ICS 35.020
L 70

CIIA

中 国 信 息 协 会 团 体 标 准

T/CIIAxxx---xxxx

政务云网络安全合规性指引

Compliance Guidelines for Government Cloud Network Security

（征求意见稿）

XXXX-XX-XX 发布　　XXXX-XX-XX 实施

中国信息协会发布

目　　次

前　言

本标准按照GB/T1.1-2009给出的规则起草。

本标准由中国信息协会提出并归口。

本标准负责起草单位：国家信息中心

本标准参加起草单位：安徽省经济信息中心、江西省信息中心、新华三技术有限公司、华为技术有限公司、深信服科技股份有限公司等单位参与编制。

本指标准主要起草人：禄凯、任金强、章恒、姜精如、杜军龙、武海龙、程寅、周剑涛、高亚楠、尚庆军、国强、刘蓓、赵睿斌、许涛、沈桂斌、董涛、薛征宇。

引　言

习近平总书记在2018年全国网络安全和信息化工作会议上指出：要运用信息化手段推进政务公开、党务公开，加快推进电子政务，构建全流程一体化在线服务平台，更好解决企业和群众反映强烈的办事难、办事慢、办事繁的问题。

国发〔2015〕5号文《国务院关于促进云计算创新发展培育信息产业新业态的意见》指出：充分发挥云计算对数据资源的集聚作用，实现数据资源的融合共享，推动大数据挖掘、分析、应用和服务。该意见同时指出：加强云计算服务网络安全防护管理，加大云计算服务安全评估力度，建立完善党政机关云计算服务安全管理制度；落实国家信息安全等级保护制度，开展定级备案和测评等工作；完善云计算安全态势感知、安全事件预警预防及应急处置机制，加强对党政机关和金融、交通、能源等重要信息系统的安全评估和监测。

发改高技〔2017〕1449 号明确指出：到“十三五”末期，构建形成大平台共享、大数据慧治、大系统共治的顶层架构，建成全国一体化的国家大数据中心。形成安全可控、集成创新、分类服务的政务云，承载国家数据共享交换枢纽、国家公共数据开放网站、国家基础信息资源库以及跨部门重大信息化工程，依托国家政务数据中心构建部门私有云，推动部门数据中心逐步向国家政务数据中心迁移。

政务云作为面向政务应用提供服务的基础平台，其通过整合公共资源，实现不同电子政务系统间的信息整合、交换、共享和政务工作协同，提高服务效率和服务能力。政务云在承载政务应用的同时，也承载了大量的事关民生的业务，对业务连续性、敏感信息保护、数据安全可靠等方面提出了更高要求。

习近平总书记指出“没有网络安全就没有国家安全”，政务云作为服务于各级政务部门的基础平台，其网络安全建设更是国家安全意志的体现。

政务云的安全首先体现在依法合规方面，应建设一个守法的、经得起服务安全审查的、达到相应网络安全等级保护标准和满足政务行业安全属性的网络安全体系。

本标准参照《GB/T22239-XXXX 信息安全技术 网络安全等级保护基本要求》（报批稿）等网络安全等级保护相关标准、《GB/T31167-2014 信息安全技术 云计算服务安全指南》、《GB/T31168-2014 信息安全技术 云计算服务安全能力要求》、《国家电子政务外网安全等级保护基本要求》、《国家电子政务外网安全等级保护实施指南》、《国家电子政务外网跨网数据安全交换技术要求与实施指南》、《国家电子政务外网安全接入平台技术规范》等进行编写，按照网络安全等级保护中要求条款的组织架构，整合上述标准体系规范中政务云安全相关要求，从而形成一套统一的政务云网络安全合规要求体系。后续将按照国家相关政策标准规范的进展持续更新完善。

本标准第一章简要介绍了政务云安全的重要性及背景；第二章分别介绍了网络安全法、网络安全等级保护、云计算服务安全审查、政务行业网络安全一般性要求等法规标准关于政务云相关的安全要求；第三章对政务云整个建设运行过程中，在网络安全方面应该采取的措施及进行的工作进行了说明；第四章以网络安全等级保护基本要求框架为基础，将云计算服务安全审查相关要求条款、政务行业网络安全一般性要求条款整合到等级保护相关层面的控制点上，形成一套统一的政务云网络安全合规要求体系。

政务云网络安全合规性指引

1 范围

本标准以国家网络安全法为指导，以国家网络安全等级保护相关要求为核心，以网络安全等级保护技术标准为基础，梳理和整合等级保护、云计算服务网络安全审查、政务行业网络安全一般性要求三个方面的内容，分析和明确各方技术要求差异，研究和制定符合各方要求的综合性对标指导要求，从而形成一体的政务云网络安全合规体系。

本标准在依据国家相关技术标准的同时，力争突出电子政务领域网络安全特点，为各级政府规划好、建设好、管理好政务云提供参考。同时，也可为其他行业的云网络安全保障工作提供参考。

2 规范性引用文件

下列文件对于本文件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文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T22240-XXXX 信息安全技术 网络安全等级保护定级指南（报批稿）
GB/T25058-XXXX 信息安全技术 网络安全等级保护实施指南（报批稿）
GB/T22239-XXXX 信息安全技术 网络安全等级保护基本要求（报批稿）
GB/T25070-XXXX 信息安全技术 网络安全等级保护安全设计技术要求（报批稿）
GB/T28448-XXXX 信息安全技术 网络安全等级保护测评要求（报批稿）
GB/T28449-XXXX 信息安全技术 网络安全等级保护测评过程指南（报批稿）
GB/T31167-2014 信息安全技术 云计算服务安全指南
GB/T31168-2014 信息安全技术 云计算服务安全能力要求
GW0013-2017 政务云安全要求
GW0104-2014 国家电子政务外网安全等级保护实施指南
GW0103-2004 国家电子政务外网安全等级保护基本要求
GW0203-2014 国家电子政务外网安全监测体系技术规范与实施指南
GW0204-2014 国家电子政务外网安全管理系统技术要求与接口规范
GW0205-2014 国家电子政务外网跨网数据安全交换技术要求与实施指南
DB36/T 979-2017 电子政务外网安全接入平台技术规范

3 术语和定义

下列术语和定义适用于本文件。

3.1

政务云 GovernmentCloud

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。

3.2

国家电子政务外网 NationalE-GovernmentNetwork

国家电子政务外网是国家电子政务重要基础设施，是承载各级政务部门用于经济调节、市场监管、社会管理和公共服务等非涉及国家秘密的业务应用系统的政务公用网络。包括中央级政务外网和地方政务外网，二者均由相应的广域网和城域网构成。中央广域网与31个省、直辖市、自治区和新疆生产建设兵团的省级政务外网互联。中央城域网用于连接在京中央政务部门，并与中央广域网高速互联。地方政务外网由省、地（市）和县级广域网和相应的城域网构成。

3.3

关键信息基础设施 CriticalInformationInfrastructure

面向公众提供网络信息服务或支撑能源、通信、金融、交通、公用事业等重要行业运行的信息系统或工业控制系统;且这些系统一旦发生网络安全事故,会影响重要行业正常运行,对国家政治、经济、科技、社会、文化、国防、环境以及人民生命财产造成严重损失。

3.4

云服务商 CloudServiceProvider

云计算服务的提供商。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。

3.5

云服务客户 CloudTenant

使用政务云开展电子政务业务和处理、存储数据的各级政务部门。

3.6

安全管理平台 SecurityOperationCenter

安全管理平台是通过采用多种技术手段，收集和整合各类网络设备、安全设备、操作系统等安全事件，并运用关联分析技术、智能推理技术和风险管理技术，实现对安全事件信息的深度分析，能快速做出智能响应，实现对安全风险进行统一监控分析和预警处理。

3.7

广域网 WideAreaNetworks(WAN)

把城市之间连接起来的宽带网络称广域网,政务外网从中央到各省的网络称为中央广域网、省到各地（市）网络称为省级广域网、地（市）到各县的广域网称为地（市）级广域网。实现国家、省、市、县纵向业务的互联网通。

3.8

城域网 MetropolitanAreaNetworks（MAN）

把同一城市内不同单位的局域网络连接起来的网络称为城域网,实现不同单位跨部门业务的数据共享与交换。

3.9

局域网 LocalAreaNetwork（LAN）

把本单位终端、主机/服务器、存储等设备，通过网络设备连接起来的网络，实现本单位业务系统、数据的互访、共享等，称为局域网。局域网是政务部门开展电子政务业务的基础，其安全、建设、运维等相关工作由网络所属单位自行负责。

3.10

逻辑隔离 LogicIsolation

逻辑隔离是一种不同网络间的安全防护措施，被隔离的两端仍然存在物理上数据通道连线。一般使用协议转换、数据格式剥离或数据流控制的方法来实现在两个逻辑隔离区域之间传输数据，并且传输的方向可以是单向或双向。

3.11

公用网络区 PublicNetworkArea

公用网络区采用统一分配的公共IP地址，是实现各部门、各地区互联互通，为跨地区、跨部门的业务应用提供数据共享与交换的网络支撑平台。

3.12

互联网接入区 InternetAccessArea

是各级政务部门通过逻辑隔离安全接入互联网的网络区域，满足各级政务部门访问互联网的需要。同时也是移动办公的公务人员通过政务外网数字证书，经网关认证后安全接入政务外网的途径。按属地化管理的原则，中央和地方分别管理各自的互联网出入口。

3.13

安全管理区 SecurityManagementArea

安全管理区主要承载安全管理信息系统，对管辖范围内网络中部署的安全防护设备进行日志采集、关联分析、对网络病毒和攻击进行告警、对安全事故提出预警和采取措施的建议，定期总结并提出分析报告。

3.14

数字证书 DigitalCertificate

数字证书为实现双方安全通信提供了电子身份认证。在利用互联网、政务外网或局域网时，使用数字证书实现身份识别和电子信息加密。数字证书中含有密钥对（公钥和私钥）所有者的识别信息，通过验证识别信息的真伪实现对证书持有者身份的认证，数字证书包含公开密钥拥有者的信息、公开密钥、签发者信息、有效期以及一些扩展信息的数字文件。

4 政务云安全合规解读

在第八届全国网络安全等级保护测评体系建设会议上提出：推动以“等保+专项安全扩展”的安全新模式，随着《网络安全法》的出台，关键信息基础设施保护、网络安全审查、密评、互联网新技术新业务评估、数据出境安全评估、个人信息安全规范、大数据安全、云计算安全和工业控制系统安全和物联网安全等等相关配套性的评测、保护标准陆续推出。网络空间的安全治理将进一步走向细分，相关领域的专门性安全要求与细则被陆续制定和施行，形成更加庞大、完善的网络安全体系，势必对各个重点行业的信息系统提出更高的安全合规与风险管理要求。

本文在政务云安全领域已率先迈出了第一步，推出了政务云网络安全合规“1+2”三合一

的模式，从而帮助相关方夯实安全基础、满足多方合规、获得整体安全、降低安全成本。

政务云网络安全合规应遵循多个标准制度规范，包括：等级保护系列标准、云计算服务网络安全审查系列标准、电子政务安全系列标准，还有目前制定中的关键信息基础设施保护、密评、个人信息保护、大数据安全等标准。**本文以网络安全法为指导，以国家网络安全等级保护相关要求为基础，整合等级保护、云计算服务网络安全审查、政务行业网络安全一般性要求三个方面的内容，从而形成一体的政务云网络安全合规体系。**后续将根据关键信息基础设施保护、密评、个人信息保护、大数据安全等相关标准的进展，进一步完善。本文参考标准及其关系框架如下图所示。

图1 政务云网络安全合规标准框架

4.1 网络安全法

《中华人民共和国网络安全法》（以下简称《网络安全法》）由全国人民代表大会常务委员会于 2016 年 11 月 7 日发布，自 2017 年 6 月 1 日起施行。《网络安全法》是我国第一部全面规范网络空间安全管理方面问题的基础性法律，是我国网络空间法治建设的重要里程碑，是依法治网、化解网络风险的法律重器，是让互联网在法治轨道上健康运行的重要保障。《网络安全法》将近年来一些成熟的好做法制度化，并为将来可能的制度创新做了原则性规定，为网络安全工作提供切实法律保障。

《网络安全法》总体架构可以概括为三大战略、四大原则和八项制度设计，提出网络安

全、人才培养和可信身份三大战略，将习总书记强调的和平、安全、开放、合作原则以立法形式确定下来，八项制度贯穿了网络运行安全、产品和服务安全、数据安全的全过程规定了网络安全等级保护制度、关键信息基础设施（CII）保护制度、网络产品和服务的审查制度、数据跨境传输制度、个人信息保护制度、安全认证和检测制度、信息通报制度、网络安全事件应急处置制度。

根据《网络安全法》的要求，政务云的安全建设需要重点关注以下方面：

a） 政务云的安全建设应遵循国家网络安全等级保护制度。

b） 政务云作为关键信息基础设施，其安全建设在网络安全等级保护建设的基础上，应实行重点防护。

c） 政务云为政务部门提供服务，采购网络产品和服务，可能影响国家安全的，应当通过中央网信部门会同国务院有关部门组织的安全审查。

d） 政务云中涉及大量公民个人信息，应建立健全信息管理制度与措施。

e） 遵循网络用户实名制要求，应推进政务终端的证书强认证制度、措施及建设。

f） 应建立网络安全监测预警和信息通报制度，深化政务云网络安全防护体系，实现全天候全方位感知网络安全态势。

4.2 网络安全等级保护

随着我国信息技术的快速发展，特别是云计算、移动互联、物联网、大数据等新技术、新应用的出现给信息安全引入了新的安全威胁与风险。为加强对采用云计算、移动互联、物联网、大数据等新技术的等级保护对象的安全保护，推动新技术、新应用安全满足等级保护合规要求，形成了等级保护系列扩展标准。

2018年6月27日，公安部正式发布《网络安全等级保护条例（征求意见稿）》（以下称“《等保条例》”），标志着《网络安全法》（以下称“《网安法》”）第二十一条所确立的网络安全等级保护制度有了具体的实施依据与有力抓手。《等保条例》共八章七十三条，包括总则、支持与保障、网络的安全保护、涉密网络的安全保护、密码管理、监督管理、法律责任和附则。相较于2007年实施的《信息安全等级保护管理办法》（以下称“《管理办法》”）所确立的等级保护1.0体系，《等保条例》在国家支持、定级备案、密码管理等多个方面进行了更新与完善，适应了现阶段网络安全的新形势、新变化以及新技术、新应用发展的要求，标志着等级保护正式迈入2.0时代。

4.2.1 定级指南

等级保护定级指南是依据等级保护相关政策文件，综合考虑保护对象在国家安全、经济建设、社会生活中的重要程度，以及保护对象遭到破坏后对国家安全、社会秩序、公共利益以及公民、法人和其他组织的合法权益的危害程度等因素，提出确定保护对象安全保护等级的方法。

网络安全等级保护定级对象的具体范围，主要包括基础信息网络、工业控制系统、云计算平台、物联网、使用移动互联技术的网络、其他网络以及大数据等多个系统平台。另外，作为定级对象的网络还应当满足三个基本特征：

第一，具有确定的主要安全责任主体；

第二，承载相对独立的业务应用；

第三，包含相互关联的多个资源。

在采用云计算的政务云中，应区分为服务提供方与租户方，各自分别作为定级对象，即**云平台及云上租户业务系统需要单独定级**。如果**属于国家关键信息基础设施的安全保护等级应不低于第三级。**

等级保护对象的级别由两个定级要素决定：

a) 受侵害的客体

b) 对客体的侵害程度

等级保护对象定级的一般流程如下：

a) 确定定级对象

b) 初步确定等级

c) 专家评审

d) 主管部门审核

e) 公安机关备案审查

定级指南中对受侵害的客体以及侵害程度的划分进行了详细的定义，具体定级划分请参照以下表格：

表1 网络安全等级保护体系下定级要素与安全保护等级的关系

受侵害的客体	对客体的侵害程度		
	一般损害	严重损害	特别严重损害
公民、法人和其它组织的合法权益	第一级	第二级	第三级
社会秩序、公共利益	第二级	第三级	第四级
国家安全	第三级	第四级	第五级

4.2.2 基本要求

为了配合《中华人民共和国网络安全法》的实施，适应云计算、移动互联、物联网、工业控制和大数据等新技术、新应用情况下网络安全等级保护工作的开展，对 GB/T 22239—2008 进行了修订，修订的思路和方法是调整原国家标准 GB/T 22239—2008 的内容，针对共性安全保护需求提出安全通用要求，针对云计算、移动互联、物联网、工业控制和大数据等新技术、新应用领域的个性安全保护需求提出安全扩展要求，形成新的网络安全等级保护基本要求标准。

新的网络安全等级保护基本要求标准包含**安全通用要求**和**安全扩展要求（含云计算、移动互联、物联网、工业控制）**。

在 GB/T 22239 网络安全等级保护基本要求包括如下 5 部分：

a) 安全通用要求

b) 云计算安全扩展要求

c) 移动互联安全扩展要求

d) 物联网安全扩展要求

e) 工业控制系统安全扩展要求

其中，安全通用要求是所有等级保护对象都必须满足的要求，安全扩展要求是针对云计算、移动互联、物联网和工业控制系统提出的针对性扩展要求。

基本要求中二级及以上要求将安全层面共划分为 10 个分类：技术部分和设计要求保持一致，即沿用“一个中心三重防护”的防护理念，在安全物理环境外，即每一级包含：安全计算环境、安全区域边界、安全通信网络、安全管理中心。

技术部分：

a) 安全物理环境

b) 安全通信网络

c) 安全区域边界

d) 安全计算环境

e) 安全管理中心

管理部分：

a) 安全管理制度

b) 安全管理机构

c) 安全管理人员

d) 安全建设管理

e) 安全运维管理

由于等级保护对象承载的业务不同，对其的安全关注点会有所不同，有的更关注信息的安全性，即更关注对搭线窃听、假冒用户等可能导致信息泄密、非法篡改等；有的更关注业务的连续性，即更关注保证系统连续正常的运行，免受对系统未授权的修改、破坏而导致系统不可用引起业务中断。

不同级别的等级保护对象，其对业务信息的安全性要求和系统服务的连续性要求是有差异的，即使相同级别的等级保护对象，其对业务信息的安全性要求和系统服务的连续性要求也有差异。

等级保护基本要求中的技术安全要求进一步细分为：保护数据在存储、传输、处理过程中不被泄漏、破坏和免受未授权的修改的**信息安全类要求（简记为 S）**；保护系统连续正常的运行，免受对系统的未授权修改、破坏而导致系统不可用的**服务保证类要求（简记为 A）**；**其他安全保护类要求（简记为 G）。标准中所有安全管理要求和安全扩展要求均标注为 G。**

在云计算安全扩展要求中，针对云计算环境，标准对云计算、云服务商、云服务客户、云计算平台、虚拟机监视器、宿主机等进行了定义，主要增加的控制项包括：“基础设施位置”、“虚拟化安全保护”、“镜像和快照保护”、“云服务商选择”、“云计算环境管理”等。主要内容如下：

a) 安全物理环境

云计算基础设施的物理位置必须位于中国境内。

b) 安全通信网络

云计算平台不承载高于其安全保护等级的业务应用系统，并实现不同云服务客户虚拟网络之间的隔离；云计算平台可以根据云服务客户业务需求提供通信传输、边界防护、入侵防范等安全机制的能力；保证云计算平台管理流量与云服务客户业务流量分离，可根据云服务客户业务需求自主设置安全策略的能力，包括定义访问路径、选择安全组件、配置安全策略。云计算平台应提供开放接口或开放性安全服务，允许云服务客户接入第三方安全产品或在云计算平台选择第三方安全服务。

c) 安全区域边界

应在虚拟化网络边界和不同等级的网络区域边界部署访问控制机制，并设置访问控制规则；应能检测到云服务客户发起的和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。 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，并在检测到网络攻击行为、异常流量情况时进行告警。应对云服务商和云服务客户相关操作进行安全审计等。

d) 安全计算环境

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。采取密码技术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。云服务商的云存储服务应保证云服务客户数据存在若干个可用的副本，各副本之间的内容应保持一致；应为云服务客户将业务系统及数据迁移到其他云计算平台和本地系统提供技术手段，并协助完成迁移过程。应能检测虚拟机之间的资源隔离失效，并进行告警；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；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。

使用密码技术保证虚拟机迁移过程中，重要数据的保密性，防止在迁移过程中的重要数据泄露。在故障发生时，应能够继续提供一部分功能，保证能够实施必要的措施。利用通信网络将重要数据实时备份至备份场地，重要数据处理系统需要热冗余，保证系统的高可用性。

e) 安全管理中心

应能对物理资源和虚拟资源按照策略做统一管理调度与分配；应保证云计算平台管理流量与云服务客户业务流量分离；应根据云服务商和云服务客户的职责划分，收集各自控制部分的审计数据并实现各自的集中审计；应根据云服务商和云服务客户的职责划分，实现各自控制部分，包括虚拟化网络、虚拟机、虚拟化安全设备等的运行状况的集中监测。

f) 安全管理制度

制定网络安全工作的总体方针和安全策略，阐明机构安全工作的总体目标、范围、原则和安全框架等。形成由安全策略、管理制度、操作规程、记录表单等构成的全面的信息安全管理制度体系。指定或授权专门的部门或人员负责安全管理制度的制定。安全管理制度应通过正式、有效的方式发布，并进行版本控制。定期对安全管理制度的合理性和适用性进行论证和审定，对存在不足或需要改进的安全管理制度进行修订。

g) 安全管理机构

建立由上到下全覆盖的安全管理组织机构。成立指导和管理信息安全工作的委员会或领导小组，其最高领导由单位主管领导委任或授权。设立信息安全管理工作的职能部门，设立安全主管、安全管理各个方面的负责人岗位，并定义各负责人的职责。设立系统管理员、审计管理员、安全管理员等岗位，并定义部门及各个工作岗位的职责，并且安全管理员为专职，不可兼任。

h) 安全管理人员

与被录用人员签署保密协议，与关键岗位人员签署岗位责任协议，离岗人员应办理严格的调离手续，并承诺调离后的保密义务后方可离开。并定期对不同岗位的人员进行技能考核。不同岗位制定不同的培训计划，对信息安全基础知识、岗位操作规程等进行培训。

i) 安全建设管理

选择安全合规的云服务商，其所提供的云平台应为其所承载的业务应用系统提供相应等级的安全保护能力；服务水平协议中规定云服务的各项服务内容和具体技术指标，在服务水平协议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。在服务水平协议中规定服务合约到期时，完整地返还云服务客户信息，并承诺相关信息在云计算平台上清除。签署保密协议，要求云服务商不得泄露云服务客户数据和业务系统的相关重要信息。将供应商的重要变更及时传达到云服务客户，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。

j) 安全运维管理

云计算平台的运维地点应位于中国境内，境外对境内云计算平台实施运维操作应遵循国家相关规定。云计算平台运维过程产生的配置数据、日志信息等存储于中国境内，如需出境应遵循国家相关规定。

4.2.3 设计要求

国家标准 GB/T 25070-2010《信息安全技术 信息系统等级保护安全设计技术要求》是各行业和领域开展信息安全等级保护设计建设整改等工作的主要依据。

新修订的 GB/T 25070 对云计算、移动互联、物联网、工业控制和大数据等新技术新应用领域提出对应的设计要求，并在适用性、时效性、易用性、可操作性上做了进一步完善。

新修订的 GB/T 25070 沿用“一个中心三重防护”的防护理念，在通用的等级保护安全设计框架下，针对云计算、移动互联、物联网、工业控制和大数据系统提出了新的安全设计框

架。在每一级的“安全计算环境设计技术要求”、“安全区域边界设计技术要求”、“安全通信网络设计技术要求”中，除了通用设计外，增加了针对云计算、移动互联、物联网、工业控制和大数据系统的设计要求。

遵循 GB 17859-1999 中的相关要求，不同等级因遵循不同的安全设计策略。具体如下：

a) 二级应遵循的设计策略

第二级系统安全保护环境的设计策略是：遵循 GB 17859-1999 的 4.2 中相关要求，以身份鉴别为基础，提供单个用户和（或）用户组对共享文件、数据库表等的自主访问控制；以包过滤手段提供区域边界保护；以数据校验和恶意代码防范等手段，同时通过增加系统安全审计、客体安全重用等功能，使用户对自己的行为负责，提供用户数据保密性和完整性保护，以增强系统的安全保护能力。

第二级系统安全保护环境的设计通过第二级的安全计算环境、安全区域边界、安全通信网络以及安全管理中心的设计加以实现。

b) 三级应遵循的设计策略

构造非形式化的安全策略模型，对主、客体进行安全标记，表明主、客体的级别分类和非级别分类的组合，以此为基础，按照强制访问控制规则实现对主体及其客体的访问控制。

c) 四级应遵循的设计策略

在第三级系统安全保护环境设计的基础上，遵循 GB 17859-1999 的 4.4 中相关要求，通过安全管理中心明确定义和维护形式化的安全策略模型。依据该模型，采用对系统内的所有主、客体进行标记的手段，实现所有主体与客体的强制访问控制。同时，相应增强身份鉴别、审计、安全管理等功能，定义安全部件之间接口的途径，实现系统安全保护环境关键保护部件和非关键保护部件的区分，并进行测试和审核，保障安全功能的有效性。第四级系统安全保护环境的设计通过第四级的安全计算环境、安全区域边界、安全通信网络以及安全管理中心的设计加以实现。

d) 定级系统互联的设计策略

遵循 GB 17859-1999 对各级系统的安全保护要求，在各定级系统的计算环境安全、区域边界安全和通信网络安全的基础上，通过安全管理中心增加相应的安全互联策略，保持用户身份、主/客体标记、访问控制策略等安全要素的一致性，对互联系统之间的互操作和数据交换进行安全保护。等级保护安全技术设计应遵循如下过程：

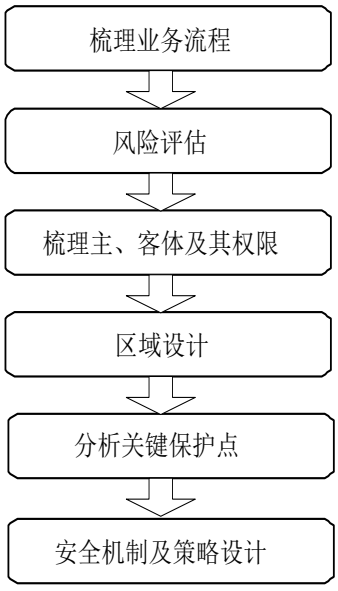

图 2 等级保护安全技术设计过程

结合云计算功能分层框架和云计算安全特点，构建云计算安全设计防护技术框架，包括云用户层、访问层、资源层、服务层、资源层、硬件设施层和管理层（跨层功能）。其中一个中心是指安全管理中心，三重防护包括安全计算环境、安全区域边界和安全通信网络。具体如图所示：

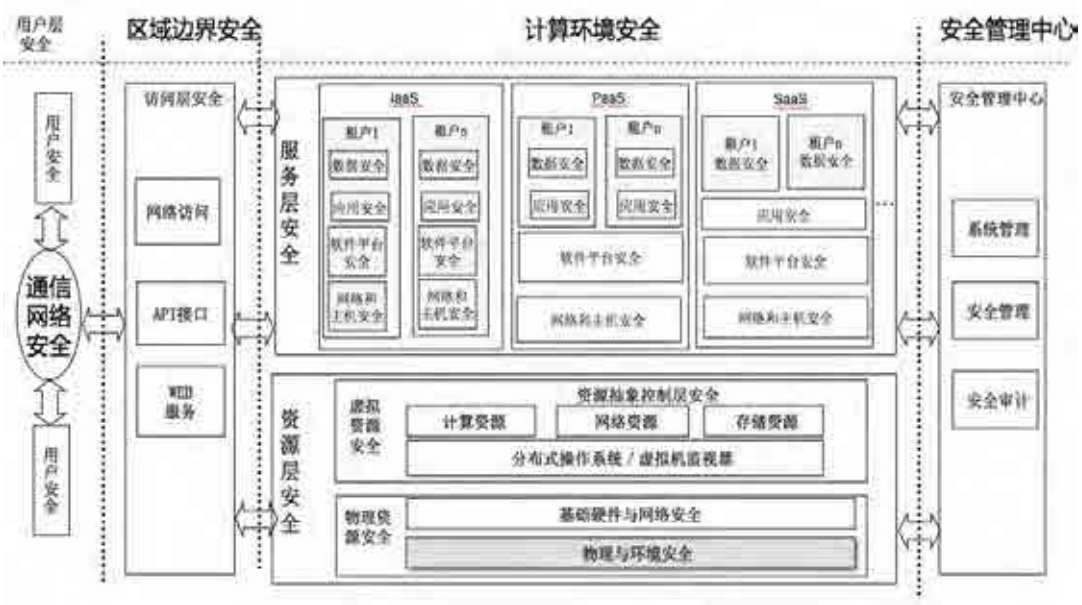

图 3 云计算安全设计防护技术框架

用户通过安全的通信网络以网络直接访问、API 接口访问和 WEB 服务访问等方式安全地访问云服务商提供的安全计算环境，其中用户终端自身的安全保障不在本部分范畴内。安全计算环境包括资源层安全和服务层安全。其中，资源层分为物理资源和虚拟资源，需要明确物理资源安全设计技术要求和虚拟资源安全设计要求，其中物理与环境安全不在本部分范畴内。服务层是对云服务商所提供服务的实现，包含实现服务所需的软件组件，根据服务模式不同，云服务商和云服务客户承担的安全责任不同。服务层安全设计需要明确云服务商控制的资源范围内的安全设计技术要求，并且云服务商可以通过提供安全接口和安全服务为云服务客户提供安全技术和安全防护能力。云计算环境的系统管理、安全管理和安全审计由安全管理中心统一管控。

设计包含两个方面：一是结合本框架对不同等级的云计算环境进行安全技术设计，二是通过服务层安全支持对不同等级云服务客户端（业务系统）的安全设计。

4.2.4 测评要求

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》是各行业和领域开展信息安全等级保护等级测评等工作的依据。

对照 GB/T 22239 网络安全等级保护基本要求的修订内容，测评要求也做了相应修订，对共性安全保护需求给出了安全测评通用要求，对云计算、移动互联、物联网、工业控制和大数据等新技术新应用领域的个性安全保护需求给出了相应的扩展测评要求。

a) 等级测评技术框架

等级测评技术框架分为**单项测评**和**整体测评**。

单项测评是针对各安全要求项的测评，支持测评结果的可重复性和可再现性。本标准中单项测评由测评指标、测评对象、测评实施和单元判定构成。修订后的单项测评中测评指标更加细化，由原标准中的安全控制点调整为安全控制点下的具体安全要求项，更有助于测评实施的开展。

整体测评是在单项测评基础上，对等级保护对象整体安全保护能力的判断。整体测评内容由原标准的安全控制点间、层面间和区域间测评等方面调整为安全控制点测评、安全控制点间测评和层面间测评。

另外，为了更好使机构测评人员明确测评工作的作用对象，在测评单元中增加了测评对象说明。测评对象是指等级测评过程中不同测评方法作用的对象，主要涉及相关配套制度文档、设备设施及人员等。

b) 标准主要内容

测评要求沿用正在修订中的《网络安全等级保护定级指南》GB/T 22240 提出的“等级保护对象”概念，并给出针对等级保护对象的安全等级保护测评的定义。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 报批稿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 报批稿中，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 报批稿中相应测评要求开发其测评指导书，如：对云管理平台、虚拟机监视器，可参照安全计算环境部分；对虚拟网络设备、虚拟安全设备，可参照安全通信网络、安全区域边界部分。

依据 GB/T 22239 报批稿标准文本架构，测评要求描述了如何从安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心、安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理十个层面进行测评实施工作。为了更加易于使用测评要求，增加《附录 B 测评单元编号说明》和《附录 D 基本要求和测评要求对应表》。

c) 测评要求的级差

不同等级的测评工作主要通过以下四个方面来体现测评要求的级差：

1) 不同级别使用不同测评方法：第一级主要以访谈为主进行等级测评，第二级以核查为主进行等级测评，第三级和第四级在核查基础上还要进行测试验证工作。不同级别使用不同测评方法，能体现出测评实施过程中访谈、核查和测试的测评强度的不同。
2) 不同级别测评对象范围不同：第一级和第二级测评对象的范围为关键设备，第三级为主要设备，第四级为所有设备。不同级别测评对象范围不同，能体现出测评实施过程中访谈、核查和测试的测评广度的不同。
3) 不同级别现场测评实施工作不同：第一级和二级以核查安全机制为主，第三级和第四级先核查安全机制，再核查安全策略有效性。
4) 等级测评的力度不同：具体见下表：“不同级别的等级保护对象的测评力度要求”。

表 2 不同级别的等级保护对象的测评力度要求

测评力度	测评方法	第一级	第二级	第三级	第四级
广度	访谈	测评对象在种类和数量上抽样，种类和数量都较少	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
	核查				
	测试				
深度	访谈	简要	充分	较全面	全面
	核查				
	测试	功能测试	功能测试	功能测试和测试验证	功能测试和测试验证

d) 与设计要求进行融合

为了更好落实等级保护制度，推动等级保护技术标准的发展，新修订的测评要求增加了《附录 C 设计要求测评验证表》。根据设计要求提出的“一个中心，三重防护”的安全保护思想，从安全管理中心、安全计算环境、安全区域边界和安全通信网络四个方面，测评要求能够全面验证新修订的《设计要求》。

4.3 云计算服务安全审查

2014 年中网办发布《关于加强党政部门云计算服务网络安全管理的意见》（中网办发文〔2014〕14 号）（以下称“14 号文”），进一步明确党政部门云计算服务网络安全管理的基本要求，提出了“安全管理责任不变，数据归属关系不变，安全管理标准不变，敏感信息不出境”四条基本要求。同时在云计算、大数据、“互联网+”等文件中都提出进一步推进政府采购云服务等相关内容，并提出相关落实措施。

云计算服务安全审查中，要求立足风险，向政府部门提供云计算服务的时候要求安全可控。结合政策要求和技术标准，基于云计算环境下的安全风险，审查党政部门云计算服务的安全性和可靠性。安全审查以审为主，同时加强监督和管理。云计算服务是持续的过程，更关键的是靠持续监督，从而保证云计算服务持续满足政务系统安全保障服务的要求。

云计算服务安全审查主要参照《GB/T 31167-2014 信息安全技术 云计算服务安全指南》、《GB/T 31168-2014 信息安全技术 云计算服务安全能力要求》，这两项标准于 2014 年正式发布，2015 年 4 月 1 号正式实施。目的是针对政府部门采用云计算服务的场景，作为政府部门的用户，应采用通过审查的云计算服务，两项标准是基本的准则。云计算服务安全审查流程见下图。

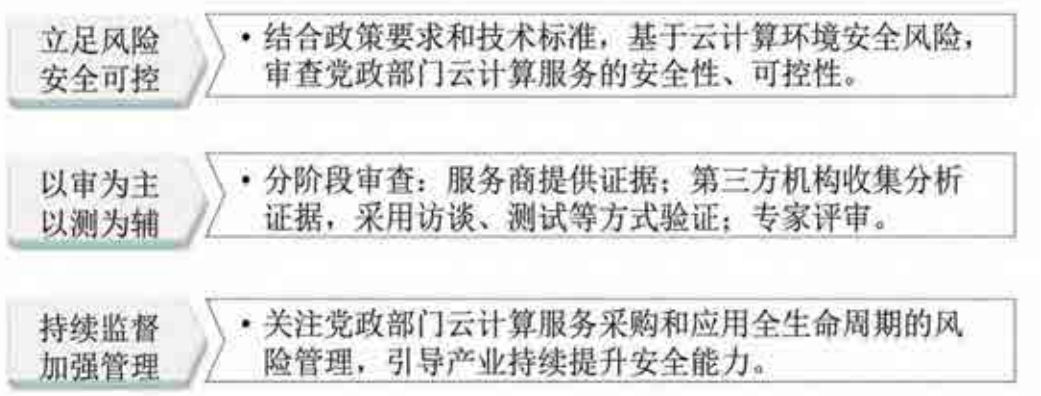

图 4 云计算服务安全审查流程

云计算服务安全指南，是从用户的视角来看，作为政府部门重点行业的客户，在采用云计算服务的时候应该如何做，指导用户安全地使用云计算服务，主要内容包括在云计算服务生命周期中采取的相应安全技术和管理措施，保障数据和业务的安全。

云计算服务安全能力要求，是从云服务商的视角，告诉云服务商，要向政府部门提供云计算服务的时候，应该具备哪些能力，要达到什么样的要求。

云计算服务安全审查职责及分工见下图。

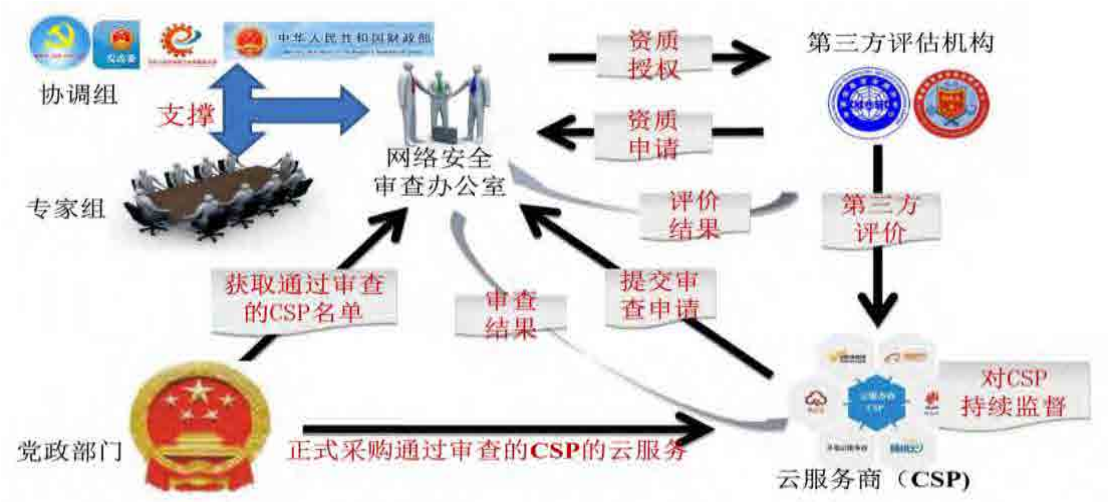

图 5 云计算服务安全审查职责及分工

4.3.1 云计算服务安全指南

《GB/T 31167-2014 信息安全技术 云计算服务安全指南》描述了云计算可能面临的主要安全风险，提出了政务部门采用云计算服务的安全管理基本要求及云计算服务生命周期各阶段的安全管理和技术要求。

本标准为政务部门采用云计算服务，特别是采用社会化的云计算服务提供全生命周期的安全指导，采购和使用云计算服务的过程可分为四个阶段:规划准备、选择服务商与部署、运行监管、退出服务，如下图所示：

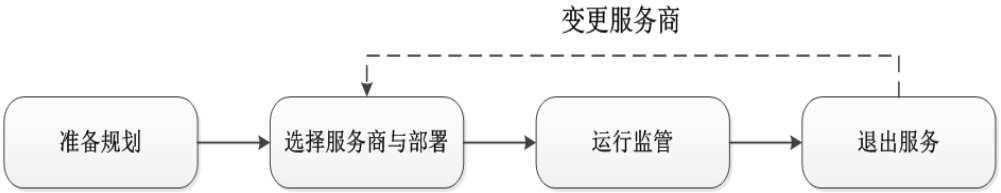

图 6 云计算服务的生命周期

在规划准备阶段，政务部门应分析采用云计算服务的效益，确定自身的数据和业务类型，判定是否适合采用云计算服务；开展政府信息和业务分类，根据数据和业务的类型确定云计算服务的安全能力要求；根据云计算服务的特点进行需求分析，确定服务优先级和安全保护要求。

在选择服务商与部署阶段，政务部门应根据安全需求和云计算服务的安全能力，以及云服务商的安全服务能力选择云服务商，并进行人员背景调查，与云服务商协商合同(包括服务水平协议、安全需求、保密要求等内容)，完成数据和业务向云计算平台的部署或迁移。

在运行监管阶段，政务部门应指导监督云服务商履行合同规定的责任义务，指导督促业务系统使用者遵守政府信息系统安全管理政策及标准，共同维护数据、业务及云计算环境的安全。

在退出云计算服务时，政务部门应要求云服务商履行相关责任和义务，确保退出云计算服务阶段数据和业务安全，如安全返还相关数据、彻底清除云计算平台上的相关数据等。

需变更云服务商时，政务部门应按要求选择新的云服务商，重点关注云计算服务迁移过程的数据和业务安全；也应要求原云服务商履行相关责任和义务。

标准框架如下图：

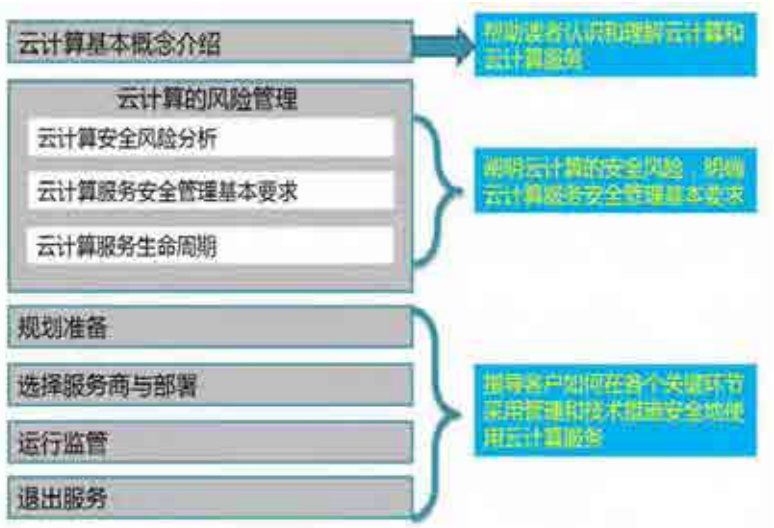

图 7 云计算服务安全指南标准框架

4.3.2 云计算服务安全能力要求

GB/T 31168-2014《信息安全技术 云计算服务安全能力要求》，**对为党政部门提供云服务的服务商提出了以下十个方面的要求：**

a) 系统开发与供应链。要求服务商主要供应链企业（包括软、硬件提供商，系统开发商、系统集成商等）、主要人员（开发人员、运维人员、管理人员、采购人员等）符合安全可控的要求。
b) 系统与通信保护。要求服务商网络、业务系统、虚拟化平台等满足信息安全技术要求，无不安全的访问接口、系统漏洞等。
c) 访问控制。要求服务商服务体系中的各类角色（包括管理员、维护人员、用户等）均有完善的鉴权机制和管理机制。
d) 配置管理。要求服务平台关键软硬件设备的配置管理受控、可靠。
e) 维护。要求政务云平台所有系统维护过程、工具、人员受控、可靠。
f) 应急响应与灾备。要求政务云具备完善的，符合系统要求的灾备系统，并有完善的应急响应制度与演练机制。
g) 审计。要求政务云系统具备可审计性，具有完善的日志管理、告警管理等能力。
h) 风险评估与持续监控。要求政务云服务提供商进行充分的系统脆弱性评估、漏洞扫描，并开展制度性的持续监控。
i) 安全组织与人员。要求政务云服务提供商具有完善的人员管理制度、培训制度。
j) 物理与环境安全。要求政务云机房物理环境安全可靠，安保系统完善。

4.4 政务行业网络安全一般性要求

目前，政务云建设存在多种方式，其中依托政务外网建设政务云为各地政府的首选方式。国家也配套发布了政务外网网络安全系列标准规范，给出了政务系统安全域划分的最佳实践。因此，本标准主要参照政务外网相关要求编制，选用其它方式建设的政务云，在安全建设方面可作为参考。

国家电子政务外网是按照中办发〔2002〕17 号文件和〔2006〕18 号文件要求建设的我国电子政务重要公共基础设施，是服务于各级党委、人大、政府、政协、法院和检察院等政务部门，满足其经济调节、市场监管、社会管理和公共服务等方面需要的政务公用网络。政务外网支持跨地区、跨部门的业务应用、信息共享和业务协同，以及不需在政务内网上运行

的业务。政务外网由中央政务外网和地方政务外网组成，与互联网逻辑隔离。政务外网由广域骨干网和城域网组成，纵向分为中央、省、市、县四级。各级政务部门根据业务需要分别接入相应层级的政务外网。

国家电子政务外网网络安全方面主要参照《国家电子政务外网安全等级保护基本要求》、《国家电子政务外网安全等级保护实施指南》、《国家电子政务外网跨网数据安全交换技术要求与实施指南》、《国家电子政务外网安全接入平台技术规范》等系列标准规范执行。

《国家电子政务外网安全等级保护实施指南》规定了国家电子政务外网安全等级保护在实施过程中，为达到国家标准规定和政务外网的基本要求而提出的安全等级保护的方法和手段，适用于指导各级政务外网的安全等级保护工作在定级、整改、报备、检查、测评和运维等实施过程中参考；各级在新建政务外网时可参照该指南开展安全等级保护工作；也可作为政务外网外包服务时对第三方提出安全保障要求的依据。

《国家电子政务外网安全等级保护基本要求》规定了国家电子政务外网不同安全保护等级网络的基本技术保护要求，适用于指导政务外网的网络安全等级保护建设、整改、自查和测评工作，可作为等级保护和信息安全主管部门对政务外网的网络安全进行检查和指导时的依据，也可作为外包服务时技术要求的依据。该要求只涉及政务外网网络安全等级保护的基本技术要求，有关物理环境、主机/服务器、应用、数据、和管理安全等共性要求，按照国家标准执行。

4.4.1 政务云安全域划分

政务云按所承载业务的不同划分为不同的区域，至少应划分面向互联网的门户网站和相关信息系统区域，部门自身的业务系统区域和跨部门共享的信息系统区域，各区域之间应采用 VPC 等技术进行隔离。区域内部信息系统按不同的安全要求确定安全等级并按相应要求保护，并做好虚拟机之间的访问控制策略，跨区域数据的访问或数据同步应有相关的控制手段。

政务云平台一般需按照网络安全等级保护第三级标准进行建设，各租户业务系统根据自身信息系统的安全要求确定信息系统等级并按要求实施不同安全级别的保护。

在“互联网业务区”和“部门业务区”中，租户可依据信息系统自身重要程度，按国家相关等级保护的标准，划分为二级等级保护系统和三级等级保护系统，并按相应等级进行防护。

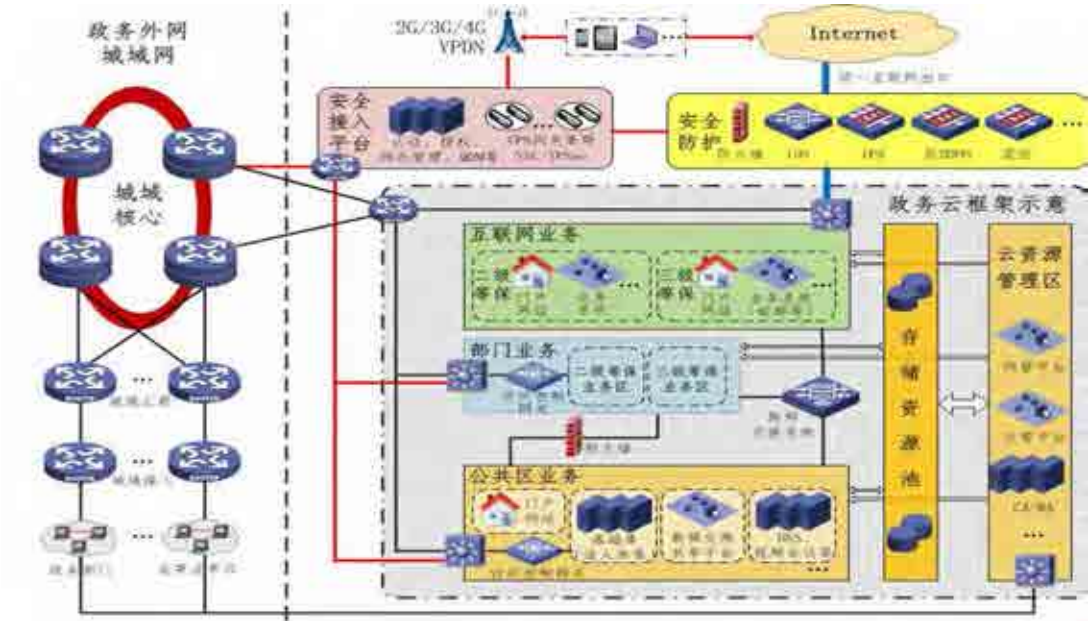

图 8 政务云安全域划分

a) 部门业务区

在政务上云前，电子政务外网中各级政务部门通过自建网络，由专线的方式接入国家电子政务外网城域网，这部分自建网络被称为局域网。

随着政务云的发展建设，各级政务部门需要把原有局域网中的业务迁移到政务云中，由运营单位在政务云中为各级政务部门提供一个逻辑隔离的区域，搭建一个安全可靠、可自主定义的环境。在该区域中部署独立的服务资源，并根据业务需求定义虚拟环境，包括定义网络拓扑、创建子网、虚拟机存储资源和划分安全组等。这个在政务云中为各级政务部门划分的独立区域被称为各级政务部门的 VPC，行使在传统政务外网中局域网的职能。在政务云中专门承载各级政务部门 VPC 的区域在本标准中被称为部门业务区。

部门业务区各政务应用系统应按国家网络安全等级保护相关标准及主管部门的要求进行定级、报备、测评、整改，并接受相关部门的检查。

b) 互联网区

互联网区是政务云为政务部门通过逻辑隔离安全接入互联网的网络区域，满足政务部门利用互联网开展公共服务、社会管理、经济调节和市场监管的电子政务业务需要。

c) 公共网络区

公共网络区是各部门、各地区互联互通的网络区域，为政务部门公共服务及开展跨部门、跨地区的业务应用、协同和数据共享提供支撑平台。此外该区域还提供政务外网的公共网络服务，如政务外网门户网站、DNS 服务等。要求互联网用户不能直接访问这个区域的数据和信息系统。

d) 安全接入平台

是政务云外部网络访问政务云内部部门业务和公共区业务的统一认证接入平台区域，区域内部署认证授权系统、VPN 接入网关、移动设备管理系统等，为各类智能移动终端和远程办公用户提供可信的安全接入和业务访问。

e) 管理区

根据网络业务及安全自身的需要，将网络管理系统、安全管理系统、电子认证服务等信息系统部署在管理区，并设置与之相适应的访问控制策略。安全等级保护确定为第三级的政务云，应建立安全管理系统（SOC），对安全防护设备的日志进行采集和综合关联分析，提出安全整改建议。对于安全事件和网络攻击等应能实时告警，有条件的相关设备应能联动，防止网络攻击等事件的进一步扩大，积极有效地保护政务云的安全。

4.4.2 部门业务区要求

部门业务区主要承载各政务部门部署或迁移的业务系统，各政务部门之间采用 VPC 隔离。应根据业务系统的安全等级进行防护。可按政务部门对信息系统的安全要求分为二级信息系统等级保护区域和三级信息系统等级保护区域，若租户同时拥有二级业务和三级业务，应确保不同等级的业务系统分属不同的资源和访问控制策略。

为保证政务云上数据的安全，互联网业务区如有数据需要与部门业务区和公共业务区数据进行交换时，应严格控制和管理。其政务内部的部门业务区之间和公共业务区之间可通过防火墙进行隔离，并通过访问控制策略等技术手段实现跨部门的数据共享与交换。

另外，对于接入政务云的各委办局单位局域网，其安全建设要防止终端“一机多用”，避免委办局终端同时可以访问互联网和电子政务外网，并保障委办局与电子政务应用系统之间相应的边界隔离手段。

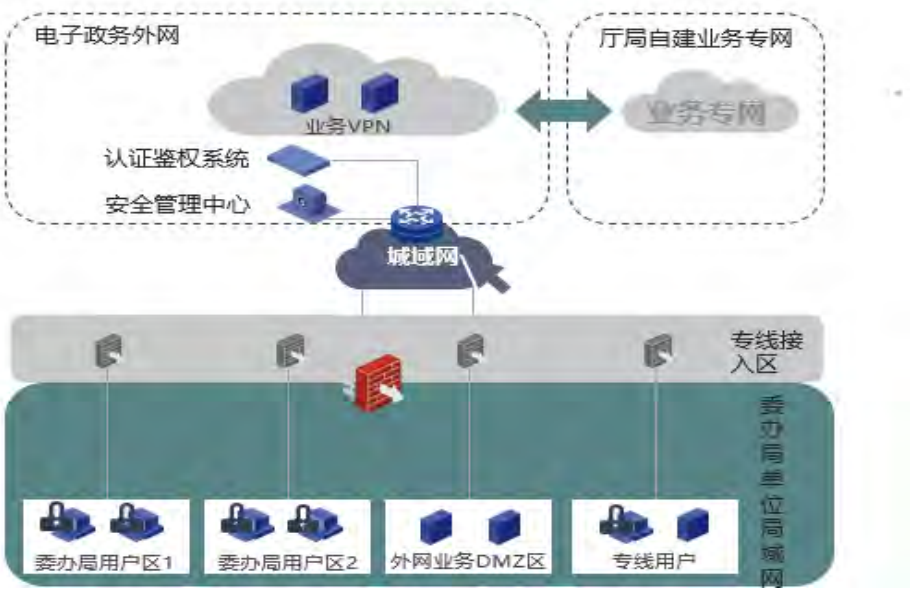

图 9 政务外网局域网安全示意图

局域网内的终端如既能访问政务外网的业务、又能访问互联网，各政务部门可根据自身业务的重要性，采取技术措施，逐步达到控制该终端访问互联网，其现有的技术手段如下，但不仅限于此：

a) 通过接入互联网侧的防火墙的访问控制策略对该终端访问互联网加以必要的限制；
b) 通过对终端硬盘分区，加密保存业务数据或相关工作文档，通过安全软件，当进行工作文档编写、数据处理时，自动断开该终端的互联网连接；
c) 通过插入 USBKey 时自动断开该终端的互联网连接，只能访问指定的政务外网服务器和应用系统；
d) 可采用虚拟终端等的技术，保证同一台终端不能同时访问政务外网业务和互联网业务。

4.4.3 互联网区要求

政务外网互联网出口的安全是重中之重，应保证互联网出口具有两个及以上的运营商出口，且能够做到链路负载均衡；出口应具备足够的防攻击手段；互联网数据中心应具备数据中心级的安全能力。总体而言，互联网出口应具有基于恶意行为攻击实时监控和安全态势感知能力。

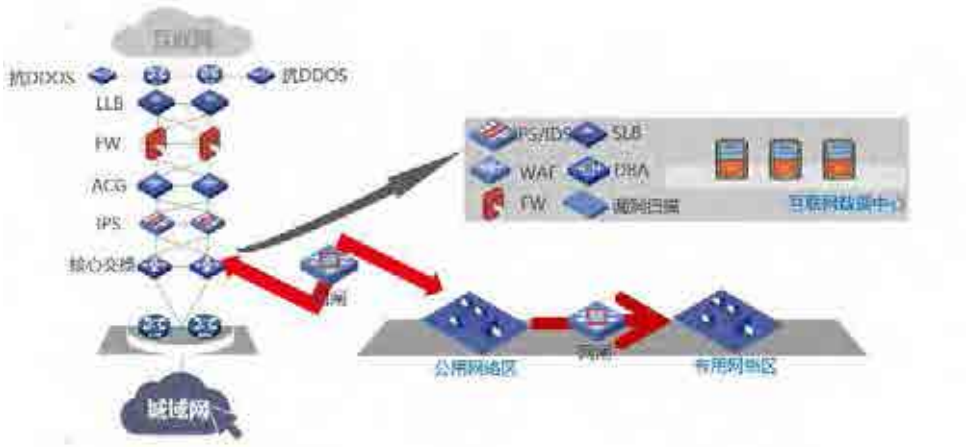

图 10 政务外网互联网出口安全示意图

根据《国家电子政务外网安全等级保护基本要求》中对互联网区安全的要求，重点需要关注：

a) 应选用二个及以上电信运营商或互联网业务提供商（ISP）作为访问互联网的出口；
b) 在采用主备方式或负载均衡等方式时，不同链路的安全策略应该保持一致；
c) 应能有效防止以下攻击行为：病毒攻击、端口扫描、木马后门攻击、拒绝服务攻击、缓冲区溢出攻击、IP 碎片攻击、SQL 注入、跨站攻击和网络蠕虫攻击等；
d) 应具备流量分析控制、异常告警等功能，能区分各类 HTTP、FTP、TELNET、SMTP、POP3、P2P 等网络协议并进行过滤；
e) 应具备监测检测恶意代码并实时告警的功能，在有条件的情况下，应能与防火墙、入侵检测等安全防护设备联动，有效阻止敏感信息的泄漏；
f) 通过互联网等公众通信网接入政务外网的各类移动业务，应尽量与政务部门访问互联网的出口业务分开，做好相应的访问控制。

4.4.4 公用网络区要求

政务外网公用网络区与互联网区信息交换必须通过跨网数据交换平台进行，跨网数据交换平台通过协议转换，以信息摆渡的方式实现双向数据传输，从而达到互联网区与公用网络区的强逻辑隔离；另外公共网络区承载着电子政务行业重要的业务系统：如共享数据交换平台、公共资源交易平台等，还应加强公共网络区数据中心安全建设。

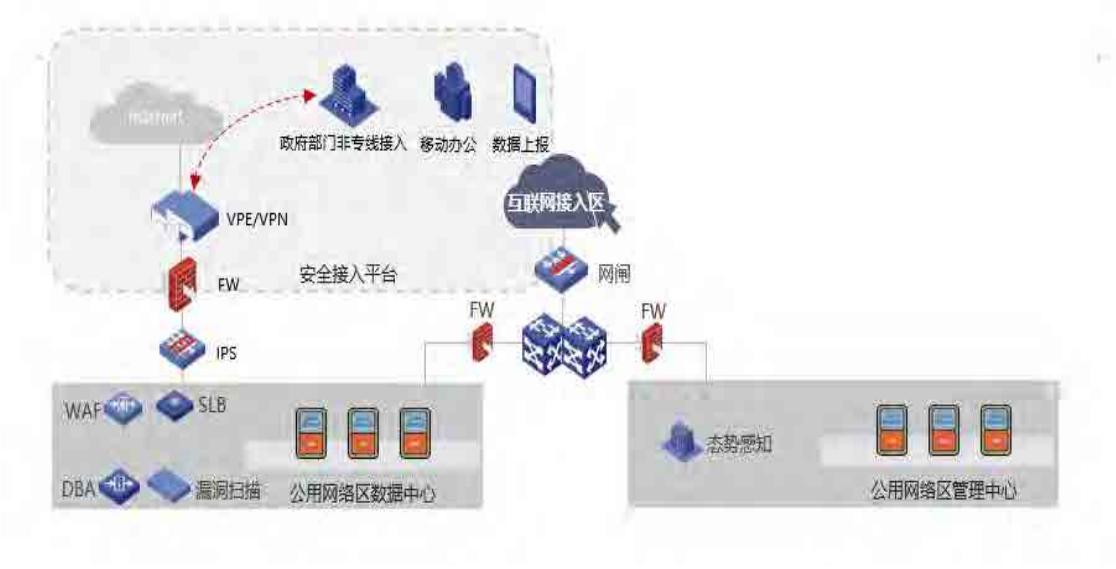

图 11 政务外网公用网络区安全示意图

根据《国家电子政务外网安全等级保护基本要求》和《国家电子政务外网跨网数据安全交换技术要求与实施指南》中的要求，重点需要关注：

a) 单向数据传输采用单向光闸或网闸作为唯一连接通道，通过协议转换，以信息摆渡的方式实现单向数据交换，同时必须确保数据无反向传输；
b) 双向数据传输采用网闸作为唯一连接通道，通过协议转换，以信息摆渡的方式实现双向数据交换；
c) 公用网络区的主要网络设备应具备设备冗余、链路冗余等级保护措施，应满足各类业务带宽、稳定性、可靠性和安全性的要求。
d) 通过互联网或其他公众通信网络对公用网络区的信息系统进行远程访问时，须采用 VPN 网关、信道加密，以及数字证书、IP 地址绑定、审计等安全措施；

e) 公用网络区与互联网接入区采用 MPLS VPN 进行逻辑隔离，二个区域的数据和系统不能直接访问；

f) 当公用网络区的主机/服务器需要从互联网接入区获取数据时，应采用安全隔离设备、防火墙、路由策略、身份认证、设备认证、审计等安全措施。

4.4.5 安全接入平台要求

安全接入平台应由 IPSec VPN 网关、SSL VPN 服务网关、基于 LDAP 或 RADIUS 的认证服务器、VPN 管理服务器等诸多安全软、硬件共同构建而成。

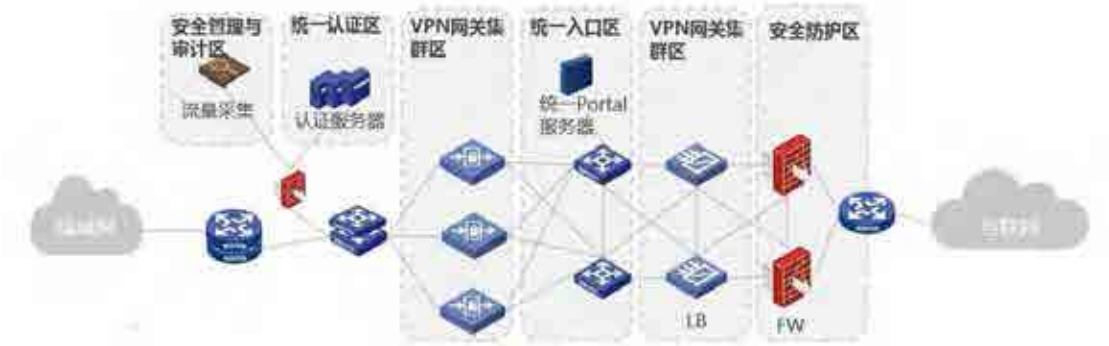

图 12 安全接入平台安全示意图

根据《国家电子政务外网安全接入平台技术规范》中对安全接入平台安全的要求，重点需要关注点如下图：

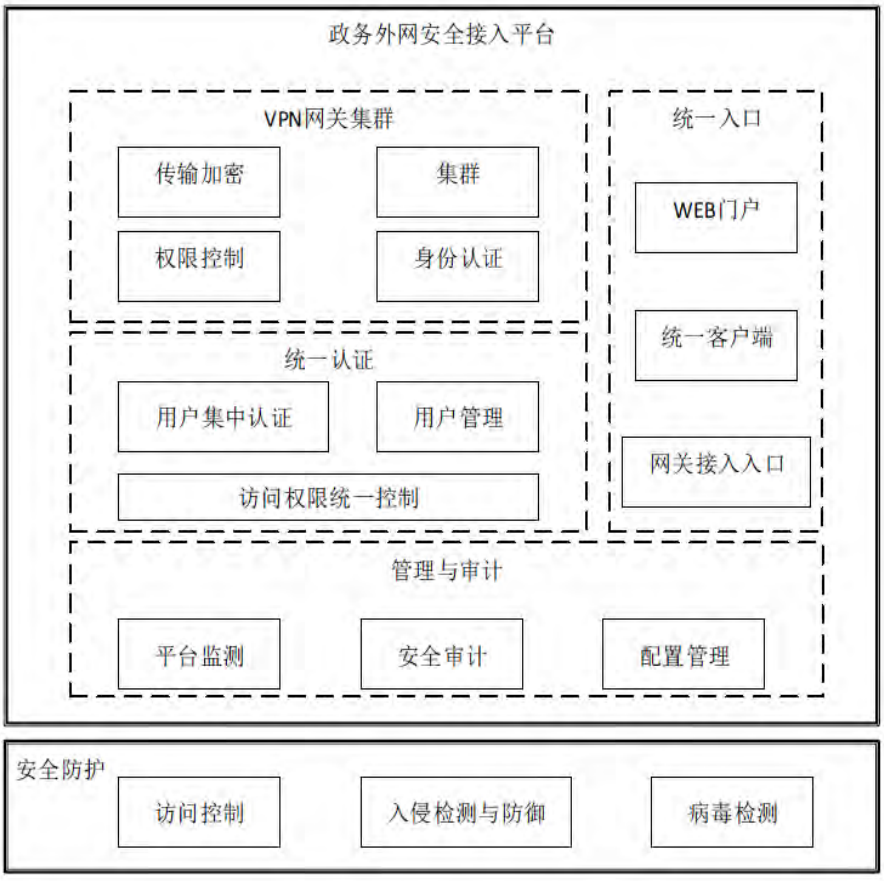

图 13 安全接入平台框架

4.4.6 管理区要求

根据网络业务及安全自身的需要，将网络管理系统、安全管理系统、电子认证服务等信息系统部署在管理区，并设置与之相适应的访问控制策略。**安全等级保护确定为第三级的政务外网，应建立网络安全态势感知系统**，对安全防护设备的日志进行采集和综合关联分析，提出安全整改建议，对于安全事件和网络攻击等应能实时告警，应能联动，防止网络攻击等事件的进一步扩大，积极有效地保护政务外网的安全，同时**能依据等级保护检查模板对全网的技术部分和管理部分进行等级保护合规核查**，并实现全网智能运维。

根据《国家电子政务外网安全等级保护基本要求》中对管理区安全的要求，重点需要关注：

a) 根据网络结构、管理分界，原则上采用国家、省二级或国家、省、地（市）三级分域分级的管理方式，根据实际需要设置分级权限，实现对网络的灵活管理；
b) 应绘制与当前运行情况相符的网络拓扑结构图、有相应的网络配置表，包含设备 IP 地址等主要信息，并及时更新、妥善保管并做好备份，且不得对外公开；
c) 网管网络应与电子政务业务网络逻辑隔离，确保网管数据的安全；
d) 对重要主机/服务器的运行状况（如 CPU 利用率、内存使用情况等）进行监测；
e) 网络管理系统应对同一管理员采用两种或两种以上组合的鉴别技术进行身份鉴别；
f) 安全管理系统（或平台）可与安全防护设备、网关、审计系统等，作为一个信息系统的整体，按信息系统安全等级保护的要求实施保护；
g) 应按日、周、月、季、年或按管理部门的要求出具安全运行报告，并对相关病毒攻击、信息安全事件提出建议；
h) 对网络及管辖区域内安全风险提出预警、对安全运行情况及态势进行分析等；
i) 应具备异构安全管理系统的互联功能，实现相关管理数据的共享、分析，为全网的安全事件应急响应、安全事件预警提供技术支撑。

4.4.7 电子认证的要求

《国家电子政务外网安全等级保护基本要求》、《国家电子政务外网电子认证管理办法》对数据加密传输存储、数据完整性校验、网络安全接入、用户身份鉴别等方面提出了相应要求，建议政务云在建设时需要**采用电子政务外网认证基础设施及相应密码技术，为政务云的数据加密传输存储、数据完整性校验、网络安全接入、用户身份鉴别提供服务。**对应到等级保护具体要求中，主要体现在以下条款上：

a) 安全计算环境
    1) 采用加密技术提供或支持云租户数据安全落地，确保云租户的数据在云计算平台以密文形式存储；
    2) 提供或支持云租户部署密钥管理解决方案，确保仅云租户能对其数据进行解密；
    3) 采用加解密技术保证网络策略控制器和网络设备（或设备代理）之间网络通信的保密性；
    4) 实现对于租户数据的安全保护，通过身份认证方式确保云服务方或第三方在云租户授权下，才可以对云租户数据库资源进行访问、使用和管理；
    5) 实现对于在网络策略控制器和网络设备（或设备代理）之间建立强身份验证和鉴别机制；
    6) 采用数字签名方式提供虚拟机镜像、快照完整性校验功能，防止虚拟机镜像被恶意篡改；
    7) 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) 安全区域边界

1) 实现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；
2) 实现云计算平台中各网络区域边界的访问控制，实现基于强身份认证的可控访问规则。

4.4.8 安全监测的要求

第三级及以上政务云应在境内实施技术维护，不得境外远程技术维护。因业务需要，确需进行境外远程技术维护的，应当进行网络安全评估，并采取风险管控措施。实施技术维护，应当记录并留存技术维护日志，并在公安机关检查时如实提供。

地市级以上云计算服务提供部门，应建立网络安全监测预警和信息通报制度，对其负责的政务云应开展安全监测、态势感知、通报预警等工作。

第三级及以上政务云服务提供部门，也应建立健全网络安全监测预警和信息通报制度，按照规定向同级公安机关报送网络安全监测预警信息，报告网络安全事件。有行业主管部门的，同时向行业主管部门报送和报告。

行业主管部门应当建立健全本行业、本领域的网络安全监测预警和信息通报制度，按照规定向同级网信部门、公安机关报送网络安全监测预警信息，报告网络安全事件。

a) 监测体系的建立

政务云基础设施运营者应：

1) 根据国家行业主管或监管部门政务云网络安全监测预警制度的要求，按照国家网络安全事件应急预案等规定，建立并完善本组织监测预警制度，提高监测能力，自主监测涉及本组织管理范围内的信息。
2) 确定监测对象、监测指标、监测频率，监测对象包括系统运行状态、网络、人员行为、物理环境和策略运行效果等。
3) 监测政务云基础设施运行、操作、故障维护等行为，并留存相关日志，尤其要对远程运维的行为进行严格的管理、控制和审计，相关的系统、网络设备日志留存不少于 12 个月。日志内容应至少包括：事件的日期和时间、类型、主体、客体、结果等信息。
4) 定期对监测情况进行安全评估，向相关人员或角色报告政务云基础设施安全状态。

b) 预警通报制度的建立

政务云基础设施运营者应以适当的方式参与本行业、本领域的政务云基础设施网络安全监测预警和信息通报制度，持续接收行业主管或监管部门发布的安全风险、预警信息和应急防范措施建议。

政务云基础设施运营者应：

1) 对监测信息进行研判，必要时发出内部的安全预警信息并提出适当的处置建议。
2) 根据本组织信息通报制度要求，向相关人员、角色和部门通报安全预警信息和建议。
3) 及时响应安全预警信息和建议，如无法响应应说明原因。

政务云基础设施运营者应根据政务云基础设施网络安全信息通报制度的要求，按照国家网络安全事件应急预案等规定，制定并完善本组织信息通报制度，包括：

1) 明确负责信息通报工作的主管领导和承担信息通报工作的责任部门、负责人和联络人。
2) 及时汇总本组织内部不同部门、不同渠道掌握的网络安全信息。
3) 明确本组织信息报送项目。

4) 规范报送信息内容和形式，信息包括事件信息和预警信息，其中：
事件信息指已经发生的网络安全事件信息，事件信息通报内容主要包括事件统计情况、造成的危害、影响程度、态势分析、典型案例等。
预警信息是指存在潜在安全威胁或隐患但尚未造成实际危害和影响的信息，或者对事件信息分析后得出的预防性信息，预警信息通报内容主要包括事件类别、预警级别、可能的受影响系统、可能产生的危害和危害程度、可能影响的范围、建议应采取的应对措施及建议等。

5) 明确具体分级标准，将预警信息分为四级，分别对应发生或可能发生特别重大、重大、较大和一般网络安全事件。

c) 信息共享制度的建立

政务云基础设施运营者应:

1) 按照政务云基础设施安全保护工作部门要求，建立与有关部门、研究机构、网络安全服务机构的信息共享渠道，接收行业主管或监管部门发布的安全风险、预警信息和应急防范措施建议。
2) 建立本组织的安全监测信息共享和分析中心，收集网络威胁迹象信息或防护措施并进行分析，必要时与行业网络安全威胁信息共享平台进行对接。
3) 对共享或接收网络威胁迹象信息或防护措施进行授权。
4) 在监控信息系统、实施防护措施、提供或接收网络威胁迹象信息和防护措施时，应实施安全控制，以保护上述网络威胁迹象信息或防护措施免受未授权访问或获取。
5) 在信息共享前，使用技术手段直接删除与网络安全威胁无直接关系的、共享时已知晓是具体人员个人信息或能够用于识别具体人员的信息。
6) 限制信息使用目的，对威胁信息的披露、留存与使用仅用于网络安全保护目的。

4.4.9 其他要求

政务云是承载各级政务部门门户网站、政务业务应用系统和数据的云计算基础设施，用于政务部门公共服务、社会管理、跨部门业务协同、数据共享和应急处置等政务应用。政务云对政府管理和服务职能进行精简、优化、整合，并通过信息化手段在政务上实现各种业务流程办理和职能服务。政务云的建设有利于减少各部门分散建设，提升信息化建设质量，提高资源利用率和减少行政支出等优势。

政务云的服务对象是各级政务部门，通过政务外网或运营商专线连接到各单位，使用云计算环境上的计算、网络和存储资源，承载各类信息系统，开展电子政务活动。

政务云安全应具备以下内容：

a) 各类政务业务应部署在物理设施独立的政务云上，不得部署在公有云上；
b) 政务云计算基础设施应按信息系统等级保护国家标准中的第三级等级保护要求建设和保护；
c) 政务云上承载互联网门户网站及部署在互联网上的信息系统计算资源和网络资源，从云计算核心交换机以下,在物理上与其他 VPC 分开部署，根据系统预设的调度策略进行资源调度和迁移。对于已建的政务云，应对互联网 VPC 的业务实时监测、控制和管理，尤其是对跨 VPC 数据共享与交换访问控制的实时监控；
d) 所有对各类资源的操作必须通过云资源管理区，并对管理员操作进行审计。要求业务流量与管理流量分开，应能区分运维管理人员、云服务客户管理员及公务人员访问业务和对各类资源的管理和控制；
e) 云服务方应提供对各信息系统的核心或敏感数据加密存储的功能，应按照国家密码

管理有关规定使用和管理政务云平台的密钥设施，并按规定生成、使用和管理密钥；

f) 应对云服务客户管理员账户及政务云的管理数据单独加密存储，重点保护。其密钥的使用和管理应符合国家密码管理局的有关规定；

g) 重要部门的信息系统在分地域部署云计算基础设施时，可将计算、网络和存储设施采用分布式部署方式部署在远端并进行统一管理；

h) 明确远程管理责任，云服务方需要对计算资源进行远程管理时，云管理单位有权对所有远程维护和诊断活动进行审计，按照对所有远程维护和诊断会话的记录进行审查；

i) 云计算环境应具备基于行为的持续监控、策略控制、事件预警、态势感知及安全事件及时处置的能力；

j) 云服务方应定期向政务云管理单位提交各云服务客户安全情况及资源使用率情况；

k) 对重点云服务客户的信息系统和数据应能重点进行安全保障，持续监控异常情况并预警；

l) 政务云应具备分级管理和控制的能力，VPC 内部信息系统之间的访问控制及数据使用等管理权限应开放给云服务客户，云服务方应具备对资源使用情况实时监测、发现异常、预警和协助处置的能力；

m) 所有上云前的应用系统应进行测试、其应用系统源代码的定制化部分应向政务云管理单位备案；

n) 云服务客户拥有本单位 VPC 内部信息系统和数据完整的使用权和管理权。

5 政务云安全合规工作指南

目前，政务云的网络安全合规性工作主要集中在三个方面：

a) 公安部门组织的等级保护工作；

b) 中央网信办组织的党政部门云计算服务网络安全审查工作；

c) 国家政务外网管理部门组织的安全检查工作。

本文主要以等级保护工作为核心，通过等级保护建设，使政务云能够同时满足上述三个方面的要求。

5.1 准备阶段

5.1.1 调研

云计算服务提供部门在调研阶段需要明确政务云建设的规模、业务范围，对迁移上云的业务类型、业务重要性程度、现有网络基础设施等进行调研。针对数据中心的网络结构的分层分区规划、架构的可靠性、架构的灵活性、架构的可管理性以及架构的技术支撑能力进行差距性分析及评估。同时结合行业及技术的最佳实践经验，对业务网络系统中重要的网络安全规划、部署、配置参数的合理性进行评估，在该阶段主要需要完成以下内容的调研准备：项目参与和配合人员名单、信息系统承载业务情况、联接线路及网络端口（网络边界）情况、网络设备情况、安全设备情况、终端设备情况、服务器设备情况、应用系统软件情况、业务数据及备份情况、管理文档、记录类文档、安全威胁情况等。

云计算服务提供部门在调研阶段同时需要关注云计算服务安全审查要求，在调研阶段完成以下内容的确认：

a) **服务模式确认。**云端有 SaaS、PaaS、IaaS 三种主要服务模式，不同服务模式下云计算服务提供部门与客户的控制范围不同。

b) **部署模式确认。**云计算有公有云、社区云和私有云三种典型部署模式，不同的部署模式下云计算基础设施部署的场所客户访问云计算服务的网络链路、是否与其他客户共享资源等属性有较大差异，客户需要综合分析部署模式对自身数据和业务的影响。

c) **功能需求的稳定性和通用性确认。**当客户的业务功能需求不断变化时，云计算服务提供部门需要不断开发、测试和部署新的组件。通用的功能需求有助于客户参考成熟的应用案例。应优先将功能需求不经常发生变化的业务部署或迁移到云计算平台。

d) **资源的动态需求特点确认。**有些业务具有临时、周期性特点，如公务员招考等业务系统，可能会出现访问和请求的突发高峰，要求可根据访问需求动态分配资源。

e) **时延确认。**时延是指云计算环境处理某个请求的是时间延迟，包括客户请求消息传输到云计算环境和结果回传时间，以及云计算环境的处理时间。

f) **业务持续性确认。**云计算服务是否会中断、是否能持续访问依赖于多方面因素，包括网络、云计算平台以及云计算服务提供部门等。应对云计算服务的可靠性、持续性需求进行充分评估，应关注中断频率与预期恢复时间。

g) **可移植性与互操作性确认。**移植是指将数据和业务系统从一个云服务商迁移到另一个云服务商的云计算平台，互操作性是指部署在云计算平台上的业务系统与其他系统进行数据交互。

h) **数据的存储位置确认。**根据国家的有关规定，存储、处理客户数据的数据中心和云计算基础设施不得设在境外，客户在确定采用云计算服务时，应禁止云服务商在境外存储、处理客户数据，不得由于客户数据存储位置的改变而改变其司法管辖权。

i) **监管能力确认。**传统计算模式中，用户直接控制、管理自己的数据和业务系统。在云计算平台中，客户的数据及运行过程中生成、获取的数据都在云服务商的直接控制下，客户没有直接的控制权。客户需要通过监管了解和掌握自身数据和业务系统在云计算平台上的状态，了解云计算平台是否提供了足够的安全防护措施满足安全需求。

5.1.2 定级

根据调研结果对政务云平台及云上业务系统分别进行定级备案，定级工作的主要内容包括：确定定级对象、确定信息系统安全保护等级、组织专家评审、主管部门审批、公安机关审核。

政务外网开展等级保护工作重点是广域网和各级城域网。政务外网中央至省、省至地（市）广域网和中央、省级和地（市）级城域网应达到安全等级保护第三级要求，地(市)至区县广域网和地(市)以下城域网应至少达到安全等级保护第二级要求。

政务云原则上要求达到不低于等级保护第三级的建设要求。政务云的等级应高于其承载业务系统的等级，由于政务云上承载的各厅局委办的业务系统多种多样，建议政务云级别定级为 G3A3S3，以适应更广泛的业务系统。

政务外网承载的各级政务部门业务应用系统，应由所属单位或主要责任单位按国家相关要求和标准自主定级、备案，相应安全责任自行承担。

等级保护的三种指标类型：

S（业务信息安全）：保护数据在存储、传输、处理过程中不被泄漏、破坏和免受未授权修改的信息安全类要求；--物理访问控制、边界完整性检查、身份鉴别、通信完整性、保密性等；

A（系统服务保障）：保护系统连续正常的运行，免受对系统的未授权修改、破坏而导致系统不可用的服务保证类要求；--电力供应、资源控制、软件容错等；

G（通用要求）：通用安全保护类要求；--技术类中的安全审计、管理制度等。

表 3 等级保护对象定级结果组合

安全保护等级	定级结果的组合
第一级	S1A1
第二级	S1A2,S2A2,S2A1
第三级	S1A3，S2A3，S3A3，S3A2，S3A1
第四级	S1A4，S2A4，S3A4，S4A4，S4A3，S4A2，S4A1
第五级	S1A5，S2A5，S3A5，S4A5，S5A4，S5A3，S5A2，S5A1

注：本文档按照网络安全等级 G3S3A3 编写。

5.1.3 规划及可行性研究

根据调研结果，进行云平台等级保护建设的可行性研究。**在等级保护的建设中需要关注“一个中心三重防护”的可行性研究，**“一个中心”：安全管理中心，对平台是否可以进行统一监控与审计进行可行性研究；“三重防护”：安全计算环境，安全通信网络和安全区域边界；其中安全计算环境需要关注主机安全加固、身份鉴别、数据库审计、权限管理、主机防病毒、应用系统安全、主机安全审计、资源控制、剩余信息保护、数据备份与恢复和抗抵赖技术；安全通信网络需要关注通信完整性和保密性，流量管理控制等；安全区域边界需要关注边界隔离、边界访问控制、边界入侵防范、边界恶意代码过滤、边界完整性保护、边界安全审计。另外，云平台安全建设还应包含网络安全等级保护中，云平台面向云上业务系统的安全扩展能力要求。

云计算服务安全审查需要关注以下10类安全要求的可行性研究：系统开发与供应链安全、系统与通信保护、访问控制、配置管理、维护、应急响应与灾备、审计、风险评估与持续监控、安全组织与人员、物理与环境保护。

在政务行业网络安全一般性要求方面，重点关注对电子政务外网的用户局域网、公用网络区、互联网接入区、专用网络区、网络管理区、安全管理区、电子认证区的相关要求及现状的调研。

5.1.4 评审

云计算服务提供部门应组织专家，对规划及可行性研究报告进行专家评审并形成会议纪要。评审内容包含且不限于：等级保护、云计算服务安全审查、政务行业网络安全一般性要求等内容。

5.2 实施阶段

5.2.1 采购

云计算服务提供部门对拟采用的云计算平台，进行自建或采购第三方云计算服务项目，达到一定规模的一般采用招标的方式。

云计算服务运营者应当采购、使用符合国家法律法规和有关标准规范要求的网络产品和服务。

第三级以上网络运营者应当采用与其安全保护等级相适应的网络产品和服务；对重要部位使用的网络产品，应当委托专业测评机构进行专项测试，根据测试结果选择符合要求的网络产品；采购网络产品和服务，可能影响国家安全的，应当通过中央网信部门会同国务院有关部门组织的安全审查。

5.2.2 方案设计

方案编制前需要开展安全现状评估工作，以确定目前定级对象安全保护的程度或水平与国家网络安全等级保护要求之间的差距，对定级对象安全方面的调整和改进提出建议。

安全现状评估工作应依据等级保护的相关技术标准，并结合定级对象的具体安全需求实施现状评估。评估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，以及制度、机构、人员、建设、运维管理等网络安全的各个方面。

应根据现状评估结果，制定和评估实施方案，并对方案进行评审与完善。

a) 安全物理环境

物理环境安全应从以下方面进行安全设计：物理位置选择、物理访问控制、防盗窃和放破坏、防雷击、防火、防水和防潮、防静电、温湿度控制、电力供应、电磁防护。

b) 安全通信网络

通信网络安全应从以下方面进行设计：网络架构、通信传输等。

c) 安全区域边界

区域边界安全应从以下方面进行设计：边界防护、访问控制、入侵防范、恶意代码和垃圾邮件防范、安全审计等。

d) 安全计算环境

计算环境安全应从以下方面进行安全设计：身份鉴别、访问控制、安全审计、入侵防范、恶意代码防范、数据完整性、数据保密性、数据备份与恢复、剩余信息保护、个人信息保护、镜像和快照保护等。

e) 安全管理中心

安全管理中心应从以下方面进行安全设计：系统管理、审计管理、安全管理、集中管控

等。

f) 安全管理体系设计

安全管理体系要从安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理五个维度进行设计。在设计时应考虑以下要点：

1） 安全策略、管理制度、制度的制定和发布、制度的评审和修订；
2） 岗位设置、人员配备、授权和审批、沟通和合作、审核和检查；
3） 人员的录用、人员的离岗、安全意识教育和培训、外部人员管理；
4） 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；
5） 服务供应商选择、云服务商选择；
6） 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、云计算环境管理等。

方案的编写还需要参照云计算服务安全能力审查的 10 类安全要求：系统开发与供应链安全、系统与通信保护、访问控制、配置管理、维护、应急响应与灾备、审计、风险评估与持续监控、安全组织与人员、物理与环境保护。

同时需要参考《国家电子政务外网安全等级保护基本要求》，包括：电子政务外网的用户局域网、公用网络区、互联网接入区、专用网络区、网络管理区、安全管理区、电子认证区等相关安全要求。

5.2.3 方案评审

云计算服务提供部门应组织专家对设计方案进行专家评审并形成会议纪要。评审内容包含且不限于：等级保护、云计算服务安全审查、政务行业网络安全一般性要求等内容。

5.2.4 建设

根据等级保护安全总体方案明确主要的安全建设内容，并将其适当的分解，主要建设内容可能分解但不限于以下内容：云平台安全基础设施建设、云平台面向云上业务系统的安全扩展能力建设。其中云平台安全基础设施建设包含：网络安全建设、系统平台和应用平台安全建设、数据系统安全建设、安全标准体系建设、人才培养体系建设、安全管理体系建设等。

可分类组合安全建设内容为不同的安全建设项目，描述项目所解决的主要安全问题及所要达到的安全目标，对项目进行支持或依赖等相关性分析，对项目进行紧迫性分析，对项目进行实施难易程度分析，对项目进行预期效果分析，描述项目的具体工作内容、建设方案，形成安全建设项目列表。

在项目建设阶段需要保障：

a) **质量管理**，质量管理首先要控制系统建设的质量，保证系统建设始终处于等级保护制度所要求的框架内进行。同时，还要保证用于创建系统的过程的质量。在系统建设的过程中，要建立一个不断测试和改进质量的过程。在整个系统的生命周期中，通过测量、分析和修正活动，保证所完成目标和过程的质量。
b) **风险管理**，为了识别、评估和减低风险，以保证系统工程活动和全部技术工作项目都成功实施，在整个系统建设过程中，风险管理要贯穿始终。
c) **变更管理**，在系统建设的过程中，由于各种条件的变化，会导致变更的出现，每一次变更处理，必须遵循同样的程序，即相同的文字报告、相同的管理办法、相同的监控过程。必须确定每一次变更对系统成本、进度、风险和技术要求的影响。一旦批准变更，必须设定一个程序来执行变更。

d) **进度管理**，系统建设的实施必须要有一组明确的可交付成果，同时也要求有结束的日期。因此在建设系统的过程中，必须制订项目进度计划，绘制网络图，将系统分解为不同的子任务，并进行时间控制确保项目的如期完成。

e) **文档管理**，文档是记录项目整个过程的书面资料，在系统建设的过程中，针对每个环节都有大量的文档输出，文档管理设计系统建设的各个环节，主要包括：系统定级、规划设计、安全实施、系统验收、人员培训等方面。

5.3 验收阶段

验收阶段需要按照国家工程验收的相关标准规定执行，在政务云网络安全验收方面主要包括等级保护测评和安全培训。

5.3.1 等保测评

该阶段工作由具备等级保护测评资质的机构开展。在开展等级保护测评工作前，**云计算服务提供部门应携带“定级报告”、“定级评审专家意见”到当地公安网监部门对该政务云进行备案，获得备案号。测评机构在开展现场测评工作前，应该在公安部“等级测评项目登记管理系统 ”系统上注册通过。**

政务云的等级测评过程中，**测评机构将对系统的技术体系和管理体系，按照国家网络安全等级保护相关要求，进行全方位的安全测评。**其中，技术体系包含：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 5 个方面的安全测评。管理体系包含：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 5 个方面的安全测评。测评过程中，**云计算服务提供部门应协调相关人员予以配合。**

另外政务云测评工作的开展首先要明确测评对象是**云计算服务提供部门负责的云平台，还是使用云服务的政务部门负责的云上系统**，对于同一条测评实施内容，针对**云平台**与**云上系统**具有不同的含义，部分条款仅适用于**云平台**，而部分条款仅适用于**云上系统**。例如测评实施中：“应检查云服务商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”仅适用于**云平台**，而不适用于**云上系统**。

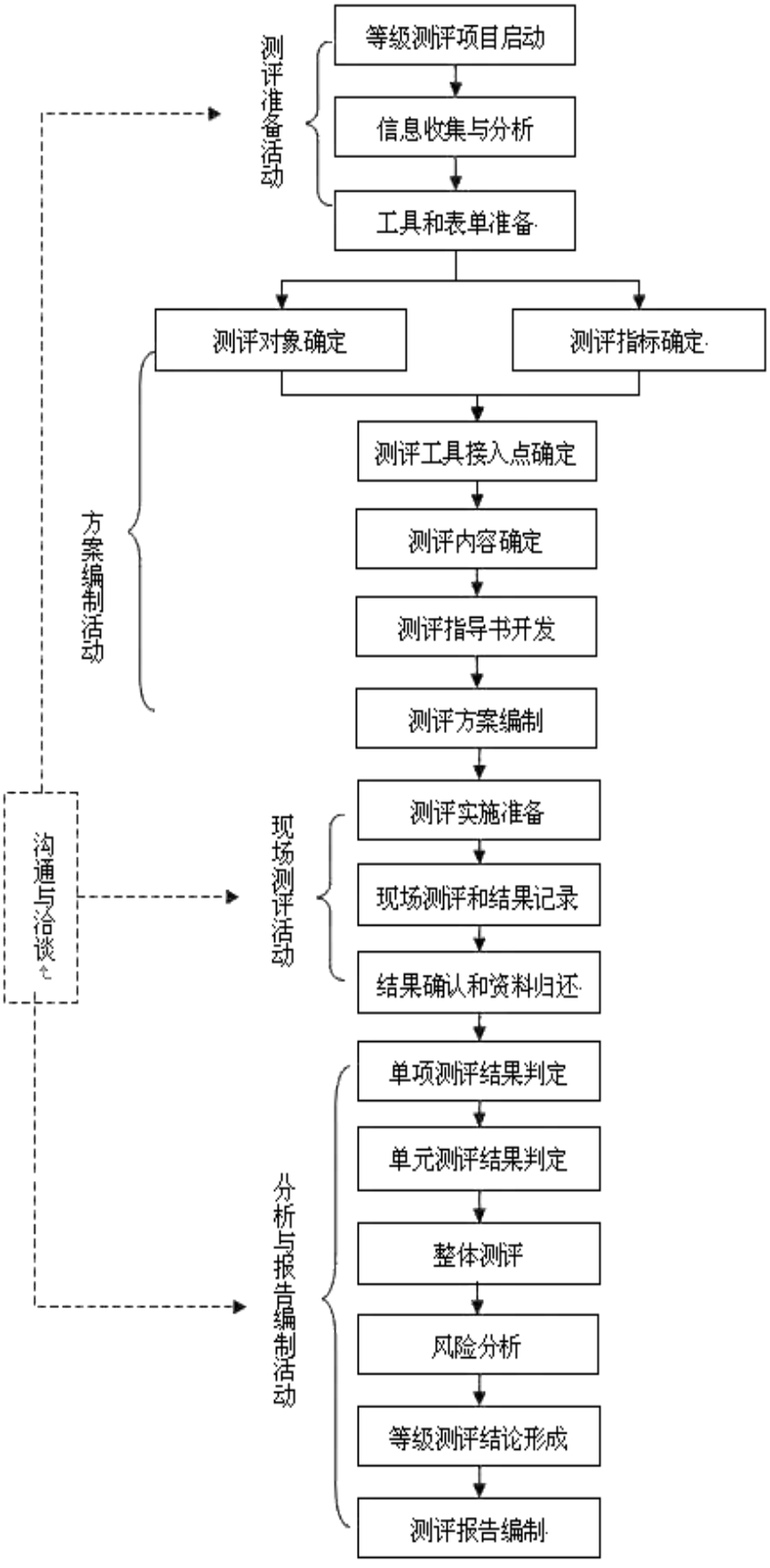

图 14 等级保护测评工作流程

现场测评活动完成后，测评机构将出具**《XXX 等级保护测评报告》。**报告的编制要具备以下基本内容：概述测评项目情况、描述被测系统情况、描述测评范围和方法、描述单元测评情况、描述整体测评情况、汇总测评结果等，在测评报告的开始需要描述本次测评的基本情况，如下表所示：

<table>
<tr><td colspan="6">信息系统</td></tr>
<tr><td>系统名称</td><td colspan="2"></td><td>安全保护等级</td><td colspan="2"></td></tr>
<tr><td>备案证明编号</td><td colspan="2"></td><td>测评结论</td><td colspan="2"></td></tr>
<tr><td colspan="6">被测单位</td></tr>
<tr><td>单位名称</td><td colspan="5"></td></tr>
<tr><td>单位地址</td><td colspan="3"></td><td>邮政编码</td><td></td></tr>
<tr><td rowspan="3">联 系 人</td><td>姓　　名</td><td colspan="2"></td><td>职务/职称</td><td></td></tr>
<tr><td>所属部门</td><td colspan="2"></td><td>办公电话</td><td></td></tr>
<tr><td>移动电话</td><td colspan="2"></td><td>电子邮件</td><td></td></tr>
<tr><td colspan="6">测评单位</td></tr>
<tr><td>单位名称</td><td colspan="2"></td><td>单位代码</td><td colspan="2"></td></tr>
<tr><td>通信地址</td><td colspan="3"></td><td>邮政编码</td><td></td></tr>
<tr><td rowspan="3">联 系 人</td><td>姓　　名</td><td colspan="2"></td><td>职务/职称</td><td></td></tr>
<tr><td>所属部门</td><td colspan="2"></td><td>办公电话</td><td></td></tr>
<tr><td>移动电话</td><td colspan="2"></td><td>电子邮件</td><td></td></tr>
<tr><td rowspan="3">审核批准</td><td>编 制 人</td><td colspan="2">（签名）</td><td>编制日期</td><td></td></tr>
<tr><td>审 核 人</td><td colspan="2">（签名）</td><td>审核日期</td><td></td></tr>
<tr><td>批 准 人</td><td colspan="2">（签名）</td><td>批准日期</td><td></td></tr>
</table>

5.3.2 安全培训

政务云项目中，应根据要求制订全面、详细的安全培训方案。培训分为集中培训、现场培训、一对一的培训等多种方式。教员不仅要有丰富的理论知识，也要有实际工作经验。针对实际情况确定培训人员、培训时间、地点，制订培训计划表，确认培训效果考核内容，并在培训前期准备培训相关手册，提供简明易懂的培训资料和讲义。**培训内容包括但不限于安全意识培训、安全防护培训、安全操作培训、安全运维培训等。**

5.4 运行阶段

5.4.1 云计算服务安全审查

中网办发文〔2014〕14号《**关于加强党政部门云计算服务网络安全管理的意见》**中指出：“中央网信办会同有关部门建立云计算服务安全审查机制，对为党政部门提供云计算服务的服务商，参照有关网络安全国家标准，组织第三方机构进行网络安全审查，重点审查云计算服务的安全性、可控性。**党政部门采购云计算服务时，应逐步通过采购文件或合同等手段，明确要求服务商应通过安全审查。**鼓励重点行业优先采购和使用通过安全审查的服务商提供的云计算服务。”

对于政务云来说，云计算服务提供部门承担着服务商的角色，应当按照上述意见要求，对其负责的政务云开展云计算服务安全审查工作。审查工作由中央网信办认可的第三方测评机构实施，审查工作参考的标准为《GB/T 31167-2014 信息安全技术 云计算服务安全指南》、《GB/T 31168-2014 信息安全技术 云计算服务安全能力要求》，**审查结束后，网络安全审查办公室将在其官网上公示通过安全审查的云计算服务。**

5.4.2 政务行业网络安全检查

各地政务云服务提供部门应按照政务行业网络安全的相关要求，积极开展政务外网、政府网站的自查工作。政务网络各接入单位应对接入的局域网、终端设备和服务器进行梳理，做好安全准入检查，及时发现和消除安全隐患，严禁各类私拉乱接行为，禁止各种非授权的网络代理行为和未经批准的无线接入方式；未通过安全准入检查的设备应暂时中断接入，待通过安全检查后方可接入政务网络。对政府网站进行安全扫描及渗透测试，发现问题及时整改并进行复测。

国家政务网络管理部门定期开展网络安全检查工作，按照政务行业网络安全相关要求，对云服务提供部门负责的政务云平台、政务部门负责的政府网站进行安全检查。云服务提供部门、政务部门应协调安排相应人员配合检查工作，对检查中发现的问题及时分析确定整改方案，按照要求完成整改，并将结果报给管理部门。

5.4.3 等保测评及监督检查

第三级信息系统应当每年至少进行一次等级测评，公安机关对第三级以上网络运营者每年至少开展一次安全检查。涉及相关行业的可以会同其行业主管部门开展安全检查。

在《网络安全等级保护条例》（征询意见稿）中要求单位每年进行一次自查，并向备案的公安机关报告，三级网络每年做测评可以看作是一次自查整改，对于二级网络来说，需要每年向公安机关提交一份自查报告，实际上是对二级网络要求进行了补充增强，但是以往四级系统是要求每半年测评一次，在新的保护条例中，第二十三条要求：第三级以上网络的运营者应当每年开展一次网络安全等级测评，发现并整改安全风险隐患，并每年将开展网络安全等级测评的工作情况及测评结果向备案的公安机关报告。

云计算服务提供部门应每年定期组织人员力量，联系测评机构进行网络安全等级保护测

评工作，以确保政务云安全防护能力能够持续达到相应等级安全保护能力要求。

5.4.4 安全监测

运行期间政务云基础设施运营者应做好如下安全监测工作：

a) 安全事件监测

1) 能够发现攻击行为，使用自动工具对攻击事件进行准实时分析。
2) 能够发现非授权的本地、网络和远程连接以及对信息系统的非授权使用；
3) 确保信息系统监测活动符合关于隐私保护的相关政策法规。
4) 以下迹象发生时，应向相关人员或角色发出警报：
受保护的信息系统文件或目录在未得到正常通知的情况下被修改；
当发生异常资源消耗时；
审计功能被禁止或修改，导致审计可见性降低；
审计或日志记录因不明原因被删除或修改；
预期之外的用户发起了资源或服务请求；
信息系统报告了管理员或关键服务账号的登录失败或口令变更情况；
进程或服务的运行方式与系统常规情况不符；
在生产系统上保存或安装与业务无关的程序、工具、脚本。

b) 云安全访问监测

1) 对信息系统设施进行物理访问监测，形成物理访问日志。
2) 定期或当安全事件发生时，对物理访问日志进行审查。
3) 安装物理入侵警报装置，对物理入侵警报装置和监测设备进行监视。
4) 对于集中部署了大量信息系统组件的区域（如服务器机房、通讯中心），除了对设施实施访问监测外，对信息系统实施单独的物理访问监测。

c) 数据泄露安全监测

1) 应对部署在政务云上的应用数据安全进行监测，及时发现涉及数据安全的相关信息，防止数据出现泄漏等安全事件。

d) 恶意代码安全监测

1) 采用白名单、黑名单或其他方式，在政务云平台上实施恶意代码防护机制。
2) 配置恶意代码防护机制，定期扫描信息系统，以及在终端或网络出入口下载、打开、执行外部文件时对其进行实时扫描。
3) 当检测到恶意代码后，阻断或隔离恶意代码、向管理员报警或采取其他举措。
4) 及时掌握系统的恶意代码误报率，并分析误报对信息系统可用性的潜在影响。
5) 在系统的出入口和网络中的工作站、服务器或移动计算设备上部署垃圾信息检测与防护机制，以检测并应对电子邮件、电子邮件附件、web 访问或其他渠道的垃圾信息。
6) 确保恶意代码和垃圾信息防护机制得到及时更新，如升级病毒库。