ICS 35.240.40
A 11

JR

中华人民共和国金融行业标准

JR/T 0168—2018

云计算技术金融应用规范 容灾

Financial application specification of cloud computing technology——

Disaster recovery

2018-08-15 发布 2018-08-15 实施

中国人民银行 发布

目　　次

前　言

本标准是云计算技术金融应用系列标准之一，云计算技术金融应用系列标准包括：

——《云计算技术金融应用规范　技术架构》；

——《云计算技术金融应用规范　安全技术要求》；

——《云计算技术金融应用规范　容灾》。

本标准按照GB/T　1.1—2009给出的规则起草。

本标准由中国人民银行提出。

本标准由全国金融标准化技术委员会（SAC/TC 180）归口。

本标准负责起草单位：中国人民银行科技司、中国人民银行福州中心支行。

本标准参加起草单位：中国金融电子化公司、网联清算有限公司、中国互联网金融协会、中国人民银行泉州市中心支行、北京中金国盛认证有限公司、北京移动金融产业联盟、中金金融认证中心有限公司、北京银联金卡科技有限公司、北京软件产品质量检测检验中心、财付通支付科技有限公司、蚂蚁金融服务集团、华为技术有限公司、阿里云计算有限公司、北京百度网讯科技有限公司、新华三技术有限公司、万国数据服务有限公司、兴业数字金融服务（上海）股份有限公司、亚马逊通技术服务（北京）有限公司、北京京东金融科技控股有限公司、中国工商银行、中国农业银行、中国银行、中国建设银行、招商银行、中国光大银行、中国民生银行、平安银行、国泰君安证券股份有限公司、华泰证券股份有限公司、中国人寿保险（集团）公司、中国人民保险集团股份有限公司、中国银联股份有限公司、天津麒麟信息技术有限公司、北京三快云计算有限公司。

本标准主要起草人：李伟、李兴锋、邬向阳、张宏基、班廷伦、强群力、杨倩、聂丽琴、林光丰、郭林、胡达川、朱勇、周国林、辛路、杨彬、陈则栋、林羽、段家钦、傅凯铮、吴永强、吴金海、白阳、于柳绮、张文涛、符海芳、汪琪、高勇、赵华、郭红英、高志民、高强裔、金怡、孔令斌、杜辉、居未伟、李明凯、王晓燕、张亮、刘刚、杨俊、郝轶、陈当阳、樊华、罗子强、雷佳杰、许涛、王绍斌、张荣典、燕冰、曹辉、董亮、苏晗、赵春华、高天游、司渤洋、来宾、种毓鑫、李澍、张洁、陈晨、章彩红、刘永福、穆冬生、宋杰、瞿红来、黄超、高坤、李荣振、李宝、巩向锋、李国光、谭晓辉、王仕、王研娟、林春、周亚国、张洋洋、张翰林。

云计算技术金融应用规范　容灾

1　范围

本标准规定了金融领域云计算平台的容灾要求，包括云计算平台容灾能力分级、灾难恢复预案与演练、组织管理、监控管理、监督管理等内容。

本标准适用于金融领域的云服务提供者、云服务使用者、云服务合作者等。

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 20988—2007　信息安全技术　信息系统灾难恢复规范

GB/T 22240—2008　信息安全技术　信息系统安全等级保护定级指南

GB/T 30146—2013　公共安全　业务连续性管理体系　要求

JR/T 0044—2008　银行业信息系统灾难恢复管理规范

JR/T 0166—2018　云计算技术金融应用规范　技术架构

3　术语和定义

JR/T 0166—2018界定的以及下列术语和定义适用于本文件。

3.1

灾难　disaster

由于人为或自然的原因，造成信息系统严重故障、瘫痪或其数据严重受损，使信息系统支持的业务功能停顿或服务水平达到不可接受的程度，并持续特定时间的突发性事件。

[JR/T 0044—2008，定义3.2]

3.2

容灾　disaster recovery

灾难恢复

为了将信息系统从灾难造成的不可运行状态或不可接受状态恢复到可正常运行状态，并将其支持的业务功能从灾难造成的不正常状态恢复到可接受的状态而设计的活动和流程。

[JR/T 0044—2008，定义3.3]

3.3

风险分析　risk analysis

确定影响信息系统正常运行的风险，评估对单位业务运营至关重要的功能，定义降低潜在危险控制手段的流程。风险分析经常会涉及到对特殊事件发生可能性的评估。

[JR/T 0044—2008，定义3.6]

3.4

业务影响分析 business impact analysis

分析业务功能及其相关信息系统资源，评估特定灾难对各业务功能的影响。

[JR/T 0044—2008，定义3.7]

3.5

业务连续性 business continuity

在中断事件发生后，组织在预先确定的可接受的水平上连续交付产品或提供服务的能力。

[GB/T 30146—2013，定义3.3]

3.6

恢复时间目标 recovery time objective

灾难发生后，信息系统从停顿到必须恢复的时间要求。

[JR/T 0044—2008，定义3.17]

3.7

恢复点目标 recovery point objective

灾难发生后，数据必须恢复到的时间点要求。

[JR/T 0044—2008，定义3.18]

3.8

系统可用性 system availability

指在要求的外部资源得到保证的前提下，云服务在规定的条件下和规定的时刻或时间区间内（不包括计划内服务中断时间）处于可执行规定功能状态的能力，一般按允许计划外年服务中断时间、可用程度至少达到“n个9”来衡量。

3.9

可用区 availability zone

在云计算平台中，综合考虑电力、网络、供水等基础设施的容灾因素划分出来的物理区域，区域内包含空调、电力设施、主机、网络、存储等物理资源。

3.10

同城可用区 availability zone in the same region

能够抵御因供电供水中断、水淹、火灾、网络故障、硬件损毁、交通中断等灾难同时影响的两个可用区互为同城可用区。一般情况下两同城可用区之间地理距离为数十公里。

3.11

异地可用区 availability zone in the different region

能够抵御因战争、洪水、海啸、台风、地震等大范围区域性灾害同时影响的两个可用区互为异地可用区。一般情况下两异地可用区之间地理距离为数百公里以上。

3.12

演练 exercise

为提高灾难恢复能力，基于灾难恢复预案进行的演习，形式包括桌面演练、模拟演练、实战演练等。

4 缩略语

下列缩略语适用于本文件。

RPO 恢复点目标（Recovery Point Objective）

RTO 恢复时间目标（Recovery Time Objective）

5 概述

近年来，云计算技术在金融领域应用逐渐深入，深刻影响和变革了金融机构的技术架构、服务模式和业务流程，但也给灾难恢复带来了新的挑战。由于多租户、虚拟化、资源池等技术特性，云计算平台在灾难恢复的影响评估、关键指标、技术要求、组织管理等方面与传统架构存在诸多差异，应重点关注并妥善应对。云计算平台本质上仍是一种信息系统，应满足国家和金融行业信息系统灾难恢复相关要求，本标准重点提出了体现云计算特性的差异化容灾要求。

6 云计算平台容灾能力分级

6.1 风险与业务影响分析

金融机构应根据业务连续性目标和业务发展规划，对云计算平台进行详细的风险分析。在风险分析过程中，云服务提供者、云服务使用者和云服务合作者应根据当前的业务场景，重点界定风险分析的目标和范围，使用恰当的分析方法，对所面临的威胁和当前体系的脆弱性进行深入剖析，评估各类风险发生的概率和可能导致的损失。

在金融领域云计算环境下，风险分析应重点关注使用云计算技术可能引发的新风险、威胁、脆弱性和损害，包括但不限于以下方面：

——云计算环境下多租户的资源竞争可能导致的系统服务能力下降或不可用。

——云计算环境下隔离措施不当可能导致的信息泄露。

——云计算环境下单点设备或性能瓶颈可能导致的系统中断。

——云计算环境下自服务管控不足可能导致的资源和信息滥用。

——云计算环境下系统故障、升级等可能导致的问题群发。

经过严谨的风险分析之后，需要对风险可能造成的业务影响进行研判。在对业务影响进行分析时，首先需要根据监管要求、业务性质、业务服务范围、数据集中程度、业务时间敏感性、功能关联性等要素进行业务功能分析，并在此基础上评估业务中断可能造成的影响，确定灾难恢复目标及恢复优先级。

在金融领域云计算环境下，业务影响分析应关注的内容包括但不限于以下方面：

——对于可能造成多个金融应用同时遭受灾难的，要综合评估云计算平台的影响。

——由于应用和数据部署的实际物理设备的不确定性，导致的同一故障影响的不确定性。

6.2 容灾能力级别划分

根据 GB/T 20988—2007、JR/T 0044—2008、GB/T 22240—2008 的相关要求，按照所承载的业务系统发生故障或瘫痪的影响范围、危害程度等对云计算平台容灾能力要求进行划分。

结合金融领域特性，将云计算平台发生故障或瘫痪的影响范围分为 4 个层级：

——内部辅助管理：未对金融机构经济效益、社会声誉产生直接影响的内部管理事项。

——内部运营管理：对金融机构经济效益、社会声誉产生直接影响的内部管理事项。

——公民、法人和其他组织的金融权益，包括：

- 公民、法人和其他组织的财产安全权、知情权、公平交易权、依法求偿权、信息安全权；
- 其他影响公民、法人和其他组织的金融权益的事项。

——国家金融稳定、金融秩序，包括：

- 国家对外活动中的经济金融利益；
- 国家金融政策的制定与执行；
- 国家金融风险的防范；
- 国家金融管理活动；
- 多数关键金融机构、金融市场及其基础设施的稳定运行；
- 其他影响国家金融稳定、金融秩序的事项。

将云计算平台发生故障或瘫痪的危害程度划分为 3 类：

——较小影响，指的是工作职能受到局部影响，业务能力有所降低但不影响主要功能的执行，出现较轻的法律问题，较低的财产损失等。

——一般影响，指的是工作职能受到一般影响，业务能力显著下降且影响主要功能执行，引发一般的法律问题，较高的财产损失等。

——严重影响，指的是工作职能受到严重影响或丧失行使能力，业务能力严重下降或功能无法执行，出现严重的法律问题等。

根据应用于金融领域的云计算平台发生故障或瘫痪的影响范围、危害程度，将其容灾能力等级划分为 6 级，具体如表 1 所示。考虑应用于金融领域云计算平台的重要性和发生故障或瘫痪的影响程度，应用于金融领域云计算平台至少应达到容灾能力 3 级要求。

表1　应用于金融领域的云计算平台容灾能力等级要求划分

影响范围	危害程度		
	较小影响	一般影响	严重影响
内部辅助管理	第 1 级	第 2 级	第 3 级
内部运营管理	第 2 级	第 3 级	第 4 级
公民、法人和其他组织的金融权益	第 3 级	第 4 级	第 5 级
国家金融稳定、金融秩序	第 4 级	第 5 级	第 6 级

6.3　关键指标

应用于金融领域的云计算平台应至少达到容灾能力 3 级要求，对应的 RTO、RPO、可用性等关键指标要求如表 2 所示。

表2　应用于金融领域的云计算平台容灾能力等级关键指标要求

容灾等级	RTO	RPO	可用性
3 级	≦24 小时	≦24 小时	每年非计划服务中断时间不超过 4 天，系统可用性至少达到 99%。
4 级	≦4 小时	≦1 小时	每年非计划服务中断时间不超过 10 小时，系统可用性至少达到 99.9%。

容灾等级	RTO	RPO	可用性
5 级	≦30 分钟	≈0	每年非计划服务中断时间不超过 1 小时，系统可用性至少达到 99.99%。
6 级	≦2 分钟	0	每年非计划服务中断时间不超过 5 分钟，系统可用性至少达到 99.999%。

6.4 技术要求

本标准按照 GB/T 20988—2007 有关内容，从数据备份、数据处理、网络能力和运维能力 4 个要素给出云计算平台容灾能力等级相关技术要求。金融领域云计算平台至少应达到容灾能力 3 级要求，相应等级的具体技术要求详见表 3 至表 6。

表3 第6级技术要求

要素	云计算相关要求
数据备份	a）数据应在同城和异地可用区至少各有一个数据副本； b）数据副本实时备份且至少一个数据副本应同步复制，保障数据一致性； c）完全数据备份至少每天一次且处于异地可用区。
数据处理	a）备用数据处理系统的主机、虚拟化平台、操作系统、中间件、应用软件等资源与生产数据处理系统完全兼容； b）在异地和同城可用区均具备与生产数据处理系统相一致的备用数据处理能力，并处于运行状态，可实时无缝切换； c）应确保备用数据处理系统具备与生产数据处理系统相同的高可用特性。
网络能力	a）提供充足的网络带宽，保证备份数据传输带宽大于业务峰值所需的带宽需求； b）异地和同城可用区的虚拟网络、物理网络、出口网络带宽及链路配置与生产系统的网络能力相同，并处于运行状态； c）支持跨异地和同城可用区的负载均衡。
运维能力	a）云计算平台应能够对灾备能力进行集成管理，支持通过可定制的标准化流程完成流量自动或集中切换，支持跨同城和异地可用区的流量均衡配置； b）灾难事件发生后，备份数据中心的云计算资源管理和调度平台仍可完成对备份数据中心的资源管理和调度； c）对生产系统关键运行状态进行实时监控和告警； d）云计算平台需要为关键的用户运营数据，如审计日志等，提供数据备份。

表4 第5级技术要求

要素	云计算相关要求
数据备份	a）数据应在同城和异地可用区至少各有一个数据副本； b）至少存在一个数据副本应同步复制，保障数据一致性；

要素	云计算相关要求
	c）完全数据备份至少每天一次且处于异地可用区。
数据处理	a）备用数据处理系统的主机、虚拟化平台、操作系统、中间件、应用软件等资源与生产数据处理系统完全兼容； b）在异地和同城可用区均具备与生产数据处理系统相一致的数据处理能力，至少有一个处于运行状态，并可实现无缝切换； c）应确保备用数据处理系统具备与生产数据处理系统相同的高可用特性。
网络能力	a）提供充足的网络带宽，保证备份数据传输带宽满足业务峰值所需的带宽需求； b）异地和同城可用区的虚拟网络、物理网络、出口网络带宽及链路配置与生产系统的网络能力相同，并至少有一个处于运行状态； c）支持跨异地或同城可用区的负载均衡。对于处于就绪状态的可用区，应支持跨可用区的自动或集中切换。
运维能力	a）云计算平台应能够对灾备能力进行集成管理，支持通过可定制的标准化流程完成流量自动或集中切换； b）灾难事件发生后，备份数据中心的云计算资源管理和调度平台仍可完成对备份数据中心的资源管理和调度； c）对生产系统关键运行状态进行实时监控和告警； d）云计算平台需要为关键的用户运营数据，如审计日志等，提供数据备份。

表5　第4级技术要求

要素	云计算相关要求
数据备份	a）至少有一个数据副本处于异地可用区； b）完全数据备份至少每天一次且处于异地可用区。
数据处理	a）在异地可用区具备灾难恢复所需的全部备用数据处理能力，并处于就绪状态或运行状态，并且可自动或集中切换； b）应确保备用数据处理系统具备与生产数据处理系统相同的高可用特性。
网络能力	a）异地可用区的虚拟网络、物理网络、出口网络带宽及链路配置与生产系统的网络能力相同，并处于就绪状态； b）应支持跨可用区的自动或集中切换。
运维能力	a）云计算平台应能够对灾备能力进行集成管理，支持通过可定制的标准化流程完成流量集中切换； b）灾难事件发生后，备份数据中心的云计算资源管理和调度平台仍可完成对备份数据中心的资源管理和调度； c）对生产系统关键运行状态进行实时监控和告警； d）云计算平台需要为关键的用户运营数据，如审计日志等，提供数据备份。

表6　第3级技术要求

要素	云计算相关要求
数据备份	a）关键数据至少有一个数据副本处于异地或同城可用区； b）完全数据备份至少每天一次且处于同城或异地可用区。
数据处理	a)在异地或同城可用区具备灾难恢复所需的部分备用数据处理能力； b）应确保云计算资源调度能力满足在数小时内配备灾难恢复所需的全部备用数据处理能力。
网络能力	a）应确保异地或同城可用区的虚拟网络、物理网络、出口网络带宽及链路配置在数小时内达到与生产系统的网络能力相同,关键资源处于就绪状态； b）应支持跨可用区的自动或集中切换。
运维能力	a）云计算平台应能够对灾备能力进行集成管理，具备流量集中切换能力； b）灾难事件发生后，备份数据中心的云计算资源管理和调度平台仍可完成对备份数据中心的资源管理和调度； c）云计算平台需要为关键的用户运营数据，如审计日志等，提供数据备份。

7　预案与演练

7.1　灾难恢复预案的制定

灾难恢复预案应包括应急和系统灾难恢复两部分。

——应急部分包括但不限于以下内容：

- 灾难场景和范围定义；
- 应急的管理机构和决策机制；
- 应急响应的流程、工具和工作制度。

——系统灾难恢复部分包括但不限于以下内容：

- 灾难恢复的范围和目标；
- 灾难恢复的总体规程；
- 各系统恢复的切换步骤、操作手册和业务功能恢复验证测试方法。

7.2　灾难恢复演练和预案管理

在云计算环境下，灾难恢复演练主要是为了验证灾难恢复预案的完整性和有效性，提高预案的执行能力，确保云服务各参与方在灾难发生时的有效协同，以及业务系统的快速恢复。具体的灾难恢复演练和预案管理要求应遵循 GB/T 20988—2007，并满足以下要求：

——云服务提供者、云服务合作者应根据云服务使用者的要求，及时提供技术和管理支持，配合执行相关演练。

——云服务提供者应至少每年进行一次相关预案的更新和演练。

8　组织管理

在灾难发生后，云服务各参与方应依据灾难实际影响，按照预先制定的灾难恢复预案密切配合、有序开展灾难恢复工作，包括但不限于：

——应确保灾难影响、应对措施、恢复进度等信息在各参与方之间及时、有效、准确的沟通和传递，重大或特别重大的事件应及时向相关主管部门和监管机构报告。

——灾难恢复完成后应及时总结经验教训，并及时告知受影响的用户。

——应定期进行灾难恢复的培训并保存培训记录。

9 监控管理

9.1 监控能力

云计算环境的灾难恢复应具备的监控能力，包括但不限于：

——应实时监控生产中心和灾备中心的业务应用可用性和性能状态。

——应能够有效监控灾备切换过程。

——应能够监控灾备同步状态。

——应具备告警功能。

9.2 监控职责

云计算平台应对灾难恢复系统的日常生产维护工作进行监控，包括但不限于：

——应监控云计算平台资源的运行状态并主动进行优化。

——应执行云计算平台资源的日常操作、维护工作和升级工作。

——应解决云计算平台资源的基础架构的故障和问题。

10 监督管理

10.1 审计

审计包括内部审计和外部审计，内部审计由云服务提供者或云服务使用者的内部人员或部门承担，外部审计由具有国家相应监管部门认定资质的中介机构组织实施。在金融领域云计算环境下，除了GB/T 20988—2007所要求的相关内容，还应重点加强对如下问题的审计：

——灾难恢复过程中云服务提供者、云服务使用者、云服务合作者之间协同是否顺畅，是否能满足不同灾难恢复需求。

——是否具备系统全流程和全环境的监控预警体系。

——是否在机制和技术架构上存在数据同步的缺陷。

——组织和流程上是否充分保证了云服务使用者的知情权和参与权。

——灾难恢复流程是否存在数据泄露的风险。

审计要求如下：

——云服务提供者应根据灾难恢复工作的情况，确定灾难恢复审计的频率，且应至少一年进行一次内部审计。

——云服务提供者应至少每年提供一次更新的预案、演练记录和报告给相关金融机构进行备案或审计。

——云服务提供者应至少每年组织一次内部审计或委托第三方进行的审计，并将审计意见、改进计划和改进结果在审计报告完成后及时交付给云服务使用者。

——云服务使用者应至少每三年组织一次对云服务提供者的审计，审计可以由云服务使用者组织也

可以由云服务使用者委托第三方独立审计机构组织。

——云服务提供者在审计报告出具后应及时对审计报告提出的改进意见给出书面答复，答复的内容至少应包括改进计划、改进措施和历次改进计划的执行情况。

10.2 通知通报

应通知各云服务参与方的情况，包括但不限于：

——需要共同协作的演练。

——发生重大事件或面临重大风险。

——需要相关方共同调整方法、流程和协作渠道。

应报告监管机构的情况，包括但不限于：

——可能影响多个金融机构的重大风险。

——涉及多个金融机构的重大事故处置情况。

——灾难性事件的处置情况报告。