程

5.2.2 关键任务

5.2.2.1 测评对象确定

a）测评机构

1）详细分析被测定级对象的整体结构、边界、网络服务、安全服务、设备部署情况等。

2）分析确定测评对象。

5.2.2.2 工具测试方法确定

a）测评机构

1）确定工具测试环境及测试对象。
2）选择测试路径。
3）根据测试路径，确定测试工具的接入点。
4）结合网络拓扑图，描述测试工具的接入点、测试目的、测试途径和测试对象等相关内容。
b）政务云租户和政务云服务方
配合测评机构选择工具测试路径并确定测试工具的接入点。

5.2.2.3 测评方案编制

a）测评机构
1）根据各租户系统情况及数量，估算现场测评工作量并确定测评项目组数量及项目组成员。
2）根据测评项目组成员安排，编制具体测评计划，包括现场工作人员的分工和时间安排。
3）汇总上述内容及方案编制活动的其他任务获取的内容形成测评方案。
4）评审和提交测评方案。测评方案应经过内部评审通过后，提交测评委托单位签字认可。
b）政务云租户
1）为测评机构完成测评方案提供有关信息和资料。
2）评审和确认测评方案。

5.3 现场测评活动

5.3.1 工作流程

现场测评活动通过与测评委托单位进行沟通和协调,为现场测评的顺利开展打下良好基础,依据测评方案实施现场测评工作,将测评方案和测评方法等内容具体落实到现场测评活动中。现场测评工作应取得报告编制活动所需的、足够的证据和资料。

现场测评活动包括现场测评准备、首测阶段现场测评、复测阶段结果确认三项关键任务。

图3 现场测评活动的关键工作流程

5.3.2 关键任务

5.3.2.1 现场测评准备

a）测评机构
召开测评现场首次会，介绍测评工作安排，政务云管理单位、云租户和云服务方对测评计划和测评方案中的测评内容和方法等进行沟通。
b）政务云管理单位
统筹协调所有云租户和云服务方现场测评工作安排，包括测评配合人员和需要提供的测评环境等，确保现场测评活动完成。

5.3.2.2 首测阶段

a）测评机构

1）开展现场测评工作，并获取相关证据。

2）安全通信网络、安全区域边界、安全管理中心统一在云服务方测评。

3）安全计算环境中的主机设备在云服务方测评。

4）各层面可复用指标项见附录A。

b）政务云租户和政务云服务方

1）明确各自的责任边界，配合测评工作。

2）云租户配合主机、应用、数据及管理层面的测评。

3）云服务方负责配合计算、存储、网络及安全等各类云计算基础设施资源、相关软件和服务方面的测评。

5.3.2.3 复测阶段

a）测评机构

1）统一安排现场复测工作；

2）召开测评现场结束会；

3）根据测评过程中发现的安全问题，为云租户提出相应建议，并总结分析共性安全问题。

b）政务云管理单位

听取各租户方等级测评情况，给出相应指导建议。

5.4 报告编制活动

5.4.1 工作流程

在现场测评工作结束后，测评机构应对现场测评获得的测评结果（或称测评证据）进行汇总分析，形成等级测评结论，并编制报告。

报告编制活动包括等级测评结论形成、测评报告编制两项关键任务。

图4 报告编制活动的关键工作流程

5.4.2 关键任务

5.4.2.1 等级测评结论形成

a）测评机构

根据测评结果记录形成测评结论。

5.4.2.2 测评报告编制

a）测评机构

1）编制各租户系统等级测评报告。

2）评审等级测评报告，并将评审过的等级测评报告按照分发范围进行分发。

b）政务云租户

1）签收测评报告。

2）向分管公安机关备案测评报告。

附录 A
（资料性）
大规模云租户测评指标复用情况（标准场景）

政务云平台服务标准化，网络架构相同，租户采用相同的云安全服务。例如：某省政务云为下属某委办局各租户系统提供统一云安全服务。按照测评层面分类，集约化主要体现在安全通信网络、安全区域边界、安全计算环境和安全管理中心。安全物理环境由云平台管理，租户无权限；安全管理需区分租户差异化测评。在以上标准场景下，大规模云租户测评指标复用情况（三级系统）如下所示：

A.1 安全物理环境

云租户不适用。

A.2 安全通信网络

A.2.1 安全通用要求部分

控制点	测评指标	是否统一测评	说明
网络架构	b)应保证网络各个部分的带宽满足业务高峰期需要；	否	各个云租户分别测评。
	c)应划分不同的网络区域，并按照方便管理和控制的原则为各网络区域分配地址；	是	核查云平台是否为每个云租户划分网络区域，并分配不同的 IP 地址，结果记录可复用。
	d)应避免将重要网络区域部署在边界处，重要网络区域与其他网络区域之间应采取可靠的技术隔离手段；	是	核查云平台是否未将云租户网络区域部署在云平台边界处，云租户网络区域之间是否采取可靠的技术隔离手段，结果记录可复用。

A.2.2 安全扩展要求部分

云租户不适用。

A.3 安全区域边界

A.3.1 安全通用要求部分

控制点	测评指标	是否统一测评	说明
边界防护	a)应保证跨越边界的访问和数据流通过边界设备提供的受控接口进行通信；	是	核查云平台是否为云租户提供访问控制设备，并由云平台统一提供被测云租户的访问控制策略，结果记录可复用。
访问控制	a)应在网络边界或区域之间根据访问控制策略设置访问控制规则,默认情况下除允许通信外受	是	核查云平台提供的网络边界的访问控制策略以及不同云租户之间的访问控制策略是

控制点	测评指标	是否统一测评	说明
	控接口拒绝所有通信；		否有效，结果记录可复用。
	b)应删除多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化；	是	核查云平台提供的网络边界的访问控制策略以及不同云租户之间的访问控制策略是否最小化，结果记录可复用。
	c)应对源地址、目的地址、源端口、目的端口和协议等进行检查，以允许/拒绝数据包进出；	是	核查云平台提供的访问控制策略中是否设定了源地址、目的地址、源端口、目的端口和协议等相关配置参数，并验证是否有效，结果记录可复用。
	d)应能根据会话状态信息为进出数据流提供明确的允许/拒绝访问的能力；	是	核查云平台提供的访问控制策略，是否能够根据会话状态信息进行访问控制，并生成会话状态列表，并验证是否有效，结果记录可复用。
	e)应对进出网络的数据流实现基于应用协议和应用内容的访问控制。	是	核查云平台是否提供应用层防护安全服务，结果记录可复用。
入侵防范	a)应在关键网络节点处检测、防止或限制从外部发起的网络攻击行为；	是	核查云平台是否提供入侵防范的安全服务，结果记录可复用。
	b)应在关键网络节点处检测、防止或限制从内部发起的网络攻击行为；	是	核查云平台是否提供入侵防范的安全服务，结果记录可复用。
	c)应采取技术措施对网络行为进行分析，实现对网络攻击特别是新型网络攻击行为的分析；	是	核查云平台是否提供相关的安全服务，以实现对网络攻击特别是新型网络攻击行为的分析，结果记录可复用。
	d)当检测到攻击行为时，记录攻击源IP、攻击类型、攻击目标、攻击时间，在发生严重入侵事件时应提供报警。	是	核查云平台提供的安全服务是否具有报警日志或攻击日志，查看日志是否记录入侵源IP、攻击类型、攻击目的、攻击时间等相关内容，结果记录可复用。
恶意代码和垃圾邮件防范	a)应在关键网络节点处对恶意代码进行检测和清除，并维护恶意代码防护机制的升级和更新；	是	核查云平台是否在关键网络节点处部署相关防范恶意代码设备或技术措施，并查看其规则库是否保持最新状态，结果记录可复用。
安全审计	a)应在网络边界、重要网络节点进行安全审计，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	是	核查云平台是否在网络边界处部署了综合安全审计系统或具有类似功能的系统平台，安全审计范围是否覆盖到全部用户，是否能对重要的用户行为和重要安全事件进行审计，结果记录可复用。
	b)审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信	是	核查云平台提供的审计记录信息是否全面，结果记录可复用。

控制点	测评指标	是否统一测评	说明
	息；		
	c)应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等；	是	核查云平台是否提供日志审计系统对日志进行收集和备份，结果记录可复用。
	d)应能对远程访问的用户行为、访问互联网的用户行为等单独进行行为审计和数据分析。	是	核查云平台是否通过 VPN 网关对远程访问用户单独进行审计；统一核查云平台是否部署了上网行为管理系统对用户行为单独进行审计分析；结果记录可复用。

A.3.2 安全扩展要求部分

控制点	测评指标	是否统一测评	说明
访问控制	a)应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；	是	核查云平台是否在虚拟化网络边界（包含以下四个边界：云平台与外部边界、云平台与云服务客户边界、不同云服务客户之间的边界、同一云服务客户不同等级业务系统之间的边界）部署访问控制机制，设置访问控制规则，并测试访问控制策略有效，结果记录可复用。
	b)应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。	否	各个云租户分别测评。
入侵防范	b)应能检测到对虚拟网络节点的网络攻击行为，并能记录攻击类型、攻击时间、攻击流量等；	是	核查云平台是否提供入侵防范的安全服务，是否具有攻击行为记录功能和内部行为监控功能，结果记录可复用。
	c)应能检测到虚拟机与宿主机、虚拟机与虚拟机之间的异常流量；	是	核查云平台流量监测设备、入侵防护系统等监测范围能否覆盖所有虚拟机、宿主机，并对虚拟机与宿主机、虚拟机与虚拟机之间的流量进行实时监测。结果记录可复用。
	d)应在检测到网络攻击行为、异常流量情况时进行告警。	是	核查在检测到网络攻击行为、异常流量时是否进行告警，并查看相关告警记录，结果记录可复用。
安全审计	a)应对云服务商和云服务客户在远程管理时执行的特权命令进行审计，至少包括虚拟机删除、虚拟机重启；	是	检查是否部署审计工具（如堡垒机）对云服务和云服务客户执行特权命令进行审计，核查审计记录是否有效，并查阅审计记录是否包括虚拟机删除、虚拟机重启，结果记录可复用。

控制点	测评指标	是否统一测评	说明
	b)应保证云服务商对云服务客户系统和数据的操作可被云服务客户审计。	是	核查云服务商访问云服务客户系统和数据时，是否采取了相关的审计机制，记录云服务商对云服务客户系统和数据的操作。结果记录可复用。

A.4 安全计算环境

A.4.1 安全通用要求部分

控制点	是否统一测评	说明
安全设备	否	若租户具备云堡垒机的普通业务使用权限，则云堡垒机结果记录可复用
服务器	否	若服务器安全配置由租户个性化修改，则分别测评；若服务器安全配置由云服务方统一提供，则结果记录可复用。
终端	否	分别测评各租户终端。
系统管理软件	否	若租户具备云管平台的普通业务使用权限，则云管平台结果记录可复用；若数据库安全配置由租户个性化修改，则分别测评；若数据库安全配置由云服务方统一提供，则结果记录可复用。分别测评各租户中间件。
应用系统和数据资源	否	分别测评各租户应用系统和数据资源。

A.4.2 安全扩展要求部分

控制点	测评指标	是否统一测评	说明
身份鉴别	a）当远程管理云计算平台中设备时，管理终端和云计算平台之间应建立双向身份验证机制。	是	核查云管平台或云堡垒机，当进行远程管理时是否建立双向身份验证机制，结果记录可复用。
入侵防范	b)应能检测非授权新建虚拟机或者重新启用虚拟机，并进行告警；	是	检查云管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，是否能够提供告警方式及记录。结果记录可复用。
	c）应能够检测恶意代码感染及在虚拟机间蔓延的情况，并进行告警。	是	检查云平台是否部署恶意代码防护系统，是否具备检测恶意代码感染及在虚拟机间蔓延情况并进行告警的功能。结果记录可复用。

控制点	测评指标	是否统一测评	说明
数据完整性和保密性	a）应确保云服务客户数据、用户个人信息等存储于中国境内，如需出境应遵循国家相关规定；	是	核查云租户业务数据、用户个人信息所在的服务器及数据存储设备是否位于中国境内，结果记录可复用。
数据备份恢复	a）云服务客户应在本地保存其业务数据的备份；	否	各个云租户分别测评。

A.5 安全管理中心

安全管理中心通过云平台提供的安全服务（如：云堡垒机、云管平台等）实现对各云租户的集中管理，本层面核查云平台所提供的安全服务，各租户记录可复用。

A.6 安全管理

控制点	是否统一测评	说明
安全管理制度	否	若租户属于同一责任主体，结果记录可复用；若租户不属于同一责任主体，则需分别测评
安全管理机构	否	若租户属于同一责任主体，结果记录可复用；若租户不属于同一责任主体，则需分别测评
安全管理人员	否	若租户属于同一责任主体，结果记录可复用；若租户不属于同一责任主体，则需分别测评
安全建设管理	否	安全通用要求需分别测评。若租户部署在同一朵云，则安全扩展要求结果记录可复用；否则需分别测评
安全运维管理	否	安全通用要求需分别测评，安全扩展要求云租户不适用