

简报

【2005】第 006 期（总第 039 期）

中国信息产业商会信息安全产业分会

2005 年 6 月

有备无患，利国利民

——中国灾难恢复行业高层论坛召开

为了对中国灾难恢复行业进行深入研究和探讨，让更多的行业、企业了解灾难事故面临的风险，掌握世界上先进灾难恢复技术的发展趋势，在国务院信息化工作办公室支持下、由我分会主办、北京泽镭科技发展有限公司承办的“中国灾难恢复行业高层论坛”于 2005 年 5 月 26、27 日在广东南海举行。

国务院信息办、中办信息中心、国家税务总局、中国人民银行、中国证监会、海关总署、国电信息中心、公安部、广电总局、国土资源部、铁道部、信息产业部、商务部及各行业、地区的信息化主管领导、各大银行、保险公司及国内外有关企业的领导参加了论坛，我分会秘书长张帆同志主持了第一天的会议。

论坛就灾准备份与灾难恢复，怎样对系统的灾难性故障进行迅速的响应和处置？如何制定适合自身实际的灾难恢复规划？中国开展灾难恢复业务将面临的主要挑战和实战方法，展开了深入而切实的讨论。同时对近日出台的指导文件《重要信息系统灾难恢复规划指南》，进行了宣讲和解释。

国务院信息化办公室网络安全组王渝次司长在会上作了重要讲话，他同时对《指南》进行了说明：“为加强对信息系统安全的管理，规范对信息系统灾难性故障的响应和处置，需要制定相应的对灾难恢复具有指导意义的规范性文件。信息系统灾难恢复规划作为一项周密的系统，需要按照科学的流程开展规划和实施。”。“考虑到灾备工作在我国刚开始起步，一些重要信息系统主管部门和运行单位感到缺乏经验，无从下手，迫切希望国家出台相应的工作指南。2004年10月开始，国务院信息办组织中国人民银行等8个国家重要信息系统主管部门以及中办、信息产业部、北京市信息办、上海市信息委、广东省信息办、GDS公司等有关单位成立了《指南》起草组。起草组既参考了有关国际标准，又结合了我国信息安全保障的实际情况，经过几个月紧锣密鼓的调研，终于于4月份出台了《指南》”。

国信办网络安全组负责灾备标准的熊四皓处长针对《指南》对各个行业及业界厂商有怎样的指导作用？进行了说明：《指南》是以信息系统灾难恢复规划的方法论为基本依据，吸取国际上先进的信息安全标准的相关内容，根据我国当前信息系统安全的发展现状，制定出对我国现阶段信息系统灾难恢复规划具有指导意义的指南文档。适用于指导信息系统的使用和管理单位的灾难恢复规划工作，对信息系统灾难恢复规划项目的审批和监督管理也可参照使用。也就是说，《指南》主要是为了给关键的行业用户做灾难恢复设计、建设、运维提供一个操作性强的参考思路。但是，《指南》对提供灾难备份技术、产品和服务的厂商也具有重要的意义，这些厂商在做有关部门的灾备建设或服务时，从此有了一个可以遵循的国家标准，防止走不必要的弯路。

GDS公司首席灾备顾问汪琪对《指南》的几个突出特点作特别发言，他指出：首先，《指南》对有关灾难备份和灾难恢复的名词术语进行了规范和梳理，这有助于澄清人们对灾难恢复的模糊认识，更好地开展灾难恢复工作。何为灾难？《指南》定义为：“由于人为或自然的原因，造成信息系统运行严重故障或瘫痪，使信息系统支持的业务功能停顿

或服务水平不可接受、达到特定的时间的突发性事件，通常导致信息系统需要切换到备用场地运行。”由此可见，灾难不只指自然的原因，也包括人为的原因，对于信息系统的连续性运行来说，灾难的范围很宽泛。

还有，何为灾难恢复？何为灾难备份？二者有何不同？

《指南》对前者的定义为：“将信息系统从灾难造成的故障或瘫痪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状态，而设计的活动和流程”。对后者的定义为：“为了灾难恢复而对数据、数据处理系统、网络系统、基础设施、技术支持能力和运行管理能力进行备份的过程。”显而易见，灾难恢复比灾难备份的外延要大。因此，汪琪提出，对国内惯用的“灾备”一词，今后要搞清其所指的确切涵义后再准确应用。例如，现在人们所说的“灾难备份”，如果是指既包括技术，也包括业务、管理的周密的系统工程，则应改为“灾难恢复”才更为精确。

其次，《指南》还以规范性附录的形式对灾难恢复的等级划分进行了描述。参照国际相关标准，并结合国内实际情况，将灾难恢复应具有的技术和管理支持分为6个等级，每个等级都包括数据备份系统、备用数据处理系统、备用网络系统、备用基础设施、技术支持、运行维护支持及灾难恢复预案等7个要素。如要达到某个灾难恢复等级，应同时满足该等级中的7个要素的要求。汪琪强调说，《指南》对灾难恢复等级的划分，融合了技术和管理，更具可操作性和对国情的适应性。

另外，《指南》的内容覆盖了灾难恢复工作的主要环节，以及每一个环节需要开展的各项具体工作。包括灾难恢复的管理，需求的确定，策略的制订和实现，预案的制订、落实和管理，预案框架等。之所以叫《指南》而不是标准，就是充分考虑了实际操作中可能遇到的复杂问题，能够为各有关部门和地方做好灾备工作提供参考。

银行系统的领导和专家针对行业特点和近年来银行业灾难恢复工作进展的情况作了发言：我国银行业务对数据的

实时性要求高，对数据备份一直比较重视。在“9.11”事件之后，各家银行进一步认识到实施灾难恢复的重要性，陆续开始考虑灾难恢复工作。目前，各行大都有数据级的备份措施，一些银行的备份数据能做到异地存放。根据各行数据集中进程的不同，灾备份中心建设进展情况也有所差别。

中国人民银行已在无锡自建了灾难应急备份中心，拟在上海建设支付系统数据备份中心。国家开发银行已于去年年底在央行的无锡灾备中心，完成了自己的异地数据备份存放，准备在今年年内筹建北京的同城灾备中心。中国农业发展银行在全行的数据大集中完成之际，将加快灾备中心的筹建工作。中国工商银行已建立了南北两大数据中心，南中心为数据中心，北中心为备份中心。中国农业银行的数据集中尚未完成，部分省行的数据中心建立了同城异地的灾备份中心。中国银行的灾备中心正在建设之中。中国建设银行的数据集中工作尚未结束，部分重要系统目前做到了同城异地的备份。此外，中国光大银行前两年已完成了同城灾备中心的建立，今年将准备在上海建立异地的灾备中心。上海浦东发展银行也将建成自己的同城灾备中心。福建建兴业银行对整个核心业务系统的数据备份和保护，以及为主机和外围网络等基础设施进行冗余备份的考虑，兴业银行2003年9月在上海启动了异地灾难备份中心。深圳发展银行则采用“合作建设、租赁服务”方式，与GDS公司合作完成了灾难备份中心系统的建设。城市商业银行和农信社的灾备进程稍慢，目前重点考虑同城备份措施。

此次大会与会人员得到这样的收获：明确目标，正确认识灾难恢复在保证行业业务持续运行中的地位和作用。因此，实施灾难恢复应从实际需求出发，明确目标，统筹规划，准确定位，突出重点，首先确保关键业务的灾难恢复。应在对信息系统的脆弱性和面临的安全威胁分析评估的基础上，根据所保护信息资产与服务价值、面临风险的大小、业务中断的损失和影响、业务恢复的优先级与相关性等因素，综合平衡安全成本投入和效益，确定灾难备份建设等级，合理选择灾难备份方案，切忌脱离实际需求，一哄而上。

充分认识灾难恢复体系的特征，合理选择灾难备份策略。首先，灾难备份资源是为高风险、小概率事件准备的，一般情况下处于闲置状态，高投入、低效益现象突出，因此，要在确保灾难备份和恢复功能的前提下，充分利用灾难备份资源，统筹安排，将日常运营和应急备份需求结合起来，使之发挥更大的效益。其次，灾难备份系统具有建设容易、运行维护难的特点。一次性建设投入高，运行维护成本可能更高，特别是长期维护一支高水平、灾难发生时能真正发挥作用的灾难恢复队伍更难。因此，灾难备份设施建设要充分利用现有各种资源，提倡资源共享，降低成本。银行业务的相似性，使得联合共建和共享社会化服务具有现实可能性。提倡使用社会化灾难备份服务，走专业化服务道路。

客观认识灾难备份的社会化服务问题。社会化服务包括灾难备份服务整体外包、投资参与灾难备份设施建设、租用第三方灾难备份设施、利用社会专业技术力量运营管理和应急支援等多种形式。从我国银行的实际情况看，国有大型银行的技术与经济实力比较强，在灾难备份中心的建设上能够走自建自营的道路；对多数中小银行来说，完全靠自己的力量建设和运行维护灾难备份中心，无论从投资上、从应用上、从应用的效果上都是不适宜的。在开展灾难备份工作的初期阶段，首先将部分业务进行外包，不失为一种有益尝试，可以在最短的时间内，利用别人最成熟的技术、管理经验，形成自己的竞争优势。

规范灾难恢复技术与管理标准。目前，由于缺乏完善的行业相关技术与管理规范，灾难恢复的很多工作难以有序展开，甚至会在灾难备份工作中产生许多新的风险。因此，应认真总结我国灾难备份工作中成功的经验，学习和借鉴国外的先进经验，抓紧开展金融业的灾难恢复技术和标准规范工作，做到标准先行。

实施灾难恢复行业监管。从上世纪 80 年代起，一些西方发达国家针对灾难恢复和企业连续运作提出了监管要求，各行业监管部门和政府对于灾难恢复制定了监管条例、指引和公告。为进一步做好银行灾难备份监管工作，人民银行和银

监会作为我国银行业的主管部门，将根据职责划分，按照国家有关部门有关通知的精神和《指南》的要求，从维护国家经济稳定运行的大局出发，积极开展工作，进一步加强对金融业灾难备份工作的监管、协调与支持。

主题词：灾备 会议

送： 国务院信息化工作办公室 信息产业部 公安部 国家保密局 国家密码管理委员会办公室 中国信息产业商会 信息安全产业分会各会员单位