

信息系统灾难恢复规范



版权归GDS所有

GB/T20988《信息系统灾难恢复规范》介绍

《灾备中心建设与管理规范》编制情况



版权归GDS所有

9.11的启示：全球关注灾备建设

2001年9月11日，恐怖份子袭击了纽约世界贸易中心，造成3栋塔楼倒塌，近3000人失踪和死亡。

Deutsche Bank

- 93年开始风险分析，并建立了一整套完整的业务连续性计划（BCP），以应对突发事件或灾难。
- 灾难发生后，德意志银行调动4000多名员工及全球分行的资源，短时间内在距离纽约30公里的地方恢复了业务运行。
- 911后，员工和客户对德意志银行都更加有信心。



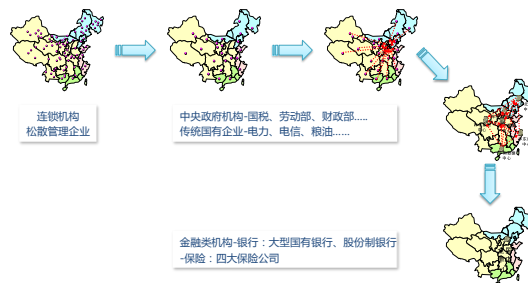
Bank of New York:

- 为自己的客户提供证券买卖服务
- 为集团内其他银行提供资金调拨服务（FR）
- 数据中心位于灾场附近
- 通讯线路全部中断
- 造成连锁反应
- 2001年10月18日，纽约银行声明，恐怖袭击破坏了部分计算机系统，一些分支机构被迫关闭，其第三季度的利润因此下降了33%。



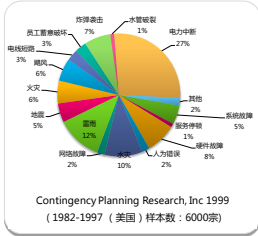
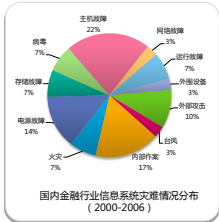
版权归GDS所有

数据中心集中化，企业风险集中



版权归GDS所有

信息化运营风险



版权归GDS所有

《信息系统灾难恢复规范》出台



背景

- 贯彻2003年8月下发的中办发[2003]27号文件《国家信息化领导小组关于加强信息安全保障工作的意见》的文件精神
- 贯彻2004年9月下发的国家网络与信息安全协调小组办公室《关于做好重要信息系统灾难备份工作的通知（信安通[2004]11号文件）》的文件精神
- 加强对信息安全管理，规范对信息系统灾难性故障的响应和处置，需制定对灾难恢复具有指导意义的规范性文件文档

起草单位

- 2004年《重要信息系统灾难恢复指南》的编制任务由国信办下达
- 由全国重要行业、中办、3个地方政府和万国数据公司形成编制组，按国家标准格式进行编制。
- 2005年4月《重要信息系统灾难恢复指南》由国信办以文件形式下发
- 2006年信安标委专家对《指南》进行审查、修改，更名为《信息系统灾难恢复规范》
- 2007年GB/T 20988《信息系统灾难恢复规范》发布



版权归GDS所有

《规范》的意义及核心内容



编制意义

- 第一份对于信息系统灾难备份建设的文件
- 对做好重要信息系统灾难恢复的规划和准备工作的具体规范和指导
- 为科学实施信息系统灾难恢复提供指导性的流程和方法。
- 是信息系统设计人员、管理人员和测评人员培训的基本教材



核心内容

- 灾难恢复规划的管理
- 灾难恢复需求的确定
- 灾难恢复策略的制订
- 灾难恢复策略的实现
- 灾难恢复预案的制订、落实和管理
- 灾难恢复的等级划分（规范性附录）
- 灾难恢复预案框架（资料性附录）

版权归GDS所有

GB/T 20988-2007 《信息系统灾难恢复规范》



灾难恢复概述

- 灾难恢复的工作范围
- 灾难恢复的组织机构
- 灾难恢复规划的管理
- 灾难恢复的外部协作
- 灾难恢复的审计和备案

灾难恢复需求的确定

- 风险分析
- 业务影响分析
- 确定灾难恢复目标

灾难恢复策略的制定

- 灾难恢复策略制定的要素
- 灾难恢复资源的获取方式
- 灾难恢复资源的要求

灾难恢复策略的实现

- 灾难备份系统技术方案的选择
- 灾难备份中心的选择和建设
- 专业技术支持能力的实现
- 运行维护管理能力的实现
- 灾难恢复预案的实现

灾难恢复7要素

- 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
- 专业技术支持能力
- 运行维护管理能力
- 灾难恢复预案

附录

- 灾难恢复的等级划分（规范性附录）
- 灾难恢复预案框架（资料性附录）
- 某行业RTO/RPO与灾难恢复能力等级的关系示例（资料性附录）

版权归GDS所有

主要内容说明——第三章



术语和定义

- | | |
|----------|---------------|
| ✓ 灾难 | ✓ 生产系统 |
| ✓ 灾难恢复 | ✓ 灾难备份中心；备用场所 |
| ✓ 灾难恢复规划 | ✓ 灾难备份 |
| ✓ 业务影响分析 | ✓ 灾难备份系统 |
| ✓ 恢复时间目标 | ✓ 数据备份策略 |
| ✓ 恢复点目标 | ✓ 灾难恢复预案 |
| ✓ 关键业务功能 | ✓ 演练 |
| | ✓ 演习 |

版权归GDS所有

主要内容说明——第三章



灾难 disaster

- 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

版权归GDS所有

主要内容说明——第三章



灾难恢复 disaster recovery

- 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

灾难恢复规划（DRP）disaster recover planning

- 为了减少灾难带来的损失和实现灾难恢复所做的事前计划和安排

版权归GDS所有

主要内容说明——第三章



恢复时间目标（RTO）recovery time objective

- 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

恢复点目标（RPO）recovery point objective

- 灾难发生后，系统和数据必须恢复到的时间点要求

版权归GDS所有

主要内容说明——第三章



灾难备份中心：备用场所 alternate site

- ▶ 用于灾难发生时接替生产系统运行进行数据处理和支持关键业务功能运作的场所，包括备用数据处理中心、备用的工作环境、备用生活设施和技术支持及运行管理人员

灾难恢复预案 disaster recovery plan

- ▶ 按定义信息系统灾难恢复过程中所需的任务、行动、数据和资源的文件，用于指导相关人员在预定的灾难恢复目标内恢复信息系统支持的关键业务功能

版权归GDS所有

主要内容说明——第三章



演练 exercise

- ▶ 于训练人员和提高灾难恢复能力的活动，包括桌面演练、模拟演练、操作演练和演习等

[灾难恢复]演习 mock drill

- ▶ 按设定的灾难场景，参与人员根据灾难恢复预案进行活动的过程

版权归GDS所有

主要内容说明——第四章



灾难恢复的管理

- ▶ 灾难恢复的工作范围
- ▶ 灾难恢复规划的组织机构及其职责
- ▶ 灾难恢复规划的管理
- ▶ 灾难恢复规划的外部协作
- ▶ 灾难恢复规划的审计和监理

版权归GDS所有

主要内容说明——第五章



灾难恢复需求的确定

- ▶ 风险分析
- ▶ 业务影响分析
- ▶ 确定灾难恢复目标

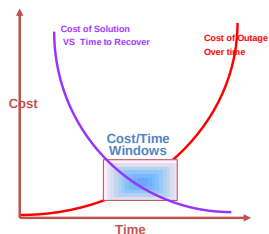
版权归GDS所有

主要内容说明——第六章



灾难恢复策略的制定

- ▶ 要素分析
- ▶ 成本风险分析
- ▶ 确定灾难恢复资源的获取方式
- ▶ 确定灾难恢复等级各要素的要求
 - 数据备份系统
 - 备用基础设施
 - 备用数据处理系统
 - 备用网络系统
 - 技术支持能力
 - 运行维护管理能力
 - 灾难恢复预案



版权归GDS所有

主要内容说明——第七章



灾难恢复预案的制订、落实和管理

- ▶ 灾备中心的选择和建设
 - 选址原则
 - 基础设施要求
- ▶ 灾难备份系统技术方案的实现
 - 技术方案的设计
 - 技术方案的验证、确认和系统开发
 - 系统安装和测试
- ▶ 技术支持能力的实现
- ▶ 运行维护管理能力的实现
- ▶ 灾难恢复预案的实现

版权归GDS所有

主要内容说明——第八章



灾难恢复预案的制订、落实和管理

- ▶ 灾难恢复预案的制订
 - 制订原则
 - 制订过程
- ▶ 灾难恢复预案的教育、培训和演练
- ▶ 灾难恢复预案的管理
 - 保存与分发
 - 维护和变更管理

版权归GDS所有

灾难恢复能力等级划分



- 第1级 基本支持
- 第2级 备用场地支持
- 第3级 电子传输和部分设备支持
- 第4级 电子传输及完整设备支持
- 第5级 实时数据传输及完整设备支持
- 第6级 数据零丢失和远程集群支持

灾难恢复7要素

- 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
- 专业技术支持能力
- 运行维护管理能力
- 灾难恢复预案

版权归GDS所有

附录A---灾难恢复等级的划分



等级一 基本支持

要素	要求
A.1.1 数据备份系统	a)完全数据备份至少每周一次； b)备份介质场外存放。
A.1.2 备用数据处理系统	—
A.1.3 备用网络系统	—
A.1.4 备用基础设施	a)有符合介质存放条件的场地。
A.1.5 技术支持	—
A.1.6 运行维护支持	a)有介质存取、验证和转储管理制度； b)按介质特性对备份数据定期进行定期的有效性验证。
A.1.7 灾难恢复预案	有相应的经过完整测试和演练的灾难恢复预案。

版权归GDS所有

附录A---灾难恢复等级的划分



等级二 备用场地支持

要素	要求
A.2.1 数据备份系统	a)完全数据备份至少每周一次； b)备份介质场外存放。
A.2.2 备用数据处理系统	a)灾难发生时能在预定时间内调配所需的数据处理设备到场。
A.2.3 备用网络系统	a)灾难发生时能在预定时间内调配所需的通信线路和网络设备到位。
A.2.4 备用基础设施	a)有符合介质存放条件的场地； b)有满足信息系统和关键业务功能恢复运作要求的备用场地。
A.2.5 技术支持	—
A.2.6 运行维护支持	a)有介质存取、验证和转储管理制度； b)按介质特性对备份数据定期进行定期的有效性验证； c)有备用设备管理制度； d)有与设备供应商签订的灾难恢复时间要求的设备供货协议； e)与相关运营商符合灾难恢复时间要求的备用通信线路协议。
A.2.7 灾难恢复预案	a)有相应的经过完整测试和演练的灾难恢复预案。

版权归GDS所有

附录A---灾难恢复等级的划分



等级三 电子传输和部分设备支持

要素	要求
A.3.1 数据备份系统	a)完全数据备份至少每天一次； b)备份介质场外存放； c)每天多次利用通信网络将关键数据定时批量传送至备用场地。
A.3.2 备用数据处理系统	a)配备灾难恢复所需的部分数据处理设备。
A.3.3 备用网络系统	a)配备灾难恢复所需的通信线路和相应的网络设备。
A.3.4 备用基础设施	a)有符合介质存放条件的场地； b)有满足信息系统和关键业务功能恢复运作要求的场地。
A.3.5 技术支持	a)在备用场地有专职的计算机机房运行管理人员。
A.3.6 运行维护支持	a)按介质特性对备份数据定期进行定期的有效性验证； b)有介质存取、验证和转储管理制度； c)有备用计算机机房管理制度； d)有备用数据设备设施维护管理计划； e)有电子传输数据备份系统运行管理制度。
A.3.7 灾难恢复预案	有相应的经过完整测试和演练的灾难恢复预案。

版权归GDS所有

附录A---灾难恢复等级的划分



等级四 电子传输及完整设备支持

要素	要求
A.4.1 数据备份系统	a)完全数据备份至少每天一次； b)备份介质场外存放； c)每天多次利用通信网络将关键数据定时批量传送至备用场地。
A.4.2 备用数据处理系统	a)配备灾难恢复所需的全部数据处理设备，并处于就绪状态或运行状态。
A.4.3 备用网络系统	a)配备灾难恢复所需的通信线路； b)配备灾难恢复所需的网络设备，并处于就绪状态。
A.4.4 备用基础设施	a)有符合介质存放条件的备用场地； b)有符合备用数据处理系统和备用网络设备运行要求的场地； c)有满足关键业务功能恢复运作要求的场地； d)以上场地应同时满足A.3.4.1~A.3.4.4。
A.4.5 技术支持	在备用场地有： a)7 x 24专职计算机机房管理人员； b)专职的数据备份技术支持人员； c)专职硬件、网络技术支持人员。
A.4.6 运行维护支持	a)有介质存取、验证和转储管理制度； b)按介质特性对备份数据定期进行定期的有效性验证； c)有备用计算机机房运行管理制度； d)有硬件和网络运行管理制度； e)有电子传输数据备份系统运行管理制度。
A.4.7 灾难恢复预案	有相应的经过完整测试和演练的灾难恢复预案。

版权归GDS所有

附录A---灾难恢复等级的划分



等级五 实时数据传输及完整设备支持

要素	要求
A.5.1 数据备份系统	a)完全数据备份至少每天一次； b)备份介质场外存放； c)采用远程数据复制技术，并利用通信网络将关键数据实时复制到备份场地。
A.5.2 备用数据处理系统	a)配备灾难恢复所需的全部数据处理设备，并处于就绪或运行状态。
A.5.3 备用网络系统	a)配备灾难恢复所需的通信线路； b)配备灾难恢复所需的网络设备，并处于就绪状态； c)具备通信网络自愈或集中控制能力。
A.5.4 备用基础设施	a)符合介质存放条件的备用场地； b)符合备用数据处理系统和备用网络设备运行要求的场地； c)有满足关键业务功能恢复运行要求的场地； d)以上场地应保持7 x 24运行。
A.5.5 技术支持	在备用场地有： a)7 x 24专职计算机机房管理人员； b)7 x 24专职数据备份技术支持人员； c)7 x 24专职硬件、网络技术支持人员。
A.5.6 运行维护支持	a)有介质存取、验证和转储管理制度； b)按介质特性对备份数据进行定期的有效性验证； c)有专用计算机机房运行管理制度； d)有硬件和网络运行管理制度； e)有实时数据备份系统运行管理制度。
A.5.7 灾难恢复预案	有相应的经过完整测试和演练的灾难恢复预案。

版权归GDS所有

附录A---灾难恢复等级的划分



等级六 数据零丢失和远程集群支持

要素	要求
A.6.1 数据备份系统	a)完全数据备份至少每天一次； b)备份介质场外存放； c)远程实时备份，实现数据零丢失。
A.6.2 备用数据处理系统	a)备用数据处理系统设备与生产数据处理系统一致的处理能力并完全兼容； b)应用软件是“集群的”，可实时无缝切换； c)具备远程集群系统的实时监控和自动切换能力。
A.6.3 备用网络系统	a)备用网络处于运行状态； b)最终用户可通过网络同时接入主、备中心。
A.6.4 备用基础设施	a)符合介质存放条件的备用场地； b)符合备用数据处理系统和备用网络设备运行要求的场地； c)有满足关键业务功能恢复运行要求的场地； d)以上场地应保持7 x 24运行。
A.6.5 技术支持	在备用场地有： a)7 x 24专职计算机机房管理人员； b)7 x 24专职数据备份技术支持人员； c)7 x 24专职硬件、网络技术支持人员； d)7 x 24专职操作系统、数据库和应用软件技术支持人员。
A.6.6 运行维护支持	a)有介质存取、验证和转储管理制度； b)按介质特性对备份数据进行定期的有效性验证； c)有专用计算机的运行管理制度； d)有硬件和网络运行管理制度； e)有实时数据备份系统运行管理制度； f)有操作系统、数据库和应用软件运行管理制度。
A.6.7 灾难恢复预案	有相应的经过完整测试和演练的灾难恢复预案。

版权归GDS所有

灾难恢复预案框架



- B.1 目标和范围**

B.2 组织和职责

B.3 联络与通讯

B.4 突发事件响应流程

 - 事件通告
 - 人员疏散
 - 损害评估
 - 灾难宣告

B.5 恢复及重建运行流程

 - 恢复
 - 重建运行
- B.6 灾后重建和回退**

B.7 预案的保障条件

B.8 预案附录

 - 人员疏散计划；
 - 产品说明书；
 - 信息系统标准操作流程；
 - 服务级别协议和备忘录；
 - 资源清单；
 - 业务影响分析报告；
 - 预案的保存和分发办法。



版权归GDS所有

RTO/RPO与灾难恢复能力等级的关系



灾难恢复能力等级	RTO	RPO
1	2天以上	1天至7天
2	24小时以上	1天至7天
3	12小时以上	数小时至1天
4	数小时至2天	数小时至1天
5	数分钟至2天	0至30分钟
6	数分钟	0



版权归GDS所有

应用情况

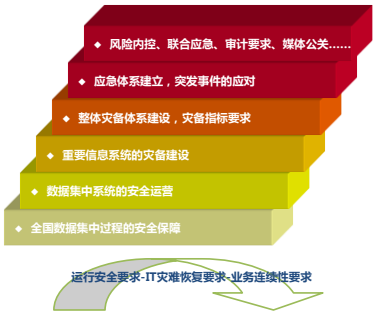


- 2008年 保监会 保监发〔2008〕20号《保险业信息系统灾难恢复管理指引》
- 2008年 人民银行 JR/T 0044-2008 《银行业信息系统灾难恢复管理规范》
- 2008年 银监会《银行业重要信息系统突发事件应急管理规范》
- 2009年 证监会《证券期货业信息系统灾难恢复管理规范》
- 2009年 人社部 人社厅发《人力资源和社会保障信息系统灾备系统建设指导意见》
- 2011年财政部《全国财政信息系统灾备建设指导意见》



版权归GDS所有

国内灾难恢复发展趋势分析



版权归GDS所有

各行业灾难恢复建设



银行、保险、证券、基金

- 大型机构灾备建设初具规模
- 中、小型机构近期普遍启动
- 业务连续性建设相对滞后

大型企业

- 国有大型企业相对重视，开始规划和建立灾难恢复设施
- 企业自身稳定发展的需要
- 上市监管部门审计的需要

政府机构

- 信息化依赖程度高的部门先行建设
- 重视统一规划和资源共享
- 重视对灾害的抵御，特别是公共事件的应急体系建设

版权归GDS所有

- GB/T20988《信息系统灾难恢复规范》介绍
- 《灾备中心建设与管理规范》编制情况



版权归GDS所有

《灾难备份中心建设和管理规范》定位



背景

- “GB/T 20988-2007《信息系统灾难恢复规范》”描绘了组织灾难恢复建设及管理体系，提出体系建立的基本要求，系统中各重要组成部分有待细化。为了深入规范体系，明确建设要求，形成业务连续性管理及灾难恢复国际标。灾备中心是灾难恢复的核心内容，因此，首要制定灾备中心建设和管理规范。

意义

- 通过对灾难备份中心的建设和运维管理进行规范，在灾备中心选址、基础设施建设、通信网络、功能区域设置布局与划分、机房环境建设、安全防范，以及灾难备份中心运行维护管理等诸多方面提出具体的指标要求，可为灾备中心的建设和使用单位和从事信息系统灾难恢复服务的各类机构提供建设和管理指南，还可为政府行业主管部门提供监督管理依据。



版权归GDS所有

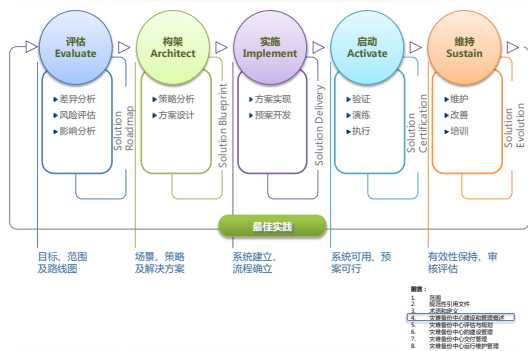
国标起草过程



时间	里程碑	文档
2009年	立项申请	《信息安全国家标准项目申请书》《推荐性国标项目建议书》
2010年	获得国家标准项目审批	《信息安全专项项目任务书》
2010年	国际起草项目组成立；收集资料，分析国内、外标准，总结、提炼最佳实践	
2011年-3	形成国际框架，完成内部讨论稿	GB《灾难备份中心建设和管理规范》内部讨论稿
2011年-5	内部讨论，形成标准草案	GB《灾难备份中心建设和管理规范》初稿
2011年-6	工作组第一次工作会议，征求专家意见	征求意见稿汇总
2011年-8	形成征求意见稿，并上报 信安标委	GB《灾难备份中心建设和管理规范》初稿
2011年-9	第二次征求意见，讨论草案	GB《灾难备份中心建设和管理规范》（草案）
2011年-10	第三次征求意见，专家评审会	GB《灾难备份中心建设和管理规范》（征求意见稿）

版权归GDS所有

《灾备中心建设与管理规范》草案内容介绍



版权归GDS所有

《灾备中心建设与管理规范》草案内容介绍



灾难备份中心评估与规划

- 灾难备份中心评估与规划工作内容
- 灾难备份中心需求评估
 - 生产系统风险分析
 - 基础设施风险分析
 - 业务影响分析
 - 应用系统关联分析
 - 应急流程与运维制度评估
- 灾难备份中心的规划
 - 灾难恢复策略制定
 - 灾难备份中心场地选址规划
 - 灾难备份中心资源获取方式规划
 - 灾难备份中心基础设施资源规划
 - 灾难备份中心信息系统规划
 - 灾难备份中心运维管理体系规划

- 灾难备份中心的方案设计
 - 灾难备份中心基础设施方案设计
 - 灾难恢复系统技术方案设计

- 文档**
- 灾备中心建设与管理规范
 - 灾备中心建设与管理规范
 - 灾备中心建设与管理规范
 - 灾备中心建设与管理规范
 - 灾备中心建设与管理规范
 - 灾备中心建设与管理规范
 - 灾备中心建设与管理规范
 - 灾备中心建设与管理规范

版权归GDS所有

《灾备中心建设与管理规范》草案内容介绍



灾备备份中心的建设管理

1. 灾备备份中心基础设施建设管理
 - 基础设施建设内容
 - 基础设施建设管理要求
 - 基础设施建设实施要求
2. 灾难恢复系统的建设管理
 - 灾难恢复系统建设内容
 - 灾难恢复系统建设要求
 - 数据备份系统建设要求
 - 备用处理系统建设要求
 - 备用网络系统建设要求
 - 灾难恢复指挥和管理系统建设要求
3. 灾难恢复预案的开发

目录：

1.	总则
2.	规范性引用文件
3.	术语和定义
4.	灾备备份中心建设和管理概述
5.	灾备备份中心建设内容
6.	灾备备份中心建设管理
7.	灾备备份中心运行维护
8.	灾备备份中心运行维护管理

版权归GDS所有

《灾备中心建设与管理规范》草案内容介绍



灾备备份中心交付管理

1. 灾备备份中心基础设施的验收和移交
2. 灾备备份系统的有效性验证
 - 数据的完整性验证
 - 数据的一致性验证
 - 数据备份与恢复能力验证
 - 信息系统切换与回切能力验证
 - 网络系统切换与回切能力验证
 - 应用系统切换与回切能力验证
3. 灾难恢复预案的验证
4. 灾备备份中心与生产中心的协作

目录：

1.	总则
2.	规范性引用文件
3.	术语和定义
4.	灾备备份中心建设和管理概述
5.	灾备备份中心建设内容
6.	灾备备份中心建设管理
7.	灾备备份中心运行维护
8.	灾备备份中心运行维护管理

《灾备中心建设与管理规范》草案内容介绍



灾备备份中心运行维护管理

1. 灾备备份中心运行维护管理原则
2. 灾备备份中心运行维护管理的组织
 - 灾备备份中心的组织形式
 - 灾备备份中心的管理职责
 - 基础设施运维管理
 - 信息系统运维管理
 - 应急及灾难恢复支持
 - 接替生产运行
 - 安全管理
3. 灾备备份中心运行维护管理制度
4. 备份中心运行维护管理内容和要求
 - 安全管理
 - 灾难恢复演练的组织管理
 - 基础设施运维管理
 - 预案维护
 - 灾备备份系统运维管理
 - 应急和切换
 - 服务商管理
 - 教育与培训
 - 基准核对管理
 - 文档和知识管理
 - 子系统验证管理
5. 灾备备份中心管理的审核与验证

目录：

1.	总则
2.	规范性引用文件
3.	术语和定义
4.	灾备备份中心建设和管理概述
5.	灾备备份中心建设内容
6.	灾备备份中心建设管理
7.	灾备备份中心运行维护
8.	灾备备份中心运行维护管理

版权归GDS所有



联络方式：汪琪 13603023960
wangqi@gds-services.com

THANKS

专家工作组成员



国务院信息化工作办公室
中央办公厅信息中心
中国人民银行科技司
信息产业部电信管理局
国家税务总局信息中心
铁道部信息办
海关总署信息中心
国家电网公司科技信息部
中国民航信息网络股份公司
中国证监会信息中心
中国保监会统计信息部
北京市信息安全服务中心
上海市信息办
广东省信息中心
万国数据服务（深圳）有限公司

单 位

版权归GDS所有