2017云栖大会·成都峰会
THE COMPUTING CONFERENCE
阿里云

云栖社区
yq.aliyun.com

阿里云
云上系统等保合规解决方案

主讲人：行逸

1.等级保护概述

2.云上等保合规方案

3.阿里云优势

基本概念

- 基本概念
  - ✓ 《信息安全等级保护管理办法》：国家通过制定统一的信息安全等级保护**管理规范和技术标准**，组织公民、法人和其他组织对信息系统**分等级实行安全保护**，对等级保护工作的实施进行**监督、管理**。
- 制度要求
  - ✓ **《中华人民共和国网络安全法》**：“国家实行**网络安全等级保护制度**。网络运营者应当按照网络安全等级保护制度的要求，履行下列安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改”。
  - ✓ 《国家信息化领导小组关于加强信息安全保障工作的意见》（中办发[2003]27号）规定：要重点保护基础信息网络和关系国家安全、经济命脉、社会稳定等方面的重要信息系统，抓紧建立信息安全等级保护制度。
- 地位和作用
  - ✓ 国家信息安全保障工作的基本制度、基本国策；开展信息安全工作的基本方法；促进信息化、维护国家信息安全的根本保障。

关注要点

- 网络安全等级保护的**适用范围**：**中华人民共和国境内**的计算机信息系统
- 网络安全等级保护的**主管单位**：**公安机关**负责网络安全等级保护工作的监督、检查、指导
- **监管力度**：**二级及以上**系统均纳入公安机关监管范围，**其中三级系统至少每年测评一次**
- **三级系统对安全产品主要要求**：**境内独立法人、自主知识产权、信息安全产品认证证书**
- **严重性**：发现不符合网络安全等级保护有关管理规范和技术标准要求，公安机关应当通知其运营使用单位限期整改，并发送**《网络安全等级保护限期整改通知书》**，逾期不改正的，给予警告并向其上级主管部门通报；在限期内拒不改进的，由公安机关处以警告或者**停机整顿**

等级保护具体分级

云上系统的等保要求绝大部分集中在二级和三级系统：

等级	等级定义	适用系统
第一级	信息系统受到破坏后，会对公民、法人和其他组织的合法权益造成损害，但不损害国家安全、社会秩序和公共利益	不重要系统
第二级	信息系统受到破坏后，**会对公民、法人和其他组织的合法权益产生严重损害**，或者对社会秩序和公共利益造成损害，但不损害国家安全	一般重要系统
第三级	信息系统受到破坏后，会对**社会秩序和公共利益造成严重损害**，或者对国家安全造成损害	比较重要系统
第四级	信息系统受到破坏后，会对社会秩序和公共利益造成特别严重损害，或者对国家安全造成严重损害	非常重要系统
第五级	信息系统受到破坏后，会对**国家安全**造成特别严重损害	极度重要系统

阿里云平台等保合规情况介绍

2016年9月，阿里云通过新的云计算安全等级保护三级要求的测评，这是目前**国内首批、也是唯一一家**通过国家权威机构依据**云等保要求联合测评**的**公共云**服务平台。

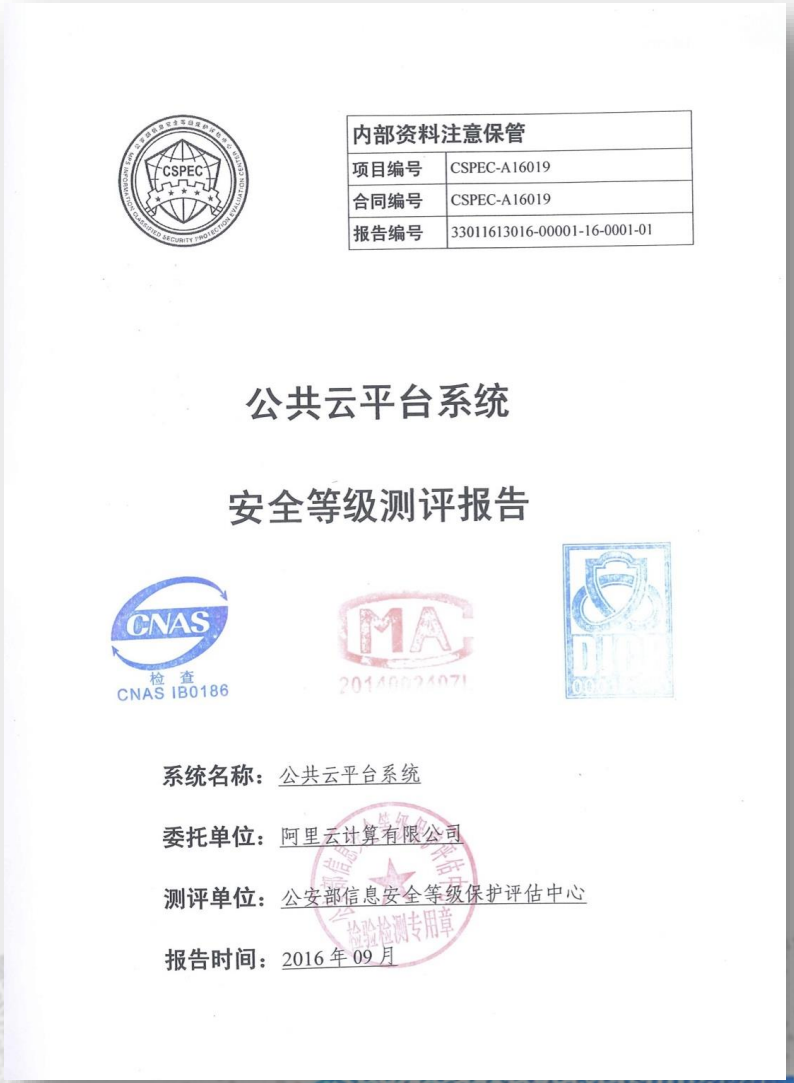
按照新的云等保要求和监管部门的意见，在具体的云上应用等级保护合规和测评中，**涉及阿里云平台侧的相关要求不再进行单独测评，可以直接引用阿里云平台的测评结论。**

阿里云将提供以下材料，协助租户云上系统通过等保测评：

1.阿里云等保备案证明

2.阿里云测评报告封面及结论页

3.阿里云客户等级保护测评说明



内部资料注意保管

项目编号	CSPEC-A16019
合同编号	CSPEC-A16019
报告编号	33011613016-00001-16-0001-01

公共云平台系统

安全等级测评报告

CNAS 检查 CNAS IB0186

系统名称：公共云平台系统

委托单位：阿里云计算有限公司

测评单位：公安部信息安全等级保护评估中心

报告时间：2016 年 09 月

可以从阿里云官网链接https://security.aliyun.com/ 获得阿里云的相关安全服务资质信息，供测评使用：

2012.07
阿里云通过ISO 27001认证

2012.09
阿里云信息系统通过信息安全等级保护三级测评

2013.05
阿里云获得全球首张云安全国际认证金牌

2013.07
阿里云获得首批工信部数据中心联盟组织的可信云服务认证

2016.03
阿里云成为国内首个通过新版ISO 20000认证的云服务商

2016.04
阿里云成为bsi全球首个通过ISO 22301认证的云服务商

2016.04
阿里金融云通过服务组织控制（SOC）独立审计

2016.05
阿里云产品通过CNAS云计算国家标准测试

2016.06
阿里云通过支付卡行业数据安全标准（PCI - DSS）认证

2016.06
阿里云通过新加坡国家标准MTCS T3级认证

云上系统合规责任共[illegible]

阿里云与云上系统

对应标准

- GB/T 22239-2008 信息安全技术 **信息安全等级保护基本要求**
- GB/T 22239.1 信息安全技术 信息安全等级保护基本要求 **第1部分 安全通用要求（征求意见稿）**
- GB/T 22239.2 信息安全技术 信息安全等级保护基本要求 **第2部分 云计算安全扩展要求（征求意见稿）**

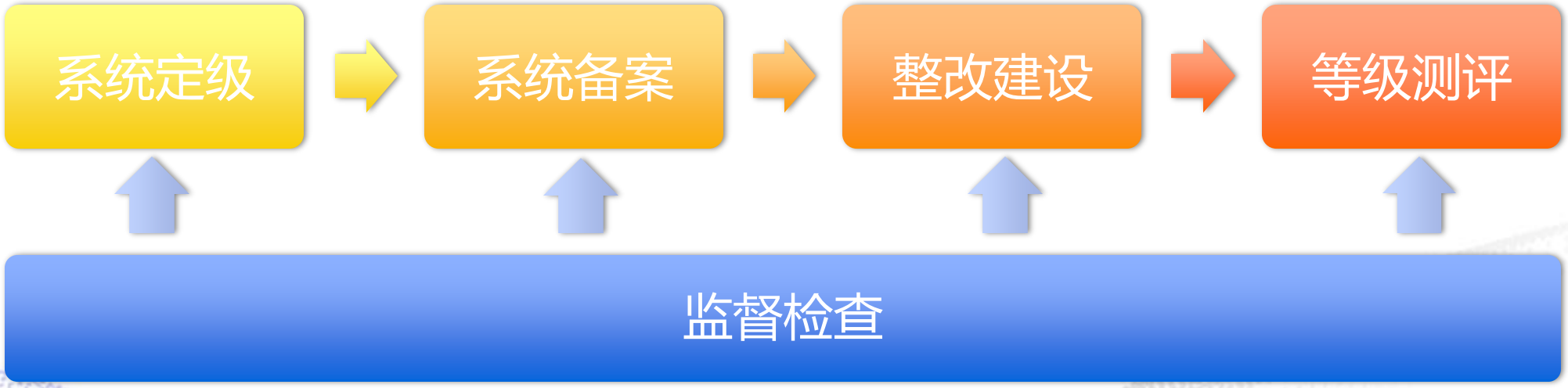
1.等级保护概述

2.云上等保合规方案

3.阿里云优势

等级保护实施流程

根据系统保护等级和各地政策的不同，等级保护实施的流程顺序略有区别，但基本都包括：系统定级、整改建设、等级测评、系统备案和监督检查等五项工作。三级系统的标准实施流程如下：



系统定级：
- 信息系统运营使用单位要按照《信息安全等级保护管理办法》和《网络安全等级保护定级指南》，初步确定定级对象的安全保护等级，起草《**网络安全等级保护定级报告**》（有统一的模板）；**三级以上系统，定级结论需要进行专家评审；**

系统备案：
- 信息系统安全保护等级为**第二级以上时**，备案时应当提交《**网络安全等级保护备案表**》和**定级报告**；第三级以上系统，还需提交**专家评审意见、系统拓扑和说明、安全管理制度、安全建设方案**等。

建设整改：
- 依据《网络安全等级保护基本要求》，利用自有或第三方的**安全产品和专家服务**，对信息系统进行安全建设和整改，同时制定相应的**安全管理制度**；

等级测评：
- 信息系统建设整改完成后，运营使用单位应当选择合适的测评机构，依据《网络安全等级保护测评要求》等技术标准，定期对信息系统安全等级状况**开展等级测评**。

监督检查：
- 公安机关及其他监管部门会在整个过程中，履行相应的监管、审核和检查等职责。

云上系统等保合规“一站式”解决方案

等保合规生态

为了便于阿里云云上系统能够快速满足等保合规的要求，阿里云通过建立**“等保合规生态”**，联合阿里云合作伙伴咨询机构、各地测评机构和公安机关，**向运营单位（阿里云客户）提供一站式、全流程等保合规解决方案。**

等级保护工作分工

- **阿里云**：**整合服务机构能力，**并提供安全产品
- **咨询机构**：提供全流程技术支撑和咨询服务
- **测评机构**：可提供等保咨询和测评服务
- **公安机关**：负责备案审核和监督检查

等保合规方案工作分

	系统定级	系统备案	建设整改	等级测评	监督检查
运营单位	确定安全保护等级，编写定级报告	准备备案材料，到当地公安机关备案	建设符合等级要求的安全技术和管理体系	准备和接受测评机构测评	接受公安机关的定期检查
阿里云	协调第三方机构为运营单位提供辅导服务	协调第三方机构为运营单位提供辅导服务	提供符合等级要求必须的安全产品和服务	提供云服务商安全资质、云平台通过等保的证明材料	
咨询合作伙伴	辅导运营单位准备定级报告，并组织专家评审（三级）	辅导运营单位准备备案材料和备案	辅导运营单位进行系统安全加固和制定安全管理制度	协助运营单位参与等级测评过程并进行整改	协助运营单位接受检查和进行整改
测评合作伙伴				测评机构对系统等级符合性状况进行测评	
公安机关		当地公安机关审核受理备案材料			公安机关监督检查运营单位开展等级保护工作

中小项目测评机构双重角色

《信息系统安全等级保护定级报告》

附件 1：《信息系统安全等级保护定级报告》模版

《信息系统安全等级保护定级报告》

一、XXX 信息系统描述

简述确定该系统为定级对象的理由。从三方面进行说明：一是描述承担信息系统安全责任的相关单位或部门，说明本单位或部门对信息系统具有信息安全保护责任，该信息系统为本单位或部门的定级对象；二是该定级对象是否具有信息系统的基本要素，描述基本要素、系统网络结构、系统边界和边界设备；三是该定级对象是否承载着单一或相对独立的业务，业务情况描述。

二、XXX 信息系统安全保护等级确定（定级方法参见国家标准《信息系统安全等级保护定级指南》）

（一）业务信息安全保护等级的确定

1、业务信息描述

描述信息系统处理的主要业务信息等。

2、业务信息受到破坏时所侵害客体的确定

说明信息受到破坏时侵害的客体是什么，即对三个客体（国家安全；社会秩序和公众利益；公民、法人和其他组织

— 9 —

《定级评审专家意见》（三级系统）

系统定级评审意见表

信息系统运营、使用单位名称			
项目负责人		联系电话	
信息系统名称	××××系统		
系统自定安全级别	××级		
专家评审建议级别	××级		
评审专家组组长	×××		
评审专家组意见： 年 月 日			
信息化主管部门意见	信息化主管部门意见（盖章）： 年 月 日		
专家组成员			
姓名	单 位	职称/职务	

4

信息系统安全等级保护备案表

信息系统安全等级保护
备案表

备 案 单 位：_____（盖章）_____
备 案 日 期：_____

受理备案单位：_____（盖章）_____
受 理 日 期：_____

— 11 —

建设整改阶段，需要运营单位根据相应的安全保护等级要求，对信息系统进行建设和整改，建立完善的**安全管理和安全技术体系。**

安全管理体系

- 安全策略和管理制度
- 安全管理机构和人员
- 安全建设管理
- 安全运维管理

安全技术体系

- 物理和环境安全
- 网络和通信安全
- 设备和计算安全
- 应用与数据安全

建设整改阶段-技术体系

技术体系的建立主要包括安全产品采购、系统配置加固和安全控制开发。阿里云可以提供完整的安全产品方案，咨询机构可以协助对系统进行安全加固，同时协调系统开发厂商进行控制措施开发和整改。

层面	类别	技术要求	阿里云产品
物理和环境安全			直接复用阿里云等保测评结论即可
网络和通信安全	网络架构		VPC 云防火墙/安全组
	通信传输		云盾.证书服务 VPN
	边界防护		VPC+NAT网关 云防火墙/安全组
	访问控制		云防火墙/安全组
	入侵防范		云盾.态势感知 云盾.DDoS高防IP 云盾.Web应用防火墙 云盾.绿网
	恶意代码防范		云盾.Web应用防火墙
	安全审计		云盾.态势感知
	集中管控		云监控 云盾.控制台 云盾.态势感知

层面	类别	技术要求	阿里云方案
设备和计算安全	身份鉴别		堡垒机
	访问控制		堡垒机
	安全审计		堡垒机 云盾.数据库审计/RDS.SQL审计
	入侵防范		云盾.先知 云盾.安骑士
	恶意代码防范		云盾.安骑士 防病毒
	资源控制		云监控
应用与数据安全	身份鉴别 访问控制 安全审计 软件容错 资源控制		主要功能需要应用系统开发商解决 Actiontrail审计阿里云控制台操作 云盾.先知
	数据完整性		KMS服务/云盾加密服务/系统开发商实现 云盾.证书服务 云盾.Web应用防火墙（防篡改）
	数据保密性		KMS服务/云盾加密服务/系统开发商实现 云盾.证书服务
	数据备份恢复		RDS(异地容灾实例)或其他异地备份措施
	剩余信息保护 个人信息保护		主要功能需要应用系统开发商解决

1.等级保护概述

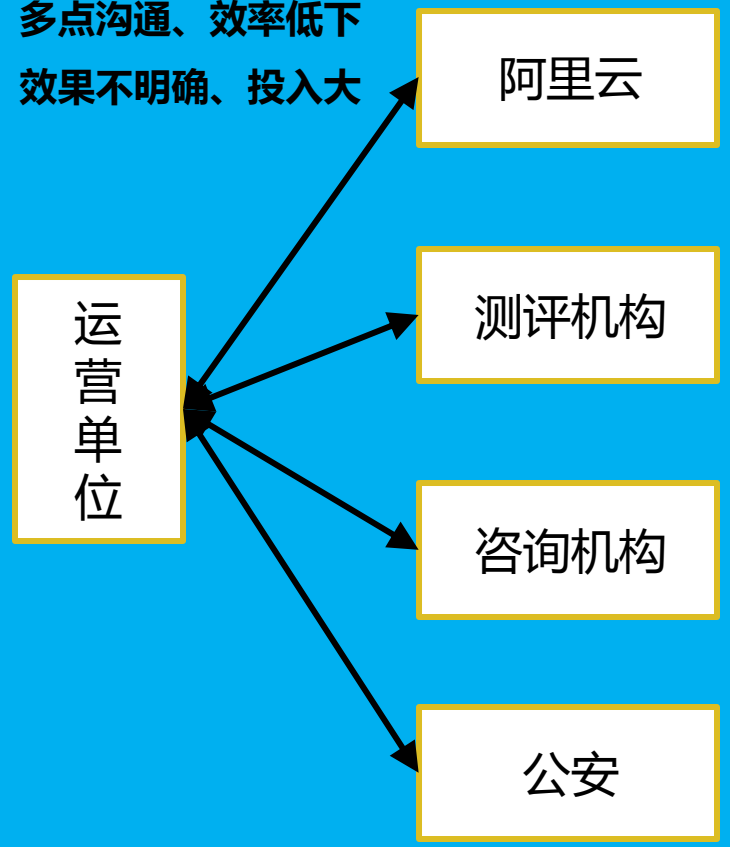
2.云上等保合规方案

3.阿里云优势

阿里云一站式服务优...

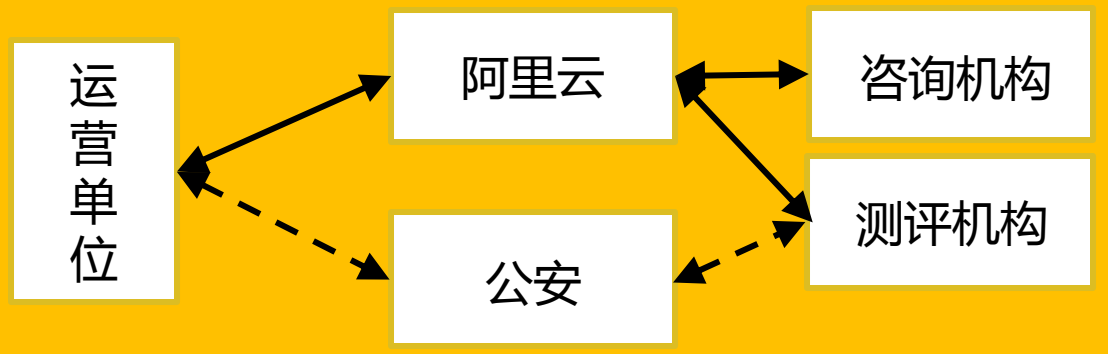
自己找测评机构

- **多点沟通、效率低下**
- **效果不明确、投入大**



VS

阿里一站式服务



- **阿里云最了解云上安全最佳实践**，提供最佳的安全防护建议，**最大化安全防护效果；**
- 阿里云甄选能力强、服务好的测评机构，**最快4周完成合规；**
- **缩小沟通面**，专业机构辅导，丰富实践经验积累，**减少运营单位工作投入。**

阿里云自身通过等保三级（公共云）、四级（金融云）测评，经验丰富：


信息系统安全等级保护
备案证明

依据《信息安全等级保护管理办法》的有关规定，阿里云计算有限公司单位的：

第三级公共云平台系统系统

予以备案。

证书编号：330116-13016-00001

中华人民共和国公安部监制

备案公安机关公章
2016年9月30日

公共云等保备案证明


信息系统安全等级保护
备案证明

依据《信息安全等级保护管理办法》的有关规定，阿里云计算有限公司单位的：

第四级金融云平台系统

予以备案。

证书编号：33000013072-16003

中华人民共和国公安部监制

备案公安机关公章
2016年9月28日

金融云等保备案证明

阿里云云盾全面满足等保要求

阿里云.云盾

数据库审计	态势感知	检测审计
加密服务	证书服务	数据安全
Web应用防火墙	先知	应用安全
堡垒机	安骑士	主机安全
高防IP	云防火墙	网络安全

阿里云.云产品

- SQL审计
- KMS
- 安全组
- VPC

参见：https://cn.aliyun.com/product/yundunall

一站式

联合各地多家咨询和测评机构，一站式合规

专业

阿里公共云/金融云通过等保三级/四级，实践经验丰富

产品合规

通过云盾和安全生态产品，全面满足合规要求

阿里云等级保护安全合规解决方案：https://cn.aliyun.com/solution/classifiedprotection.html

2017云栖大会·成都峰会
THE COMPUTING CONFERENCE

阿里云

云栖社区
yq.aliyun.com

飞天·智能

APSARA INTELLIGENCE

2017云栖大会·成都峰会

5月23日 成都世纪城天堂洲际大酒店