ICS 35.020
L 80

DB37

山　东　省　地　方　标　准

DB37/T 2636—2014

信息安全技术　信息系统灾备服务规范

2014-12-15 发布　　2015-01-15 实施

山东省质量技术监督局　发布

前　言

本标准按照GB/T 1.1—2009给出的规则起草。

本标准由山东省信息标准化技术委员会提出并归口。

本标准起草单位：山东省计算中心（国家超级计算济南中心）、山东省数据灾备服务中心、山东华迪智能技术有限公司、华为技术有限公司、山东亿云信息技术有限公司、威海北洋电气集团股份有限公司、山东正中计算机网络技术咨询有限公司。

本标准主要起草人：李刚、周鸣乐、顾卫东、王平、李旺、李钊、孙忠周、冯正乾、刘瑜、田松、王玮、刘波、杨晓晖、李敏、金峰、宋佐江、刘文臣、朱勇。

引　言

信息系统灾备建设完成后，信息系统灾备服务是确保系统可用性、进行数据备份、确保灾难备份网络系统的可用性、支持运营管理的最有效手段，本标准对信息系统灾备服务进行研究，制定明确、合理的信息系统灾备服务规范，指导灾备服务的实施，保证信息系统灾备服务的可用性、稳定性和持续性。

信息安全技术　信息系统灾备服务规范

1　范围

本标准规定了信息系统灾备服务的术语和定义、参考模型、服务准备、灾难备份服务、灾难应急处置服务、灾难恢复服务、演练服务、服务总结与维持。

本标准适用于提供信息系统灾备服务的机构（以下简称“机构”）及灾备需求用户（以下简称“用户”）。

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 20988—2007　信息安全技术　信息系统灾难恢复规范

3　术语和定义

GB/T 20988—2007中确立的以及下列术语和定义适用于本文件。

3.1

信息系统灾备服务

能满足用户在灾难发生时，对数据和系统恢复所提供的一种保障。

3.2

信息系统灾难应急处置

为了应对灾难的发生所做的准备，以及在灾难发生后所采取的措施。

4　灾备服务参考模型

为保障信息系统灾备服务的顺利进行，本标准的主要内容包括如下几个方面，关系如图1所示：

a)　对信息系统灾备服务准备内容作出一般性规定，包括灾备服务内容、服务项目组、灾难恢复能力等级、灾备预案、环境建设、培训和咨询；

b)　对信息系统灾备服务实施内容作出一般性规定，包括灾难备份服务、灾难应急处置服务、灾难恢复服务和演练服务；

c)　对信息系统灾备服务总结内容作出一般性规定，包括服务总结、体系维护和体系审核。

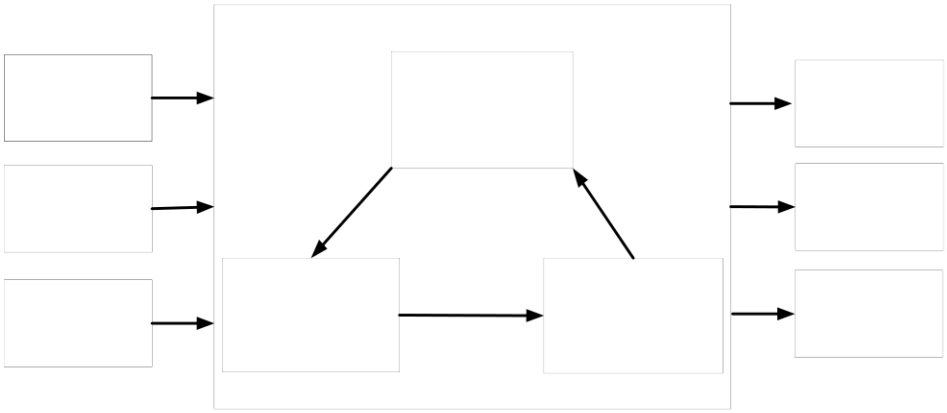

图1　信息系统灾备服务参考模型

5　灾备服务准备

5.1　服务内容确定

5.1.1　机构在提供灾备服务前，应就灾备服务内容与用户达成一致。

5.1.2　灾备服务内容应包括：

a)　机构进行灾备服务的目标；

b)　机构进行灾备服务的原则；

c)　机构进行灾备服务的范围；

d)　用户信息系统的灾难恢复能力等级；

e)　机构与用户的沟通方式与沟通内容。

5.1.3　机构与用户应按照约定时间对灾备服务内容进行评审。当用户业务环境发生变化时，机构与用户应对灾备服务内容进行调整。

5.2　服务项目组建立

5.2.1　为确保提供的信息系统灾备预案在灾难应急处置及恢复阶段被有效运行，机构应建立内部灾备服务项目组，明确规定灾备服务各相关方面的角色及关系，项目组结构示意图如图 2 所示：

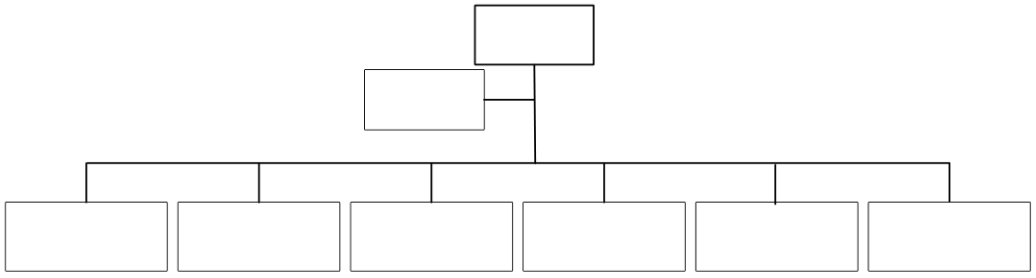

图2　灾备服务项目组结构示意图

5.2.2　服务项目组内各角色的人员职责包括：

a)　应急指挥——灾备服务和处理的负责人，协调机构的内部资源与外部资源，组成应急恢复服务体系，下达应急指令；

b)　应急协助——协助应急指挥，指导并监督各小组的工作；

c)　用户联系小组——负责在灾难发生时与用户进行沟通联系；

d) 系统切换小组——负责灾难备份系统与恢复系统的切换，按照灾备预案，启动灾难恢复系统；
e) 设施维护小组——负责监控机房环境、动力系统，确保在灾难发生时基础环境的完好和可靠；
f) 资源协调小组——负责组织、协调周边的环境资源，包括通讯系统、办公环境、会议系统、交通车辆等的安排协调；
g) 技术支持小组——负责在应急处置和切换过程中提供技术支持。

注：一般由设备供应商提供所需的技术支持与设备备件等。

5.2.3 项目组内各角色的人员宜有多个备份计划。项目组内各角色人员的变更应书面通知其它各角色人员。机构应建立对项目组的评审制度，评审宜至少每年进行一次。

5.3 灾难恢复能力等级划分

5.3.1 确定信息系统灾难恢复能力等级的主要参考要素为：
a) 信息系统的重要程度；
b) 紧急程度；
c) 系统损失；
d) 社会影响。

5.3.2 机构应协助用户按照以上要素对信息系统进行评估，确定系统的灾难恢复能力等级。

5.3.3 信息系统的灾难恢复能力等级可划分为六级，具体划分方式应符合 GB/T 20988—2007 附录 A 的规定。

5.4 预案制定

5.4.1 预案制定与评审

5.4.1.1 机构应根据风险评估和系统灾难恢复能力等级制定灾备应急预案。

5.4.1.2 预案包括总体预案和针对某个信息系统的专项预案及其附则。

5.4.1.3 预案中应考虑到各种应急资源的协调。应急资源宜包括人员、备品备件、资金、系统工具等。

5.4.1.4 为能够为灾备服务人员提供快速明确的指导，预案应明确、简洁，易于在紧急情况下执行，宜使用检查列表和详细规程。

5.4.1.5 灾备预案内容应包括：
a) 编制目的、依据和适用范围；
b) 项目组结构及人员职责；
c) 监测和预警机制；
d) 服务启动；
e) 服务处置；
f) 服务总结；
g) 保障措施；
h) 附则。

5.4.2 预案发布

5.4.2.1 经过内部评审确认的灾备预案，应由机构管理者或授权管理者发布。

5.4.2.2 机构应确认经过培训后的各专业灾备服务项目组的所有人员都能正确理解并执行预案。

5.4.2.3 机构应建立灾备预案的版本控制。

5.4.3 预案维护

5.4.3.1 预案的更新维护

5.4.3.1.1 机构应定期与灾备服务项目组的有关人员联系，及时核对灾备预案中的灾备服务项目组的成员及联络方式的变更情况，对预案进行及时的文档更新及分发，确保预案的有效性。

5.4.3.1.2 对于某个信息系统的变更，灾备服务项目组负责对专项预案的相关文档进行更新维护。

5.4.3.1.3 在灾备演练和灾难应急处置后，根据灾难恢复结果，机构与灾备服务项目组应对预案进行必要的更新与完善。

5.4.3.2 预案的修订、保存和发布

5.4.3.2.1 灾备预案应有不同的编号。

5.4.3.2.2 机构应确保在用户和灾备服务项目组至少各有一套完整的预案，并由双方指定人员妥善保管。

5.4.3.2.3 机构宜至少每年一次对灾备预案进行审核，制作新的修订版本，并发布。

5.4.3.2.4 新版本发布后，旧版本灾备预案应作回收登记并保留一定期限后销毁。

5.5 环境建设

5.5.1 灾难应急处置及系统恢复期间，机构应提供信息系统灾难恢复环境，宜配备以下设施：

a) 灾难恢复系统；
b) 电话和 Internet 接入；
c) 灾备网络接入端口；
d) 灾难恢复指挥工作会议设施；
e) 共享打印机、传真机、复印机、碎纸机、电子白板。

注：上述设施均处于门禁系统、电视监控系统的保护范围，所有负载均处于UPS保护范围内。

5.5.2 针对云计算应用系统的灾备服务，除 5.5.1 所述设施外，机构还应建立恢复的虚拟环境，应至少包括：

a) 虚拟环境；
b) 虚拟支撑软件。

5.6 培训服务

5.6.1 机构应制定灾备服务培训计划，并组织相关人员参与。

5.6.2 灾备预案应作为灾备服务培训的主要内容。

5.6.3 培训应使得被培训人员明确其在灾备服务过程中的责任范围，明确应急处置的操作规范和操作流程。

5.6.4 培训应定期举行，宜至少每年一次。

5.7 咨询服务

为帮助用户选择合适的灾备服务内容，机构应提供灾备咨询服务。咨询服务内容应包括：

a) 根据风险分析和业务影响分析的结果，结合用户的具体情况，制定信息系统恢复策略；
b) 根据信息系统恢复目标，确定灾难恢复能力等级；
c) 分析各种资源的获取方式；
d) 估算各种解决方案的投资成本与效益；
e) 形成灾备服务咨询报告。

6 灾难备份服务

灾难备份服务应包括：

a) 前期检查：
   1) 计算设备运行状况检查；
   2) 存储设备的检查；
   3) 网络设备运行情况检查；
   4) 灾备系统与生产系统的连通性检查；
   5) 数据传输网络的传输流量与传输质量检查；
   6) 软件运行检查。
b) 数据备份服务：
   1) 数据备份方式确定；
   2) 数据备份实施；
   3) 数据一致性检查。
c) 决策支持服务：
   1) 灾难备份系统状态报告；
   2) 监控数据分析报告；
   3) 灾难备份实施进展报告。

7 灾难应急处置服务

7.1 应急调度

7.1.1 信息系统灾备应急调度应包含：

a) 在规定时间要求内，迅速组织人员勘察、分析，并与用户沟通，并启动预案；
b) 通过网络、媒体、广播等多种手段快速获取灾难的相关信息；
c) 及时组织并协调相关部门及人员召开应急处置工作会议；
d) 根据应急处置要求，对涉及应急处置的灾备服务项目组下达调度命令。

7.1.2 机构应对调度过程记录进行整理、归档。

7.2 处理

7.2.1 灾备服务项目组应基于灾备预案进行灾难的处理，处理原则包括：

a) 应按照相应灾难恢复能力等级要求，恢复业务系统；
b) 采用的方法、手段不应造成新的灾难发生。

7.2.2 灾备服务项目组应对应急处置过程及结果信息进行记录，并及时告知用户。

7.2.3 灾备服务项目组与用户应对处理与恢复的结果进行确认。

8 灾难恢复服务

8.1 从灾难发生到灾难宣告，机构应在短时间内做出重大的决策。机构宜从灾备服务的服务架构、服务流程、技术手段等多个方面，确保服务目标的实现。

8.2 当正式宣告灾难发生后，信息系统灾备服务项目组应进行以下操作：

a) 根据要求通告用户；

b) 系统工作环境提供：
   1) 提供灾备系统的监控平台；
   2) 提供灾难恢复指挥中心；
   3) 提供灾难恢复配套资源（办公、生活等）。
c) 配合灾备系统切换：
   1) 灾备系统数据的完整备份；
   2) 灾备系统的切换准备就绪报告；
   3) 相关人员到岗就位；
   4) 配合执行灾备系统切换；
   5) 进度控制；
   6) 切换过程中问题记录、分析、总结及报告。
d) 监控：
   1) 灾备系统运行状况；
   2) 机构与用户的线路状况；
   3) 数据传输网络的传输流量与传输质量。
e) 技术支持：
   1) 计算设备技术支持；
   2) 存储设备技术支持；
   3) 网络系统技术支持；
   4) 数据库、中间件系统技术支持；
   5) 第三方服务商的现场技术支持。
f) 后勤保障支持：
   1) 启动特殊授权处理流程，简化实施人员进出机房手续等；
   2) 设备调拨、到货；
   3) 办公环境保障；
   4) 生活辅助设施保障。

9 灾备演练服务

9.1 演练目的

信息系统灾备演练服务的目的包括：

a) 确认灾难备份的项目组机构、人员、软硬件设备、设施是否满足灾难恢复的需求；
b) 检查备份数据的有效性；
c) 检查灾难备份网络系统的可用性；
d) 使灾备服务项目组人员更加熟悉灾难恢复的有关过程及操作；
e) 确认参与灾备演练的系统可成功进行系统恢复；
f) 验证灾备预案中各种文档、操作流程和操作规程有效性；
g) 验证系统恢复的时间是否在规定的时间之内；
h) 检查灾备服务项目组进行灾备服务的能力。

9.2 演练频率

应至少每年进行一次有用户参与的灾备演练。

9.3 演练步骤

信息系统灾备演练步骤宜形成灾备演练记录。演练步骤应包括：

a) 模拟灾难发生；
b) 启动灾备预案；
c) 启动系统恢复流程；
d) 模拟灾难断开数据复制链路；
e) 恢复系统准备；
f) 启用恢复系统，并确认恢复系统的可用性和正确性；
g) 启动用户信息系统，并确认和验证系统和数据的可用性；
h) 正式接替用户业务运营；
i) 灾难备份服务重新运行。

9.4 演练恢复

在演练过程中，应实时观察业务系统运行情况，当演练完成且业务系统运行正常后，应及时恢复系统到演练前状态，并清理演练环境。宜包括如下几个方面：

a) 恢复灾难备份系统；
b) 恢复数据正常通信；
c) 清理演练环境，删除演练数据。

9.5 演练总结

演练结束后，应就演练过程进行总结。宜包括以下内容：

a) 更新灾难备份系统；
b) 更新灾备预案；
c) 形成演练总结报告；
d) 文档资料更新；
e) 文档资料存档。

10 灾备服务总结与维持

10.1 服务结束

10.1.1 申请

10.1.1.1 灾备服务项目组应建立、审议信息系统灾备服务结束的策略和程序。

10.1.1.2 灾备服务项目组应对信息系统灾备服务的过程文档和各评审报告进行整理。

10.1.1.3 灾备服务项目组应由应急指挥或授权管理者向机构提出信息系统灾备服务结束申请，并提交相关文档资料。

10.1.2 核实

机构接到信息系统灾备服务结束申请后，逐项核实申请内容，以判别信息系统灾备服务处置过程和结果信息是否属实。

10.1.3 结束通报

10.1.3.1 机构应建立、审议信息系统灾备服务结束通报制度。

10.1.3.2 机构应向用户提供结束通报信息，内容应包括：

a) 信息系统灾备服务的级别；
b) 服务对应的预案信息；
c) 信息系统灾备服务处置的过程情况；
d) 信息系统灾备服务结束申请的处理意见；
e) 信息系统灾备服务结束通报的范围和涉及接受者。

10.2 服务总结

服务总结应包含：

a) 灾难事件发生的原因分析；
b) 灾备服务的处理过程和结果；
c) 评估信息系统灾备服务造成的影响；
d) 研究制定降低灾难发生频率和减轻损害的方法。

10.3 服务体系的保持

10.3.1 体系保持措施

为保证信息系统灾备服务的有效性，机构应对信息系统灾备服务体系进行维护和审核。

10.3.2 体系维护

10.3.2.1 机构应建立明确的服务体系维护计划，确保任何影响到灾备应急处置与灾难恢复的重大变更都能被识别出来，同时采取必要的措施对这些变更进行分析，并对服务体系做出相应调整，这种调整涉及灾备服务内容、灾备预案和资源配置。

10.3.2.2 体系维护的结果应包括：

a) 体系维护活动的文档记录；
b) 确保灾备服务的相关人员都已经明确体系的调整内容，并接受必要的培训；
c) 当需要对项目组架构、人员配备进行调整时，保留必要的文档记录。

10.3.3 体系审核

10.3.3.1 机构应按照预定的时间间隔对信息系统灾备服务体系进行审核，以确保体系具有持续的适用性。信息系统灾备服务体系审核应包括评估体系不足和改进建议。

10.3.3.2 体系审核的内容应包括：

a) 相关利益方的要求和反馈；
b) 项目组所采纳的用于支持灾备服务的各种技术、产品和流程；
c) 应急预案的测试结果及实际执行效果；
d) 可能影响信息系统灾备服务体系的各种业务变更；
e) 近期在处置信息系统灾备服务过程中的经验和教训；
f) 培训的结果和反馈。

10.3.3.3 体系审核的结果应包括：

a) 信息系统灾备服务体系的改进目标；
b) 改进信息系统灾备服务体系的有效性；
c) 所需的各种资源清单，包括人员、软硬件、资金等。