ICS 35.100.05，35.240.40
L79，A11

T /IA C

中 国 保 险 行 业 协 会 团 体 标 准

T/IAC XXXXX—2018

面向保险行业的云服务提供方能力要求

Service capability requirements for insurance industry cloud service providers

（征求意见稿）

201X-XX-XX 发布　　XXXX - XX - XX 实施

中国保险行业协会　　发　布

目　　次

前　言

本标准按照GB/T 1.1-2009给出的规则起草

本标准由中国保险行业协会提出并归口

本标准起草单位：中国信息通信研究院，中国太平洋保险（集团）股份有限公司，中国人寿保险股份有限公司数据中心，中国人民财产保险股份有限公司，安心财产保险有限责任公司，华为技术有限公司，深圳市腾讯计算机系统有限公司，北京优帆科技有限公司，云栈科技（北京）有限公司，杭州数梦工场科技有限公司，北京易捷思达科技发展有限公司

本标准起草人：

引　　言

为了保证云服务提供方在为保险行业提供云服务时，能够根据机构实际情况，提供满足互联网环境下计算资源弹性变化等需求的服务，结合保险行业特点以及金融机构云计算系统安全建设需要,对为保险行业提供服务的云服务提供方，从服务能力和资质两方面做出具体指引要求，并给出服务协议参考架构。

面向保险行业的云服务提供方能力要求

1 范围

本标准规定了云服务提供方为保险行业提供云服务时，需具备的服务能力。

本标准适用于正在或可能为保险行业提供云服务的企事业单位。主要分为两类，一类是隶属于同一保险集团、面向本保险集团内各级机构提供云服务的云服务方，一类是云服务方与云服务客户不属于同一系统集团。

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，仅所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/T 29246-2017 信息技术 安全技术 信息安全管理体系 概述和词汇

GB/T 31167-2014 信息安全技术 云计算服务安全指南

GB/T 32400-2015 信息技术 云计算 概览与词汇

3 术语和定义

下列术语和定义适用于本文件。

3.1

云计算 cloud computing

一种通过网络将可伸缩、弹性的共享物理和虚拟资源池按需自服务的方式供应和管理的模式。

注：资源包括服务器、操作系统、网络、软件、应用和存储设备等。

[GB/T 32400-2015，定义3.2.5]

3.2

云服务提供方 cloud service provider

提供云服务的参与方。

注1：目前有两种保险类云服务提供方，一类是隶属于同一保险集团、面向本保险集团内各级机构提供云服务的云服务方，一类是云服务方与云服务客户不属于同一系统集团。

注2：定义没有安全按照 GB/T 32400-2015

3.3

云服务客户 cloud service user

为使用云服务而处于一定业务关系中的参与方。

注：业务关系不一定包含经济条款。

[GB/T 32400-2015，定义3.2.11]

3.4

第三方评估机构 third party assessment organization

独立于云服务提供方和客户的专业评估机构。
[GB/T 31167-2014，定义3.5]

3.5

完整性 integrity

准确和完备的特性。
[GB/T 29246-2017，定义2.40]

3.6

可用性 availability

被授权实体按需访问和使用的特性。
[GB/T 29246-2017，定义2.9]

3.7

基础设施即服务层 infrastructure as a service

为云服务客户提供云能力类型中的基础设施能力类型的一种云服务类别。

注：包括虚拟主机、物理主机、虚拟存储、物理存储、网络资源、数据复制、安全设备、传输线路等，对应硬件或基础设施产品、机房托管。服务方可以按照客户需求提供专属云、容灾云以及备份云等服务。

3.8

平台即服务 platform as a service

为云服务客户提供云能力类型中的平台能力类型的一种云服务类别。

注：包括金融数据库、内容分发、安全防护等。服务方可以按照客户需求为保险行业提供容器以及大数据技术等服务。

3.9

软件即服务 software as a service

为云服务客户提供云能力类型中的应用能力类型的一种云服务类别。

注：包括办公自动化系统、客户关系管理系统、人力资源管理系统等。

4 保险业云服务提供方服务能力要求

4.1 数据持久性

对保险业云服务提供方的数据持久性能力要求如下：

——应承诺数据存储的持久性，保证数据承诺范围内的保存不丢失；
——应承诺数据的一致性，支持数据完整性破坏检测，在检测到完整性错误时采取必要的恢复措施；
——根据保险行业的实际情况，定期进行数据备份，保证数据的完备，并对备份数据的有效性进行检查，每次抽检数据量不低于 5%。采用多副本备份时，应采用适当的机制保证多副本的一致性。

4.2 数据可销毁性

对保险业云服务提供方的数据可销毁性能力要求如下：
——在用户要求删除数据或设备在弃置、转售前必须将其所有数据彻底删除，并无法复原。

4.3 数据可迁移性

对保险业云服务提供方的数据可迁移性能力要求如下：
——应能够控制数据的迁移，在保险行业客户启用或弃用云服务时，数据可根据数据量级在一定时间要求内迁入和迁出。

4.4 数据安全隔离性

对保险业云服务提供方的数据安全隔离性能力要求如下：
——与外部通信时，应根据加密策略自动对数据进行安全加密和解密操作，保证数据在存储、传输中都是秘文状态；
——当需要对数据进行迁移时，应对其内部密码、密钥、证书等敏感数据进行加密，保证数据的私密性和完整性；
——关键业务信息，如鉴别信息，应采用加密方式存储，并支持保险行业云服务使用方选择第三方加密，且秘钥可以在使用方本地保管和维护；
——对多个客户保存在同一数据库实例和数据库表中的数据，应对的客户进行有效隔离，保证客户之间的数据不可见；
——每个虚拟机应获得独立的资源，且只能访问分配给该虚拟机的磁盘。还应支持控制虚拟机之间以及虚拟机和物理机之间所有的数据通信。

4.5 数据知情权

对保险业云服务提供方的数据知情权能力要求如下：
——应告知用户数据存储位置（至少精确到数据中心级别）和使用程度等信息。

4.6 服务可审查性

对保险业云服务提供方的服务可审查性能力要求如下：
——应支持在必要的条件下，按用户要求由于合规或是安全取证调查等原因，在规定时间内可以提供相关的信息，如关键组件的运行日志、运维人员的操作记录、审计日志、系统日志等；
——应支持网络流量镜像日志、云管理操作日志等日志导出给保险行业；
——云服务提供方应设立专门的安全协调员或部门，负责与保险行业安全部门，以及中国银行保险监督委员会及其派出机构对接，遵从中国银行保险监督委员会信息科技监管政策、规范要求；配合中国银行保险监督委员会及其派出机构对提供云计算服务的保险行业进行风险监测、现场核查和信息科技风险事件处置；按照中国银行保险监督委员会要求，完成自查和问题整改等。

4.7 服务功能

对保险业云服务提供方的服务功能能力要求如下：

——应具备计算、存储、网络方面的功能，保证为客户提供相应的云计算服务；

——应为保险行业相关部门及负责人员提供详细的技术和使用说明文档,以确保客户能正常使用云计算产品；

——应支持资源管理的分权管理，能够实现对资源最小粒度的管控模型。

4.8 服务可用性

对保险业云服务提供方的服务可用性能力要求如下：

——针对保险行业，承诺不低于 99.95%的服务可用性；

——应在软件、硬件发生故障时能恢复至正常状态；

——需保证计算、存储、网络、控制节点中的单一或多个节点在发生故障时，不影响云计算服务或整个平台的使用；

——确保保险行业日常业务云上功能模块能够连续运行，不出现中断。在某些系统或子系统功能失效的情况下，关键系统不至于瘫痪，主要功能不会丧失。

4.9 服务资源调配能力

4.9.1 虚拟机资源配置调整

对保险业云服务提供方的虚拟机资源配置调整能力要求如下：

——应具备较强的虚拟机资源弹性扩展能力，支持 VCPU、内存的灵活升降；

——应在合理的时间区间内完成配置调整。

4.9.2 存储容量配置调整

对保险业云服务提供方的存储容量配置调整能力要求如下：

——应具备较强的存储容量弹性扩展能力，支持存储容量的灵活升降；

——应具备与存储系统的软件定义存储开放对接能力；

——应在合理的时间区间内完成配置调整；

——支持存储性能选择，可以根据不同性能需求选择存储类型。

4.9.3 网络资源调整

对保险业云服务提供方的网络资源调整的能力要求如下：

——应具备较强的网络资源弹性扩展能力，支持网络带宽的灵活升降；

——应具备支持保险行业多个内部用户的能力（IP 地址重叠）；

——应在合理的时间区间内完成配置调整。

4.9.4 资源池扩充

对保险业云服务提供方的资源池扩充能力要求如下：

——应具备较强的物理节点弹性扩充能力；

——应在合理的时间区间内完成配置调整。

4.10 变更协商权

对保险业云服务提供方的变更协商权能力要求如下：

——应保证云服务客户的变更协商权，云服务提供方在开展任何可能会影响云服务客户使用云服务的变更时，应在变更前告知云服务客户，并征得云服务客户同意后进行变更。

4.11 故障恢复能力

对保险业云服务提供方的故障恢复能力要求如下：

——应建立完善的故障管控体系，包括故障监控、快速定位、自动化恢复、故障告警等，严格执行信息系统 7×24 小时监控制度；

——应具备设置多个告警级别的功能；

——应支持配置告警阈值；

——应支持监控平台、邮件、短信等渠道的告警；

——应具备多种故障恢复手段或技术，如降级恢复、临时方案、彻底解决等，针对不同故障，选择不同的故障恢复手段；

——应有专门的故障维修人员负责保障工作；

——应支持提供真实完整故障报告；

——应提供基于云服务的开发、运维、使用的技术说明文档；

——云服务提供方应根据中国银行保险监督委员会《保险业信息系统灾难恢复管理指引》，建立科学预警机制，设立应急组织结构，分级制定应急预案。

4.12 网络接入能力

对保险业云服务提供方的网络接入能力要求如下：

——应确保网络带宽能达到保险行业购买的服务要求；

——支持多种接入方式，如专线或 IPSecVPN 等，满足保险业务在多个机构进行互通；

——支持关闭管理控制台的公网访问。

4.13 安全能力

对保险业云服务提供方的安全能力要求如下：

——提供高等级业务安全防护，如防恶意注册、登陆保护等；

——具有完善的安全监控和防御体系，提供7×24小时安全服务；

——具有多重网络安全防护措施，能够有效防御DDos攻击、Web入侵、DNS劫持等问题；

——当用户有需求时，能够满足用户拥有独立物理空间和物理设备的需求；

——至少具有同城双中心的容灾备份能力，可自主选择建议建设异地灾备中心。

4.14 服务计费准确性

对保险业云服务提供方的服务计费准确定能力要求如下：

——云服务提供方为保险行业提供的云计算产品需具备资源计量的功能，提供的云计算服务需具备准确的计量系统；

——在计费系统规则出现变更时，应及时通知云服务用户；

——能够按实际的使用量或购买量计费；

——提供包年包月的计费；

——支持弹性降费。

4.15 服务协议规范性

对保险业云服务提供方的服务协议规范性能力要求如下：

——与用户签订的服务协议应具有规范性，相应参考框架以及规范性描述见附录 A。

4.16 第三方服务

对保险业云服务提供方与第三方服务的能力要求如下：

——应支持与其他云服务提供方配合协作，并支持接入多云管理平台。

5 保险业云服务提供方资质要求

5.1 内部云服务提供方资质要求

对内部保险业云服务提供方的资质要求如下：

a) 数据中心的机房设计标准必须符合国家标准规范和中国银行保险监督委员会的要求，数据 来源于中华人民共和国境内的，数据中心的物理位置应当位于境内。
b) 具备信息安全管理体系评估认证，具有健全的组织架构、有效的风险治理架构和专职的信息科技风险管理团队，定期开展风险评估和审计工作。
c) 具备与所承担服务范围和业务规模相适应的服务管理体系。
d) 支持内部结算等计量方式。（可选）

5.2 外部云服务提供方资质要求

对外部保险业云服务提供方的资质要求如下：

a) 在中华人民共和国境内注册的法人机构或所在国家/地区监管当局已与我国金融监督管理机构签订谅解备忘录或双方认可的其他约定的境外服务供应商。
b) IaaS、PaaS 服务提供方应具有 IDC 牌照；工信部或其认可的第三方评估机构出具的相关评估资质证明。
c) 具备信息安全管理体系评估认证，具有健全的组织架构、有效的风险治理架构和专职的信息科技风险管理团队，定期开展风险评估和审计工作。
d) 具有足够的技术能力、人力资源和设施、环境，满足云计算服务的质量和安全管理要求。（可选）
e) 具备一年以上的金融云服务经验，服务客户数不少于一家或具备一年以上的非金融云服务经验，服务客户数不少于三家。（可选）

附 录 A
（资料性附录）
保险业云服务提供方服务协议参考框架

注 1：以下所有示例仅为例子，不是标准规范内容。

注 2：所列指标项，可以根据不同服务不同用户需求，适当裁剪或增加。

1. 数据持久性

包括但不限于4.1节所要求内容。

示例 1：

合同期内每月对象文件的持久性为 99.99%。意为每月用户 10000 个存储的文件，合同期内每月数据不丢失的概率为 99.99%，即每月只有 1 个文件丢失的可能性。

2. 数据可销毁性

包括但不限于4.2节所要求内容。

示例 2：

在用户要求删除数据或设备在弃置、转售前服务商将采取高级清零操作彻底删除用户所有数据，并无法复原，硬盘报废时将消磁。

3. 数据可迁移性

包括但不限于4.3节所要求内容。

示例 3：

服务商将提供的 X 格式的数据服务，或支持用户现有数据存储方式，在用户迁入迁出时提供技术转换手段到标准 Y 格式。

4. 数据安全隔离性

包括但不限于4.4节所要求内容。

示例 4：

服务商提供 X 数据加密算法和 Y 数据隔离方法,保证同一资源池用户数据互不可见。

5. 数据知情性

包括但不限于4.5节所要求内容。

示例 5：

（1）服务商告知用户的数据存在 X 数据中心。（2）有 3 个备份，存储在 Y 数据中心。（3）用户有权选择本身数据的数据中心位置，无权选择备份数据的数据中心位置。（4）两个数据中心当地的法律遵守中华人民共和国 Z 法律。（5）用户所有数据不会提供给任意第三方，除政府监管部门监管审计需要。用户所有数据不会存在国外数据中心或用于国外业务或数据分析。用户的行为日志会用于 A 业务的机器人自动数据分析，但不会对外呈现用户个人信息数据。

6. 服务可审查性

包括但不限于4.6节所要求内容。

示例 6：

在 X 条件下由于合规或是安全取证调查等原因可以提供相关的信息，如关键组件的运行日志、运维人员的操作记录给用户。

7. 服务功能

包括但不限于4.7节所要求内容。

示例 7：

服务商承诺用户提供 X 的服务器功能，Y 操作软件等等。每一项功能提供给用户相关的说明。

8. 服务可用性

包括但不限于4.8节所要求内容。

示例 8：

服务商承诺用户 99.9%的可用性，即用户每月服务可用时间应为 30 天×24 小时×60 分钟×99.9%=43156.8 分钟，即存在43200-43156.8=43.2 分钟的不可用时间。并且在服务不可用的统计单元为单台云主机算，不可用时间规定为服务不可用 5 分钟以上算一次不可用，计入不可用时间，低于 5 分钟不可用不计入不可用时间。

9. 服务资源调配能力

包括但不限于4.9节所要求内容。

示例 9：

服务商承诺用户，可以满足计算资源 20%的容量，24 小时完成；100%的容量需要 2 天；每次最大可扩展 100%容量，最小 10GB 的容量。

10. 变更协商权

包括但不限于4.10节所要求内容。

示例 10：

服务商承诺用户，在开展任何可能会影响用户使用云服务的变更时，在计划变更日的 A 个工作日前以电话方式告知云服务客户，在云服务客户同意后进行变更。

11. 故障恢复能力

包括但不限于4.11节所要求内容。

示例 11：

服务商承诺由于统计或计费逻辑造成云服务不可用，可临时将统计计费下线优先保障客户的服务，系统架构设计上可以支持降级，保证服务运行。

12. 网络接入能力

包括但不限于4.12节所要求内容。

示例 12：

用户可以购买 xbps 到 ybps 的带宽，为 IDC 出口带宽。云服务的网络连接到 A 和 B 电信运营商。

13. 安全能力

包括但不限于4.13节所要求内容。

示例 13：

服务商承诺提供7×24小时的安全服务。

14. 计费条款

计费条款应包括以下内容：

——应明确计费方式与标准。

——应明确支付方式。

示例 14：

后付费模式，按照使用量以小时为单位计费，按照页面公布的当时有效的计费模式与标准为准。

15. 服务变更和终止条款

服务变更和终止条款应包括以下内容：

——应明确双方服务变更、终止的前提条件。

——应明确在满足前提条件下，双方应承担的权利和义务。

——应约定告知方式，确保双方能通知对方。

示例 15：

用户使用一段时间后觉得不满意，要求终止，需提前 2 个月告知，服务商将用户未消耗的余额返还给用户即可。另外一种是服务商不再提供服务，那么需要提前 2 个月通知客户转移服务，并返回用户未消耗的余额。

16. 服务赔偿条款

服务赔偿条款应包括以下内容：

——应承诺在某项服务指标没有达到服务协议中的要求时，提供相应的赔偿。

——应明确可获得赔偿的指标项，赔偿的具体方式，赔偿额度的计算方式，最低赔偿，最高赔偿等。

——应明确云服务方不承担责任的赔偿。

——由于用户自身操作不当导致的可用性不达标，可不承担赔偿责任。

示例 16：

服务商承诺用户如果可用性没有达到服务等级承诺，则会赔付相当于损失时间的相同时长。但由于用户自身操作不当导致的可用性不达标，则不承担赔偿责任。

17. 用户约束条款

用户约束条款应包括以下内容：

——应明确用户约束的范围，比如相关法律法规禁止的内容和行为。

18. 服务商免责条款

服务商免责条款应包括以下内容：

——应告知用户自身免责的条款，并将其以网站等方式对外正式公布，做到充分透明。

——免责条款应包括免责的范围和解释，免责的情景等信息。

示例 17：

因不可抗力或者其他意外事件，使得本服务条款的履行不可能、不必要或者无意义的，遭受不可抗力、意外事件的一方不承担责任。不可抗力、意外事件是指不能预见、不能克服并不能避免且对一方或双方当事人造成重大影响的客观事件，包括但不限于自然灾害如洪水、地震、瘟疫流行等以及社会事件如战争、动乱等。

参 考 文 献

[1] GB/T 22080-2008 信息技术 安全技术 信息安全管理体系要求
[2] GB/T 22081-2008 信息技术 安全技术 信息安全管理实用规则
[3] GB/T 31167-2014 信息安全技术 云计算服务安全指南
[4] GB/T 31168-2014 信息安全技术 云计算服务安全能力要求
[5] GB/T 31496-2015 信息技术 安全技术 信息安全管理体系实施指南
[6] GA/T 1390.2-2017 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
[7] JR/T 0071-2012 金融行业信息系统信息安全等级保护实施指引
[8] JR/T 0072-2012 金融行业信息系统信息安全等级保护测评指南
[9] JR/T 0073-2012 金融行业信息安全等级保护测评服务安全指引
[10] JR/T 0166-2018 云计算技术金融应用规范 技术架构
[11] JR/T 0167-2018 云计算技术金融应用规范 安全技术要求
[12] JR/T 0168-2018 云计算技术金融应用规范 容灾
[13] YDB 144-2014 云计算服务协议参考框架
[14] ISO/IEC TR 27015:2012 信息技术 安全技术 金融服务信息安全管理指南
[15] 保险公司信息系统安全管理指引（试行）（保监发〔2011〕68号）
[16] 保险业信息系统灾难恢复管理指引（保监发〔2008〕20号）