

面向保险行业的云服务提供方能力要求 (征求意见稿)

编制说明

中国信息通信研究院
2019年11月

《面向保险行业的云服务提供方能力要求》（征求意见稿）编制说明

一、工作简况

（一）任务来源

本标准由中国保险行业协会提出，于 2019 年 10 月获得了中国保险协会标准立项（立项号为 2019029-IAC）。

（二）协作单位

本标准由中国保险行业协会提出并归口。本标准的起草单位主要包括：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。

（三）主要工作过程

1、前期研究

1) 2017 年 9 月至 2019 年 3 月，起草组开展了六次保险行业云计算标准研讨会，起草组成员收集相关文献资料、政策文件、标准和数据，在前期调研及资料分析的基础上，依据 GB/T 1.1-2009《标准化工作导则 第 1 部分：标准的结构和编写规则》等标准编制要求，形成了《面向保险行业的云服务提供方能力要求》标准草案一稿。

2) 2019 年 4 月，中国保险行业协会在北京召开了保险行业云计算标准研讨会。期间，起草组成员对面向保险行业的云服务提供方能力要求和标准规范在研讨会上进行了详细的研讨，并提出了修改意见。

3) 2019 年 4 月至 9 月，起草组对标准草案进行了修订，形成《面向保险行业的云服务提供方能力要求》标准草案二稿。

2、标准计划申请

2019 年，开展了标准修订项目申报工作，提交了立项申请书初稿。并于 2019 年 10 月获批立项。

3、标准研制

2019 年 10 月，中国保险行业协会在北京召开了预审会，起草组成员来自保险企业、信息科技企业的数十位专家代表，对标准草稿的内容进行详细的讨论。形成了《面向保

险行业的云服务提供方能力要求》征求意见稿。

二、标准编制原则和确定标准主要内容

（一）制定原则

本标准面向保险行业的云服务提供方能力要求。本标准以通用性、实践性、规范性为原则，在编制过程中遵循：

1. 通用性原则。本标准为推荐性标准，应在全国范围内，考虑不同云服务提供方能力的共性要求提炼出来形成标准，以适应全国保险行业的特点。

2. 实践性原则。在切实做好本标准整体框架设计的基础上，以标准应用和指导服务实际工作为目标。编写过程中贯彻国家关于积极采用国际标准的政策，密切结合我国国情，从行业的实际水平出发，研究标准应规范的技术指标，做到技术先进合理、使用方便、切实可行。

3. 规范性原则。

标准按照 GB/T 1.1-2009《标准化工作导则 第1部分：标准的结构和编写》、GB/T 20000.2-2009《标准化工作指南 第2部分：采用国际标准》的要求和规定进行编写，保证标准形式和内容的规范性。

（二）制定论据

在本标准编制过程中，充分以现有国家法规、标准和监管相关规定为依据，并借鉴行业内多家保险公司的云计算搭建和建设的实务操作经验。

1、本标准主要参照了下列国家政策：

保险公司信息系统安全管理指引（试行）（保监发〔2011〕68号）

保险业信息系统灾难恢复管理指引（保监发〔2008〕20号）

2、本标准主要参照了下列标准：

GB/T 22080-2008 信息技术 安全技术 信息安全管理体系要求

GB/T 22081-2008 信息技术 安全技术 信息安全管理体系实用规则

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 31168-2014 信息安全技术 云计算服务安全能力要求

GB/T 31496-2015 信息技术 安全技术 信息安全管理体系实施指南

GB/T 32400-2015 信息技术 云计算 概览与词汇

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

JR/T 0071-2012 金融行业信息系统信息安全等级保护实施指引

JR/T 0072-2012 金融行业信息系统信息安全等级保护测评指南

JR/T 0073-2012 金融行业信息安全等级保护测评服务安全指引

JR/T 0166-2018 云计算技术金融应用规范 技术架构

JR/T 0167-2018 云计算技术金融应用规范 安全技术要求

JR/T 0168-2018 云计算技术金融应用规范 容灾

YDB 144-2014 云计算服务协议参考框架

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

(三) 主要技术内容

本标准主要对面向保险行业的云服务提供方能力要求进行规范。标准范围及主要技术内容如下：

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。

本标准的主要技术内容包括：

——范围

——规范性引用文件

——术语和定义

——保险业云服务提供方服务能力要求

——保险业云服务提供方资质要求

——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

——参考文献

三、主要试验(或验证)的分析、综述报告，技术经济论证，预期效果

(一) 主要试验的分析、综述报告

在信息化技术得到高速发展的当下，保险行业也进入了信息化高速发展的时期。所以，制定一套适合于我国保险业发展的云计算标准就显得尤为重要，加大和重视云计算

在保险行业的运用,可以在很大程度上减轻保险公司的人力资源,还可以节约公司的资金投入,为公司的发展注入强劲动力。

众多国家政策推动保险行业云计算的发展和建设。国务院于 2015 年发布的《关于积极推进“互联网+”行动的指导意见》明确指出了“互联网+”行动的指导意见,积极鼓励各金融机构利用云计算等技术手段,加快金融产品的服务创新。中国人民银行发布的《金融科技(FinTech)发展规划(2019-2021年)》也强调了在新一轮科技革命和产业变革的背景下,金融科技蓬勃发展,云计算等信息技术与金融业务深度融合,为金融发展提供的创新活力的重要性。中国银行保险监督管理委员会和中国人民银行联合发布的《2019年中国普惠金融发展报告》也明确指出了要积极引导企业借助云计算等现代信息技术手段提高服务质量,降低运营成本,创新普惠金融技术和产品。

随着近年来互联网的高速发展,互联网保险业务有了较强的发展,保险行业同时展现明显数字化的趋势。传统渠道业务占比呈逐年减少的态势,互联网业务占比呈逐年增加的态势。移动场景化成为消费者的主要行为特点,用户希望得到定制化的产品服务,同时对消费体验的诉求也在不断提高。

结合目前国内外在保险行业面向保险行业的云服务提供方能力要求的现状以及存在的问题,在标准制定过程中,对相关保险行业的特色属性进行了充分的调研和论证,主要体现在:

1. 针对保险行业面对的较严格合规性的监管要求和信息披露的特性,面向保险行业的云服务提供方提供的服务应具备可审查性。面向保险行业的云服务提供方由于合规或安全取证调查等原因按用户要求,在规定时间内应可以提供相关的日志等信息。云服务提供方还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管理委员会及其派出机构对接,遵从中国银行保险监督管理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管理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管理委员会要求,完成相关的问题整改。

2. 针对保险行业以客户为中心的经营模式,面向保险行业的云服务提供方提供的服务应具备高可用性,需可保证计算、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,还应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，来保障保险行业可靠高效的 7×24 小时运营。

3. 针对保险行业的产品业务变更迭代速率较快的特点，保险业云服务提供方应具备较高的变更协商权能力，保证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变更。例如，在计费系统规则出现变更时，应及时通知云服务用户。

4. 保险行业面临着非法接入、网络入侵、黑客攻击、病毒传播、DDoS 攻击等各种安全问题，其底层和其上的系统软件可能存在的安全漏洞将影响到整个平台系统的安全。针对保险行业用户及平台的信息与数据对于安全性要求较高的特点，面向保险行业的云服务提供方提供的服务应具备数据可持久的特性，定期对数据进行备份并保证数据在承诺范围内的保存不丢失，数据在通信、传输、存储的过程中还应保证私密性和完整性。

5. 中国银行保险监督管理委员会为完善信息系统安全保障体系，发布了《保险公司信息系统安全管理指引（试行）》，对通过管理机制和技术手段加强信息安全，保障保险行业业务连续性提出了详细的要求。包括建立覆盖网络、数据、存储、灾备等层面的安全事件管理及制度；按照等级保护管理要求实施信息系统安全等级保护；制定管理信息的采集、传输、交换、存储等环节的相关制度和流程，增强重要数据信息的控制和保护等要求。保险行业的云计算架构与部署应遵守《保险公司信息系统安全管理指引（试行）》中的各项要求，建立有效的评估审核流程与监督管理机制，定期对云服务提供方技术实力、安全资质、风险控制水平、诚信记录、财务状况等方面进行审查与评估，构建运维安全审计系统，建立完善的合规审查机制，以满足中国银行保险监督管理委员会等机构的监督检查。

6. 中国银行保险监督管理委员会为规范指导保险行业信息系统灾难恢复工作，提高防范灾难风险的能力，发布了《保险业信息系统灾难恢复管理指引》，对保险行业应统筹规划信息系统灾难恢复工作，达到相应最低灾难恢复能力等级提出了要求，包括对重要数据的备份和传输的安全管理的要求，保障数据的完整性要求；灾难备份中心建设和运行维护的要求；对灾难备份中心位置、人员、环境、网络通讯服务等内容的要求和灾难备份中心的自建、共建和外包等建设方式的要求。保险行业灾难备份中心的建设和管理，从硬件、机房、网络、系统运维、安全等方面均应满足中国银行保险监督管理委员会等机构对保险行业信息系统灾难恢复工作的监管要求。

（二）技术经济论证

随着互联网时代给保险公司带来的业务需求的变化,给 IT 系统需求的变化也会带来变化,包括快速的需求变化带来的快速响应和上线、用户访问不确定性导致的对弹性伸缩的需求和应用可用性要求高带来的对运维自动化的高要求。保险公司需要强大的技术力量来满足快速变化的客户偏好和 IT 系统需求,云计算可为保险行业提供支撑,适应互联网时代市场的快速变化。

当前保险行业云计算市场产品差异较大,试错成本较高。保险行业对 IT 系统的稳定性有着较高的要求,一旦出现宕机等事故将对保险公司的生产生活产生一定影响。相关监管要求趋于严格,落地情况也各有不同。虽金融行业相关监管机构已经有明确的政策支持金融机构 IT 系统使用云计算技术,但各家保险公司具体落地实施的程度不同。

(三) 预期效果

本标准起草过程中,与数十位来自于保险企业,信息科技企业的专家进行调研与讨论,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。能力要求主要包括数据持久性、数据可销毁性、数据可迁移性、数据安全隔离性、数据知情权、服务可审查性、服务功能、服务可用性、服务资源调配能力、变更协商权、故障恢复能力、网络接入能力、安全能力、服务计量准确性、服务协议规范性和服务可配合性等十五个方面。通过分析评估与调研,不断修改调整标准中的体系内容,最终形成了本标准。

为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做出具体指引要求,并给出服务协议参考架构。

四、与国外同类标准的对比分析

本标准为首次自主制定,不涉及国外标准采标情况。

五、与国家现行法规、标准的关系

无。

六、重大分歧意见的处理经过和依据

无。

七、标准作为强制性或推荐性标准的建议

本标准建议作为推荐性标准发布实施。

八、贯彻标准的要求和措施建议

建议本标准作为推荐性标准发布实施。本标准建立了面向保险行业的云服务提供方能力要求的管理规范，建议向保险行业积极推荐采用本标准。

同时，建议根据国家法规、标准和监管规定的变化情况，结合行业公司在标准实施过程中反馈的意见建议，适时对本标准进行修订完善。

九、废止现行有关标准的建议

无。

十、其他应予说明的事项

无。

中国信息通信研究院

2019. 11