云计算保险风险评估指引
（征求意见稿）

编制说明

中国信息通信研究院
2019年11月

《云计算保险风险评估指引》（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2019026-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，中国人民财产保险股份有限公司。

（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《云计算保险风险评估指引》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，起草组成员对云计算保险风险评估指引和标准规范在研讨会上进行了详细的研讨，并提出修改意见。

3）2019年4月至9月，起草组对标准草案进行了修订，形成《云计算保险风险评估指引》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《云计算保险风险评估指引》征求意见稿。为进一步明晰标准服务范围，建议将原《云计算风险评估方法》在征求意见稿时，更名为《云计算保险风险评估指引》。

二、标准编制原则和确定标准主要内容

（一）制定原则

本标准为云计算保险风险评估指引。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，考虑不同公司的云计算风险评估方法提炼出来形成标准，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。

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 信息安全管理实用规则

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

本标准主要对云计算保险风险评估方法进行规范。标准范围及主要技术内容如下：

本标准规定了云计算风险评估方法,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。

本标准适用于保险公司在云服务商为云平台投保时，由保险公司或第三方评估机构进行云服务商风险管理水平的评估，以作为投保的有效依据。

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

——概述

——风险评估

——(资料性附录) 云计算风险管理能力评估指标及权重

——(资料性附录) 风险评估结果

——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

云服务市场处于高速的发展阶段，预计未来几年将会保持稳定增长。近年来，以政企用户为主的云服务模式越来越多,国内公共云服务逐步从互联网向传统行业市场延伸。传统行业用户更加关心云服务不可用和存储数据丢失带来的经济损失，不管是云服务不能正常使用还是存储数据丢失，对企业级用户都将是重大事故。一方面，主流云服务商占据很大一部分市场，一旦云服务出现宕机，受有很大数量的企业收到影响；另一方面，随着越来越多的企业和政府将数据上云，宕机事故也能引发企业自身很大的灾难。因此，云服务存在的风险赔偿问题引起了各个企业的广泛关注。

随着近些年云风险事故的频发，安全问题成为企业上云的主要顾虑。保险机制能够

为云服务商和云客户提供切实的经济保障，在事故后将损失有效转嫁。国家和政府在推动企业上云的同时，也鼓励通过保险手段构建安全可控云计算产业体系。工信部印发的《推动企业上云实施指南（2018-2020）》第24条指出，应“积极探索利用保险模式对上云企业给予保障”。事后的云保险从用户角度评估云服务抵御服务不可用、数据丢失、信息泄露等风险管控的能力。

云保险是适应云计算服务不断发展特别是向传统产业加速延伸而开展的一种新探索，对于创建安全可信的云计算服务环境、培育云计算使用信心具有重要意义。支持产业界各方开展云保险服务实践，逐步扩大保障范围、扩展服务类型、完善政策环境，形成可复制可推广的云保险方案和政策经验。本标准服务于云保险，评估结果为确定云保险保费的重要依据。

（二）预期效果

本标准规定了云计算风险管理框架，针对云计算运行过程中面临的服务不可用、数据丢失、数据泄露等风险，提出了风险管理方法。云计算风险管理流程包括风险评估、风险处置、风险接受、风险沟通以及风险监视和评审等内容。适用于云计算企业对云计算涉及的系统、人员、管理制度进行风险管理，帮助云计算厂商控制云计算对外运营的风险，帮助云服务客户选择风险可控的云计算厂商。

通过事前评估，建立合理的风险管理组织架构，可以有效得规避风险。通过对云计算关键点包括基础设施、网络、计算资源、存储资源、应用、业务、数据、管理规范、运维运营、风险整合划分等进行识别，对风险管控措施进行识别，通过风险识别结果可估算出风险概率。

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。本标准建立了云计算保险风险评估方法的管理规范，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