

# TC608云计算标准和开源推进委员

## 云计算安全及风险管理工作组



# 工作组标准总览

安全服务类标准	《基于云计算的业务安全风险解决方案技术要求》	《面向互联网云计算的安全态势感知平台能力要求》	《面向云计算的安全运营中心能力要求》	《研发运营安全解决方案整体框架》 《静态应用程序安全测试工具能力要求》 《交互式应用程序安全测试工具能力要求》
	《全因子信任安全 第2部分：零信任解决方案要求》		《全因子信任安全 第3部分：数据保护工具要求》	
云服务安全类标准	《云计算服务安全要求 第1部分：通用安全要求》	《云计算服务安全要求 第2部分：SaaS安全要求》	《可信云服务安全测评方法 第1部分：云主机》	
数据安全类标准	《云服务用户数据保护能力参考框架》			
	《云服务用户数据保护能力评估方法 第1部分：公有云》		《云服务用户数据保护能力评估方法 第2部分：私有云》	
安全框架类标准	《云计算风险管理框架》	《云计算安全责任共担模型》	《全因子信任安全 第1部分：总体架构》	
	《面向云计算的可信研发运营安全能力成熟度模型》			

# 工作完成情况

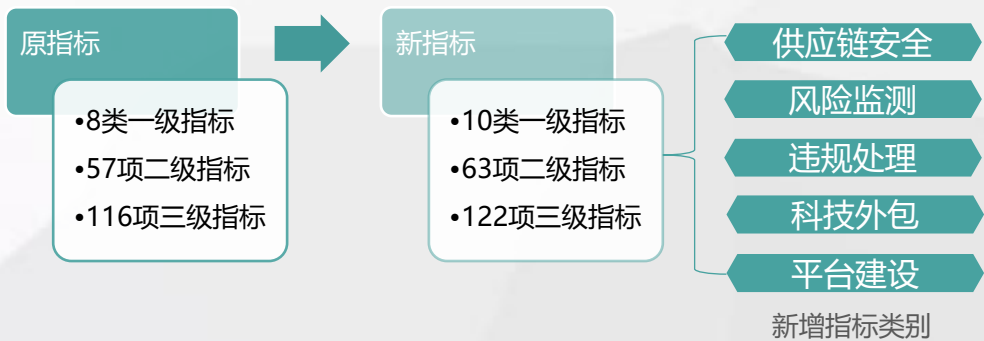
## 云计算风险管理标准

同步在ITU立项 Y.ccrm: Cloud Computing - Framework of Risk Management

制定标准:  
《云计算风险管理框架》

规定了云计算风险管理框架，针对云计算运行过程中面临出现的服务不可用、数据丢失、数据泄露等风险后果提出管理方法，云计算风险管理过程包括风险评估、风险处置、风险接受、风险沟通以及风险监视和评审等内容。

18年底，结合产业发展情况，对《云计算风险管理框架》标准进行了**修订**，新增两大类风险管理指标。



### 通过评估企业（14家）：

中国电信、腾讯云、华为云、阿里云、百度云、京东云、中国移动、UCloud、平安科技、浪潮云、曙光云、联通沃云、金山云、浦发银行

开展评估:  
云计算风险管理能力

将云计算风险管理能力分为基础级、增强级、先进级。  
根据评估结果统计，**基础设施、网络攻击防护、研发安全是软肋**：

- 对于部分云服务商，机房为租用或集团所属，**对机房建设标准掌握程度不够**。
- 云环境下物理边界消失，攻击来源复杂，部分云服务商对南北向流量防护机制较为健全，但**缺少东西向流量**的安全管控。
- 研发阶段安全机制建设不足，**安全设计、开源治理等存在缺陷**。

### 本批参与评估企业：

招商银行

# 工作完成情况

## 云服务用户数据保护能力系列标准

- 1、《云服务用户数据保护能力参考框架》
- 2、《云服务用户数据保护能力评估方法 第1部分：公有云》
- 3、《云服务用户数据保护能力评估方法 第2部分：私有云》

云服务用户数据保护能力评估（公有云/私有云），覆盖了**18个评估内容39项评估点**，从**事前防范**、**事中保护**和**事后追溯**三个层面进行能力评估。2019年首次开展分级评估，将云服务商用户数据保护能力划分为**基础级和增强级**。目前**13家厂商18个云平台**通过能力评估。

**联通云（公有云，私有云）、福建移动、浦发银行**正在参与本批次云服务用户数据保护能力评估。

评估内容（数据保护能力）	
数据持久性	数据私密性
数据隐私性	数据知情权
数据防窃取性	数据可用性
数据访问安全性	数据传输安全性
数据迁移安全性	数据销毁安全性
数据返还安全性	内部人员管控
入侵防范	恶意代码防范
应急响应	安全审计
用户投诉与反馈	服务可审查性

厂商	增强级
腾讯云	公有云、专有云
华为云	公有云、私有云
UCloud	公有云
浪潮云	公有云、私有云
阿里云	公有云、私有云
金山云	公有云
百度云	公有云、私有云
中国移动	公有云
上海有孚	公有云
佳讯飞鸿	私有云
华大基因	私有云
华云	私有云
平安科技	金融云

# 工作完成情况

## 云主机安全首次分级

**基础级** 《可信云服务安全测评方法 第1部分：云主机》标准

**增强级** 《云计算服务安全要求 第1部分：通用安全要求》标准

主机安全作为安全防护的“**最后一公里**”，是安全防护的最后保障。通过开展云主机安全标准制定和评估工作，以实现的云主机安全、可靠，促进云计算服务商和云计算用户共同维护主机安全

**百度云、银联云**正在参与本批次云主机安全评估

评估内容（基础级）	评估内容（增强级）
密钥策略安全	访问控制
身份鉴别安全	身份鉴别
登录策略安全	数据安全
数据传输安全	安全审计
口令策略安全	安全运行
日志管理管理	安全策略管理
审计策略安全	
补丁管理安全	
服务及端口安全	
Web安全	

**通过评估企业（13家）：**  
金山云、UCloud、浪潮云、上海有孚、万达信息、  
中国电信、京东云、平安科技、中国移动、阿里云、  
联通沃云、腾讯云、华为云

# 工作完成情况

## 《基于云计算的业务安全风险解决方案技术要求》

### 通过评估企业：

**内容安全：**腾讯云、同盾科技、阿里云、华为云

**五大类解决方案：**内容安全、交易反欺诈、营销反欺诈、信贷反欺诈、钓鱼反欺诈

**五大类指标要求：**服务模式、功能要求、风控技术、性能要求，安全管理

提供直播安全解决方案，为直播及服务企业提供图片、视频、直播的鉴黄服务

提供个人和企业信贷风控能力，通过信息采集、风险分值评估等方式对信贷风险提供监控和预警

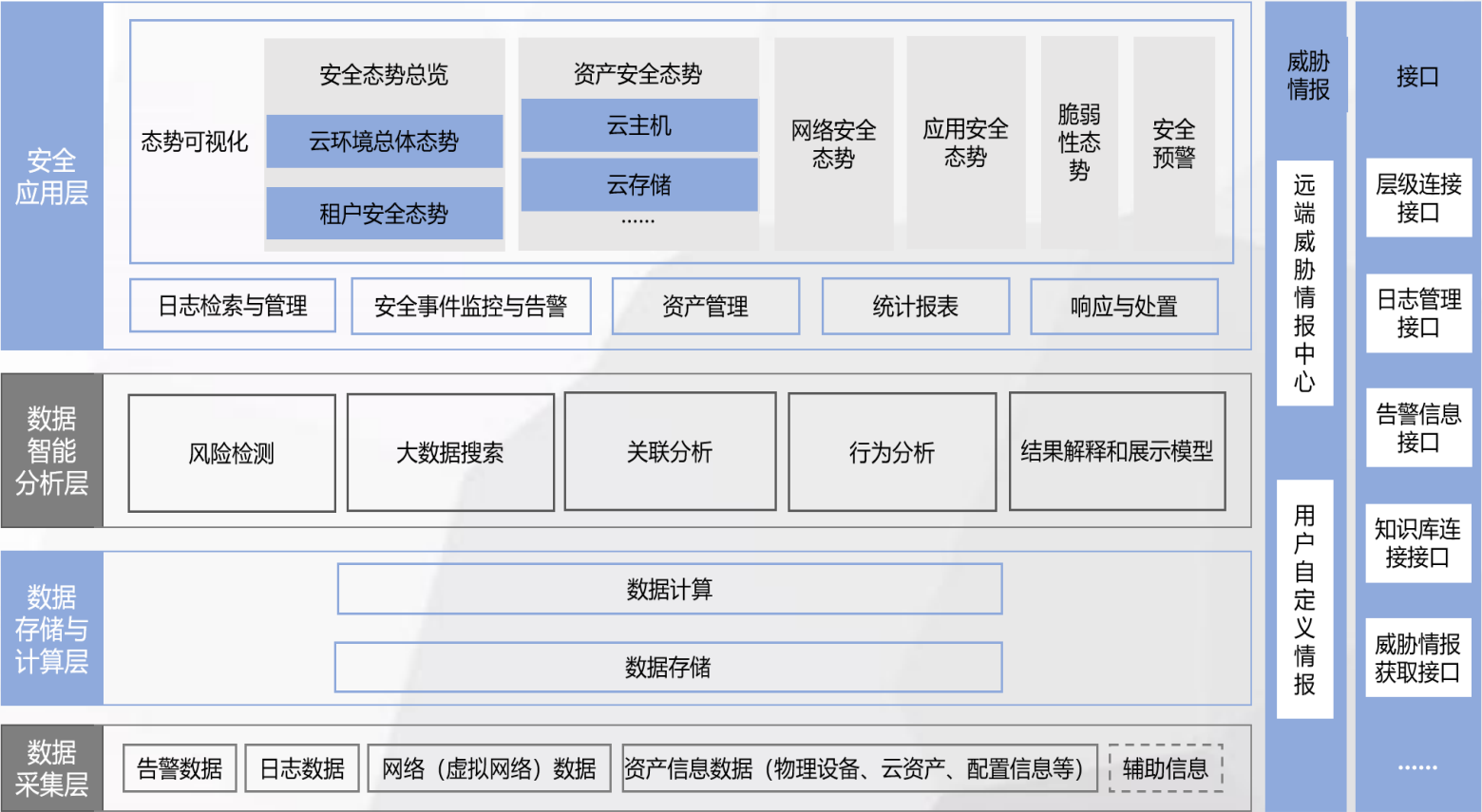
提供企业账户、营销、交易等关键业务中所遇到的欺诈问题

提供防羊毛党、防好评、防刷点击等营销作弊行为。



# 工作完成情况

## 《面向互联网云计算的安全态势感知平台能力要求》



### 八大建设原则:

易用性、动态性、兼容性、可靠性、通用性、可管理性、安全性、可扩展性

### 五大功能要求:

数据采集层、数据存储与计算层、数据智能分析层、安全应用层、威胁情报

### 通过企业

- 阿里云
- 金山云
- 华为云

- 移动云
- 腾讯云
- 浙江联通

### 本批参评企业

- 天翼云



# 工作完成情况

## 《面向云计算的安全运营中心能力要求》

面向云计算的安全运营中心能力  
评估要求分为两大类，**平台能力**  
**要求**和**安全人员能力**要求。

包含**16类**一级指标

**71项**平台能力要求指标

**18项**安全人员能力要求指标

### 平台能力要求

#### 云资产管理

- 资产管理
- 资产收集
- 资产展现
- 资产维护
- .....

#### 安全策略管理

- 安全基线
- 集中管理
- 展现与分析
- 自定义创建
- .....

#### 安全运营 流程管理

- 流程内容和  
配合
- .....

#### 安全风险 评估管理

- 系统安全风  
险评估
- 网络安全风  
险评估
- .....

#### 安全团队管理

- 攻击防御
- 主动响应
- 被动响应
- .....

#### 通用技术要求

- 用户隔离
- 多级管控
- 安全审计
- 权限控制
- .....

#### 安全漏洞和 补丁要求

- 漏洞发现
- 漏洞管理
- 漏洞分析
- 补丁获取
- .....

#### 安全事件分析和 告警要求

- 日志、流量、  
文件预处理
- 威胁情报利  
用
- 攻击溯源

#### 自动化响应 与通知

- 安全编排
- 安全设备联  
动
- 工单交互
- .....

#### 实时监控和 可视化展示

- 实时监控
- 大屏展示
- 安全集成
- 合规报表
- .....

#### 安全运营知识库

- 分场景安全  
运营知识库
- 知识库完善
- .....

#### 接口要求

- 云平台接口
- 日志接口
- 南向接口
- 北向接口
- .....

#### 数据源采集要求

- 安全设备
- 网络流量
- 威胁情报
- 日志数据
- .....

#### 数据存储、 处理要求

- 隔离存储
- 隔离处理
- 存储期限  
合规
- .....

### 安全人员能力要求

#### 安全运营 流程管理

- 人员职责
- 安全运营  
处理流程
- .....

#### 安全团队管理

- 安全团队  
能力要求
- 高级安全  
分析
- 威胁情报  
利用
- .....

#### 安全运营 考核管理

- 安全量化  
指标
- 量化考核
- 考核上报
- 数据展现
- .....

#### 安全运营知识库

- 安全应急  
预案
- 应急指导
- .....

### 通过企业

- 华为
- 腾讯云
- 深信服
- 阿里云

- 联通云
- 浪潮
- 启明星辰
- 奇虎360

### 本批参与及对接企业

- 招商银行
- 浦发银行
- 知道创宇
- 天融信
- 安恒

- 恒安嘉新
- 奇安信
- 京东云
- 卫士通

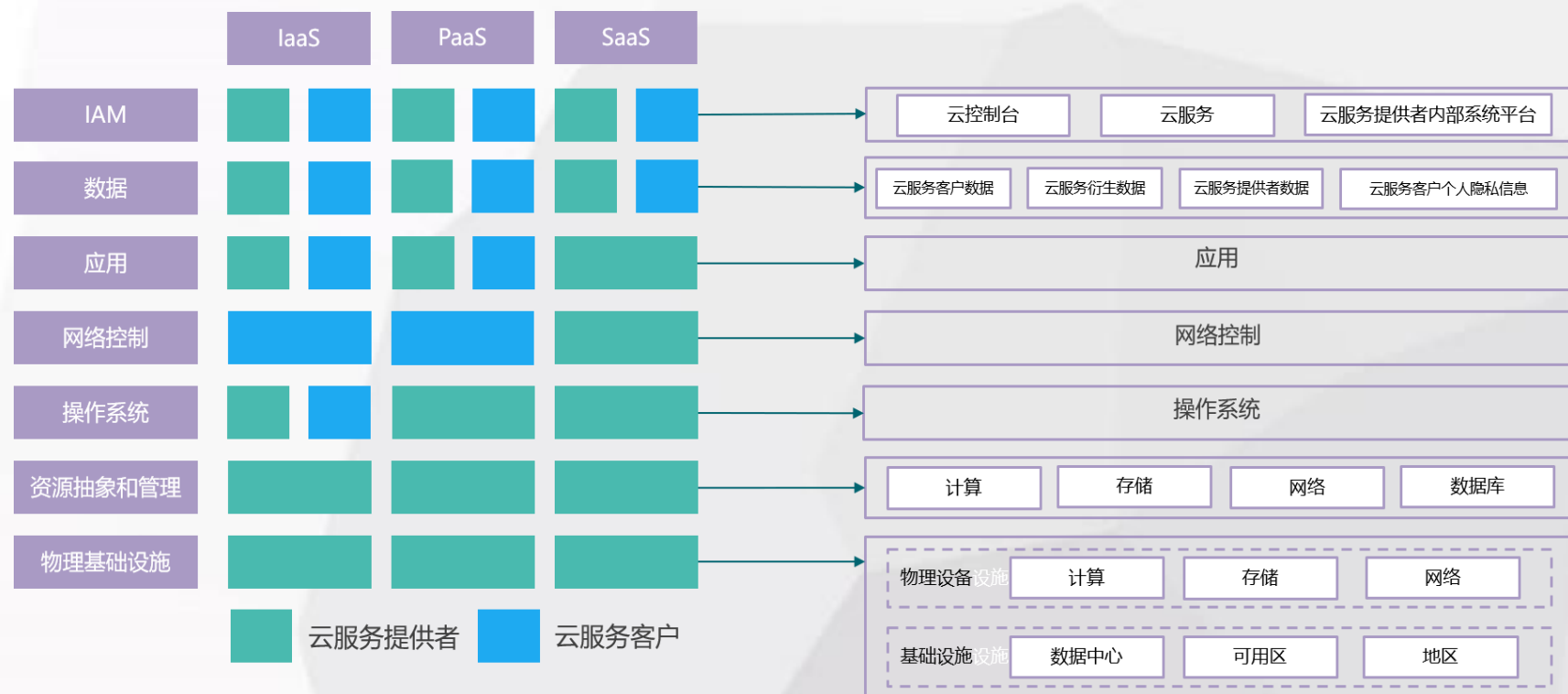


# 工作完成情况

## 《云计算安全责任共担模型》

### 三大类评估内容：

- ✓ 云服务商—云服务责任承担能力评估，评估云服务商承担的最小安全责任是否满足标准要求
- ✓ 云服务客户—云服务安全使用能力评估，评估云服务客户对所使用云服务的安全使用能力
- ✓ 云服务管理方—云服务责任管理能力评估，考察专有云、私有云管理方（如政务云主管方）能够基于业务场景和安全要求对云平台的责任进行有效管理



### 云服务责任承担能力 评估通过企业：

阿里云、华为云、  
腾讯云、浪潮云

### 云服务责任管理能力 评估通过企业：

烟台市大数据局

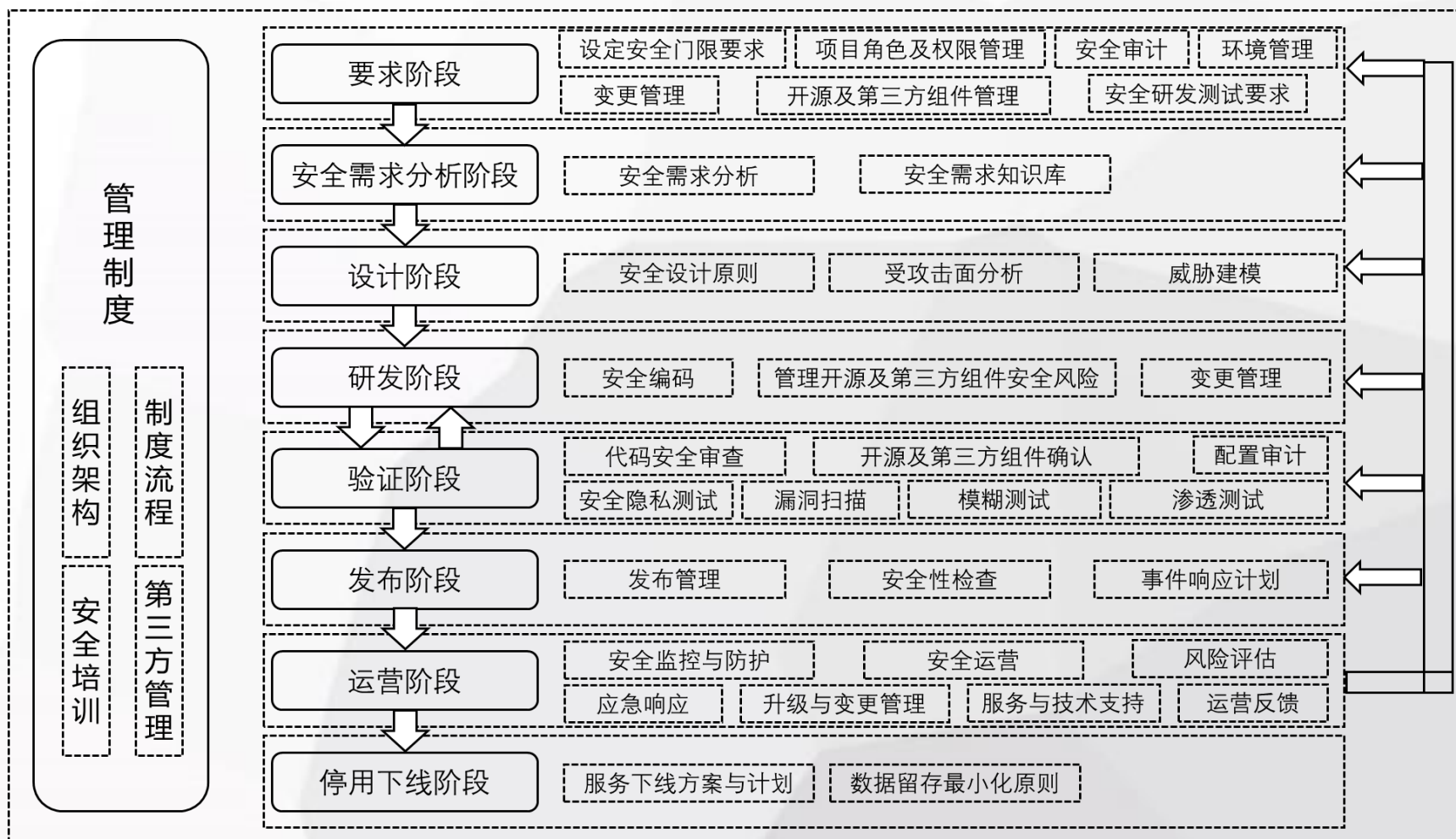
### 本批正在对接企业：

联通云、天翼云

# 工作完成情况

## 《面向云计算的可信研发运营安全能力成熟度模型》

对于厂商的研发运营安全能力从软件应用服务全生命周期，搭配管理制度**9大部分**进行评估，分为**基础级、增强级、先进级三个级别**



首批面向云计算的可信研发运营安全能力成熟度评估工作正在持续推进过程中，预计于2021年上半年完成首批评估工作

# 工作完成情况

## 研发运营安全工具系列标准

### 评估标准:

#### 静态应用程序安全测试 (SAST) 工具能力要求

扫描分析能力要求

灵活性能力要求

分析辅助能力要求

开发流程嵌入能力要求

扩展性能力要求

兼容性能力要求




部署能力要求

安全性能力要求

服务支持能力要求

#### 交互式应用程序安全测试 (IAST) 工具能力要求

对于厂商提供的研发运营安全工具能力从用户视角出发，涵盖扫描分析能力要求、灵活性能力要求、分析辅助能力要求、开发流程嵌入能力要求、扩展性能力要求、兼容性能力要求、部署能力要求、安全性能力要求、服务支持能力要求九大评估部分，帮助用户进行选型参考。

    
**首批研发运营安全工具评估将于  
2021年上半年启动**

**目前正在与悬镜、开源网安、奇安信、新思等企业推进首批评估相关工作。**

# 工作完成情况

《云计算服务安全要求 第 1 部分：通用安全要求》

《云计算服务安全要求 第 2 部分：SaaS安全要求》

作为云安全的重要组成部分，云服务的安全能力以及云服务自身的安全性不但是云服务用户云上业务系统的安全性的重要保障，还是维持系统合规水平的关键环节。因此建立统一的云服务安全设计标准，对于规范和提高云服务的安全能力有非常现实的意义。

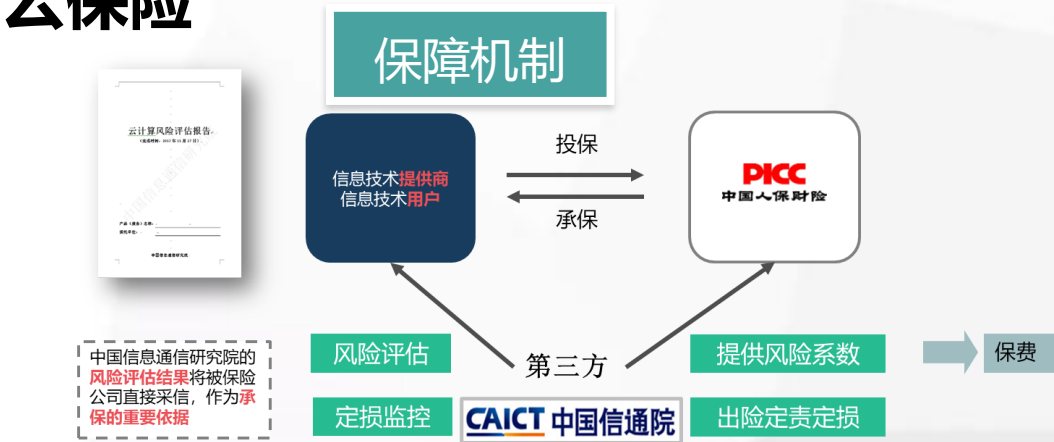
**首批云服务安全评估（IaaS/PaaS安全，SaaS安全）工作正在持续推进过程中**

**目前正在与阿里、华为、腾讯、移动、电信、浪潮、百度、UCloud、用友、微盟、深信服、杭州天谷、知道创宇、同创永益、财智共享等企业推进首批评估相关工作。**



# 工作完成情况

## 云保险



产品概述

在保险期间，企业提供云计算服务时，由于故障责任、误操作责任和第三方责任等，导致用户服务不可用或数据丢失，依据服务协议，应由企业承担的经济赔偿责任，保险人按照保险合同约定负责赔偿。

### 保障内容

**保障对象**

云计算服务商  
数据中心服务商  
互联网服务商

**保障内容**

服务不可用  
数据丢失

### 模式创新升级

云保险模式创新升级，首次推出将**可信云MSP评估与云保险结合推广的创新模式**，对MSP企业进行“事前+事后”的持续保护，**帮助企业建立用户的可信品牌**。



### 云保险优势

- 企业对可能面临的风险带来的经济损失进行有效转移，为企业分担成本。
- 云保险作为可信云帮助企业建立客户信任的**可信品牌**的重要一环。增加客户信任，扩大企业影响力。

# 在研标准及近期计划

《全因子信任安全 第1部分：总体架构》

01

《全因子信任安全 第2部分：零信任解决方案要求》

02

《全因子信任安全 第3部分：数据保护工具要求》

03



7月27-28日 可信云大会

高性能 混合云 数字政府 云边 云安全 软件安全 软件质量

2021 年可信云大会

主办单位：中国信息通信研究院  
支持单位：中国通信标准化协会云计算标准和开源推进委员会  
混合云产业联盟、云服务经验自律委员会、网络风险与保险创新实验室  
承办单位：云计算开源产业联盟  
协办单位：中国 IDC 圈

大会开幕式		
主持人：中国信息通信研究院领导		
时间	内容	演讲人
9:00-9:05	致辞	工业和信息化部领导
9:05-9:10	致辞	中央国家机关政府采购中心领导
9:10-9:20	可信云评估总体发展情况通报	中国通信标准化协会领导
9:20-9:30	可信云最新评估结果发布 ——首批多云互联评估结果 ——首批云迁移评估结果 ——首批云主机安全分级评估结果 ——首批云服务安全评估（IaaS、PaaS、SaaS） ——首批 SAST、IAST 评估结果发布 ——首批研运安全成熟度评估结果发布 ——首批高性能计算平台云标准评估结果（拟） ——首批混沌工程测试平台评估结果 ——首批可观测性平台评估结果 ——首批云原生技术架构/业务应用成熟度评估结果 ——首批金融场景容器性能评估结果 ——首批 3G/4G/5G 边缘云平台能力评估 ——首批云化 MEC 边缘云能力评估 ——首批边缘容器服务能力评估	工业和信息化部信息通信发展司领导 中国信息通信研究院领导

	——首批边缘智能服务能力评估 ——首批边缘一体机技术能力评估 ——首批边缘安全能力评估 ——首批边缘视频监控平台能力评估	
09:30-09:35	MSP 保险保障项目发布 DDoS 保险保障项目发布 数字保险保障项目发布	中国信息通信研究院领导
9:35-9:40	2021 可信云技术最佳实践 2021 可信云服务最佳实践 2021 可信云技术最佳实践	中国信息通信研究院领导
9:40-9:45	全球云计算高性能创新大赛启动仪式	工业和信息化部信息通信管理局领导
云服务产业发展		
主持人：中国信息通信研究院领导		
9:45-10:00	《云计算发展白皮书（2021）》	中国信息通信研究院
10:00-10:20	主题演讲	合作企业
10:20-10:40	《云原生发展白皮书》	中国信息通信研究院
10:40-10:55	《云服务安全成熟度（CSSM）白皮书》	华为
10:55-11:15	主题演讲	技术专家
11:15-11:30	主题演讲	合作企业
11:30-11:45	《云安全白皮书》	中国信息通信研究院
高性能论坛		
时间	内容	演讲人
13:30-13:55	主题演讲	中国信息通信研究院专家
13:55-14:20	主题演讲	合作伙伴
14:20-14:45	主题演讲	中国信息通信研究院专家
14:45-15:10	主题演讲	合作伙伴
云安全论坛		
时间	内容	演讲人
13:30-13:55	全因子信任安全系列标准	中国信息通信研究院专家
13:55-14:20	主题演讲	合作伙伴

8.15 上午		
可信行业云标准发布		
主持人：中国信息通信研究院云计算与大数据研究所领导		
时间	内容	演讲人
9:00-9:05	致辞	工业和信息化部信息化和软件服务业司领导
9:05-9:10	致辞	行业监管部门领导
9:20-9:25	可信行业云最新评估结果发布 ——专有云模式政务云服务评估结果发布 ——政务云综合水平评估结果发布 ——政务云解决方案评估结果发布 ——公有云模式的政务云服务评估结果发布 ——数字政府一体化支撑平台评估结果发布 ——可信金融云服务（银行类）能力评估 ——可信金融云解决方案能力评估 ——数字文娱（视频云&游戏云）评估结果发布	中国信息通信研究院
9:00-9:35	云服务综合信用水平评估结果发布	中国信息通信研究院
主持人：中国信息通信研究院云计算与大数据研究所领导		
9:35-10:00	主题演讲	合作企业
10:00-10:25	主题演讲	技术专家
10:25-10:40	中国云 MSP 服务发展调查报告	中国信息通信研究院
10:40-11:00	主题演讲	合作伙伴
11:00-11:20	主题演讲	技术专家
11:20-11:35	数字文娱云计算应用与发展研究报告	中国信息通信研究院
数字政府论坛		
时间	内容	演讲人
13:30-13:55	数字政府一体化支撑平台建设与应用白皮书	中国信息通信研究院专家
13:55-14:20	主题演讲	合作伙伴
14:20-14:45	数字政府最佳实践案例集	中国信息通信研究院专家



THANK YOU



谢谢大家