ICS 03.060
A 11

IAC

中 国 保 险 行 业 协 会 标 准

T/IAC 7—2017

保险业灾备建设基本要求

Basic requirement of the construction of disaster prevention in insurance industry

2017-12-29 发布　　2018-06-12 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:阳光保险集团股份有限公司、中国太平洋保险(集团)股份有限公司、中国人民保险集团股份有限公司。

本标准主要起草人:刘洋、陈羊羊、刘强、关胜。

引　言

随着保险业务快速增长，业务运营与创新对信息系统的依赖越来越强，数据集中带来的数据中心风险高度集中，为有效防范保险业信息系统风险，保护行业客户的合法权益，有必要对灾难备份中心的建设进行要求和规范，为保险业灾备中心建设提供指导和借鉴。

保险业灾备建设基本要求

1 范围

本标准规定了保险业灾难备份建设的基本原则、基本内容、工作流程、机构与人员、建设要求和日常运维要求。

本标准适用于保险业灾难备份的建设与管理。

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 9361—2011 计算机场地安全要求

3 术语和定义

下列术语和定义适用于本文件。

3.1

恢复时间目标 recovery time objective；RTO

灾难发生后，信息系统或业务功能从停顿到必须恢复的时间要求。RTO 取值越小，表示业务连续性管理系统的业务恢复能力越强。

3.2

恢复点目标 recovery point objective；RPO

灾难发生后，系统和数据必须恢复到的时间点要求。RPO 指标主要反映业务连续性管理体系下备用数据的时效性，RPO 取值越小，表示系统对数据完整性的保护能力越强。

4 概述

4.1 灾备建议的基本原则

4.1.1 适用性

灾备建设前，应制定灾备建设策略与规划，策略和规划应符合信息系统现状、符合业务发展和 IT 建设需要。

4.1.2 一体化

灾备建设时，数据与系统应进行灾难备份，并规范灾难恢复管理流程，实现生产与灾备系统一体化管理。

4.1.3 可靠性与稳定性

灾备系统作为生产的备用系统，在生产中心发生意外时可能接管业务运行，并持续一定时间。灾备

系统需具备与生产环境相当的可靠性与稳定性。

4.1.4 扩展性

在系统规划与策略设计时应考虑系统扩容因素和体系扩容演进方法。

4.1.5 生产灾备同步性

灾备系统规划应与生产环境规划保持同步性。

4.2 灾备建设的基本内容

4.2.1 灾备建设的基本内容包括：

a) 数据备份系统；
b) 备用数据处理系统；
c) 备用网络系统；
d) 备用基础设施；
e) 专业技术支持能力；
f) 运行维护能力等。

4.2.2 数据备份系统主要包括但不限于：

a) 数据备份硬件；
b) 数据备份软件；
c) 数据备份介质；
d) 依靠电子传输的数据备份系统，主要包括：数据备份线路、相应的通信设备。

4.2.3 备用数据处理系统主要包括但不限于：

a) 备用计算机；
b) 外围设备；
c) 软件。

4.2.4 备用网络系统是指最终用户用来访问备用数据处理系统的网络，主要包括但不限于：

a) 备用网络通信设备；
b) 备用数据通信线路。

4.2.5 备用基础设施是指恢复所需的并能够支持灾备系统运行的建筑、设备和组织，主要包括但不限于：

a) 介质的场外存放场所；
b) 备用的机房；
c) 灾难恢复工作辅助设施；
d) 容许灾难恢复人员连续停留的生活设施。

4.2.6 专业技术支持能力是指为灾备系统的运转提供支撑和综合保障的能力，以实现灾备系统的预期目标，主要包括但不限于：

a) 硬件、系统软件和应用软件的问题分析和处理能力；
b) 网络系统安全运行管理能力；
c) 沟通协调能力。

4.2.7 运行维护管理能力主要包括但不限于：

a) 运行环境管理；
b) 系统管理；
c) 安全管理；

d） 变更管理。

4.3 灾备建设的工作流程

4.3.1 灾备建设阶段划分

根据灾备建设工作的目标和侧重点，灾备工作主要包括以下阶段：

a） 分析阶段；

b） 设计阶段；

c） 实施阶段。

4.3.2 分析阶段

分析阶段主要是对灾害潜在损失、各种影响及现行恢复能力等方面定性及定量分析评估，包含风险分析、业务影响分析、恢复能力评估等内容。分析阶段应符合以下要求：

a） 对于保险业核心业务系统及部分周边系统的应用级灾备，要求业务能够在 RTO 规定时间内，启动灾备中心并能够持续运行，根据 RPO 要求选择适当的数据复制或备份策略；

b） 对于数据级灾备的业务系统，要求灾备中心能够获得生产系统数据，数据差异满足 RPO 要求，应进行数据可用性校验，服务器及网络环境满足系统运行要求后，能够恢复业务的运行。

4.3.3 设计阶段

设计阶段应根据分析阶段结果制定组织恢复策略，提供为实现组织业务持续所必需的解决方案和实施计划，达到组织在人员结构、流程及技术等层面的恢复需求。设计阶段应符合以下要求：

a） 建立覆盖日常管理、应急响应、切换回切操作、演练管理的全面的灾难恢复流程；

b） 应急响应和切换回切操作流程应满足 RTO 和 RPO 要求；

c） 保证流程可操作性和正确性。

4.3.4 实施阶段

实施阶段主要包括建立灾难恢复预案、实施灾难恢复预案的桌面演练、执行灾难恢复预案及灾难恢复测试、执行灾难恢复预案维护方案。

5 机构与人员

5.1 组织机构

5.1.1 应建立灾备恢复组织机构，灾难恢复组织机构包括且不限于：

a） 灾难恢复领导小组；

b） 灾难恢复实施及运维小组。

5.1.2 灾难恢复机构的具体情况需要在灾难恢复计划中准确说明。

5.1.3 灾难恢复的职能架构和职责必须先定义，其中一些职位可由多人担任，一些人可负责两种或多种职责。灾备职能架构可以是常设机构，也可以是根据灾难恢复规划的要求临时设立。

5.2 组织职责

5.2.1 灾难恢复领导小组

灾难恢复领导小组是灾难恢复工作的组织领导机构，组长应由公司的最高管理层成员担任，主要职责是领导和决策灾难恢复的重大事宜，制订灾难恢复体系的目标。

5.2.2 灾难恢复管理小组

灾难恢复管理小组是常设办公机构，向上对灾难恢复领导小组提出审批要求，向下负责灾难恢复体系的日常管理工作。

5.2.3 灾难恢复日常运行小组

灾难恢复日常运行小组支持灾备中心日常运维的管理，为灾难恢复提供技术支持，同时在灾难发生后，执行系统恢复、业务恢复、外部协作等具体工作事项。

6 灾备建设要求

6.1 灾备资源要求

6.1.1 灾备中心场地资源要求

根据监管单位《保险业信息系统灾难恢复管理指引指引》要求，灾难备份中心机房环境应达到GB/T 9361—2011 中 B 类机房标准。

6.1.2 灾备中心地理位置建设要求

同城灾备中心应能够抵御小范围区域内的灾难，异地灾备中心应能够抵御较大范围区域内的灾难，距离应由灾备等级和灾备目标等确定。

6.1.3 灾备中心运维要求

灾备架构中关键的数据复制备份过程以及生产灾备一体化运维应由保险公司确定的灾备岗位负责和管理，对于灾备中心应用级灾备的业务层面运维由保险公司信息技术人员或运维人员远程访问方式实施。

6.1.4 灾备中心恢复预案要求

灾难恢复预案框架的开发、制定、桌面演练及预案管理制度应由保险公司信息技术人员及相关业务部门人员提供必要的协助支持。

预案的落实（基于灾备技术方案实现的灾备切换操作流程）、维护更新及实际灾备演练，由保险公司灾难恢复组织内定义的相关岗位负责组织与实施。

6.2 灾备系统基础架构技术要求

6.2.1 数据备份与数据复制要求

根据监管机构相关要求，确定不同应用系统的灾备等级与灾备目标。根据不同的灾备指标组合，宜采取适当的数据复制技术策略支持，降低建设、运维成本以及系统技术复杂性。

6.2.2 灾备系统网络建设要求

灾备系统部署须具备涉及业务系统所需的基础网络、内部分支公司的广域网链路、外联单位的广域网链路，以保证发生灾难切换后，业务系统能够为相关内联机构、外联机构提供业务访问和服务。

灾备中心的网络应参考生产中心的建设标准、网络架构、区域划分，考虑网络的可靠性、冗余性、安全性、扩展性，以提供业务支撑为目标的策略规划。

6.2.3 应用部署要求

灾备中心与生产中心应用系统版本须保持一致，可以适当降低高可用性和承载能力要求。

6.2.4 主机及虚拟化建设要求

灾备中心主机的部署要求以能接管业务为标准，同时注重节约建设和运营成本。

6.2.5 存储部署要求

灾备中心的存储要求可用存储空间至少应与生产中心一致，当生产中心的应用对存储提出更多容量空间要求时候，容灾中心同样能够满足变更条件。

6.2.6 主备系统时间同步要求

灾备中心和主中心须引入时间同步功能模块，保证主备中心的相关服务器的系统时间同步。

6.2.7 主备系统联动变更要求

灾备体系至少是由主备中心两套以上 IT 基础架构组成，关键 IT 元素在主备中心的“对称性部署”，是保证灾备系统随时具备切换和回切能力的必要条件。

6.2.8 灾备系统切换要求

灾备系统切换需满足 RTO 和 RPO 指标要求，按照切换预案及既定步骤操作，并制定应急预案处理切换过程中出现的异常情况。所有灾备切换操作应统一指挥，对整个切换过程的指令及执行情况进行详细记录。

6.2.9 灾难恢复流程要求

灾备中心除与生产中心执行相同的日常运维流程外，还需制定一套生产与灾备环境的灾难恢复流程，指导灾难发生时的数据中心间业务系统的切换。保险业在灾难恢复阶段需要考虑从应急响应，到灾难切换和计划回切的整体流程。

7 灾备中心日常运维要求

7.1 应急响应要求

7.1.1 发布应急通告

应在灾难即将或刚发生时发布应急通告。应急通告流程需要明确规定通知流程、通知策略和通知内容等。通知中所传递的信息类型和内容应明确清晰，所传递的信息数量和详细程度可依据被通知的对象确定。

7.1.2 损害评估

灾难发生时，损害评估人员应尽快到达灾难现场查看灾难状况和确定事态的严重程度，召集相应的专业人员对灾难事件进行评估，确认灾难对信息系统造成的影响，确定下一步行动。

损害评估结果确定后，应将最新信息按照预定通告流程通知相应的团队。

7.1.3 灾难决策

制定灾难决策时应确定灾难恢复计划启动的条件。当损害评估结果达到一项或多项启动条件时，

将由被保险公司授权的人员正式发出灾难宣告。

启动条件的确定宜基于以下方面：

a） 评估损失状况；

b） 执行灾难恢复流程的资源需求；

c） 损失是否足以构成立即宣布灾难；

d） 转移至灾备中心是否比修复花费更多时间；

e） 灾备中心系统运行的健康状态；

f） 受影响的关键服务的恢复时间。

7.1.4 灾难宣告

灾难宣告是区分灾难和一般性应急问题的重要标识。灾难的正式宣告要求保险公司内部相关部门提供恢复所需的资源决策。

根据灾难决策的结果，由被授权的灾难宣告人员发出灾难宣告，宣布启动灾难恢复计划，并通知各有关部门。

7.2 灾难切换

在切换复杂系统时，如涉及多个独立应用系统的业务系统，切换进程应反映出业务影响分析中所确定的系统优先顺序，优先恢复重要和关键的系统。

7.3 灾难恢复演练要求

保险公司每年至少执行一次模拟演练或一次真实演练，确保灾备系统有效性。

参 考 文 献

[1] GB/T 20988—2007 信息安全技术 信息系统灾难恢复规范.
[2] 中国保险监督管理委员会.关于做好保险信息系统灾难备份工作的通知(保监发[2004]127号).
[3] 中国保险监督管理委员会.保险公司信息系统安全管理指引(保监发[2011]68号).
[4] 中国保险监督管理委员会.保险公司开业验收指引(保监发[2011]14号).
[5] 中国保险监督管理委员会.保险业信息系统灾难恢复管理指引(保监发[2008]20号).