信息系统
灾难恢复与能力评估

Disaster Recovery Capability Evaluation
for Information Systems

刘建毅　李欣一　主　编
关继铮　王　枞　副主编

北京邮电大学出版社
www.buptpress.com

信息系统灾难恢复与能力评估

刘建毅　李欣一　主　编
关继铮　王　枞　副主编

北京邮电大学出版社
www. buptpress. com

内 容 简 介

本书主要介绍了信息系统灾难恢复体系构建、灾难恢复能力评估的相关知识与实用技术，从灾难恢复规划设计、建设实施和运维维护三方面讨论了企业信息系统应具备的灾难恢复能力，对当前一些较成熟的技术和解决方案进行了分析比较。本书的特色是理论与实用相结合，使读者能够利用书中的方法和步骤去解决实际应用中的常见问题。

本书适合IT系统客户服务人员、技术支持工程师、技术培训人员、数据恢复技术工程师、信息安全工作人员、系统管理人员、安全保密部门、存储技术相关人员、学生及任何对相关技术或工作感兴趣的读者作为学习材料。

图书在版编目（CIP）数据

信息系统灾难恢复与能力评估 / 刘建毅，李欣一主编. -- 北京 ：北京邮电大学出版社，2017.2
ISBN 978-7-5635-4934-4

Ⅰ. ①信… Ⅱ. ①刘… ②李… Ⅲ. ①信息系统－安全技术－评估 Ⅳ. ①TP309

中国版本图书馆CIP数据核字（2016）第223789号

书　　名：信息系统灾难恢复与能力评估
著作责任者：刘建毅　李欣一　主编
责 任 编 辑：张珊珊
出 版 发 行：北京邮电大学出版社
社　　址：北京市海淀区西土城路10号(邮编:100876)
发 行 部：电话：010-62282185　传真：010-62283578
E-mail:publish@bupt.edu.cn
经　　销：各地新华书店
印　　刷：保定市中画美凯印刷有限公司
开　　本：787 mm×1 092 mm　1/16
印　　张：15
字　　数：369千字
版　　次：2017年2月第1版　2017年2月第1次印刷

ISBN 978-7-5635-4934-4　　定　价：35.00元

前　言

随着灾难防御意识的逐步深入，世界各国政府、组织、机构和企业都投入巨资进行包括信息系统安全保障、安全事件应急响应、系统灾难恢复及系统安全评估等内容的信息系统灾难防御体系研究和建设。因此，建立完整、有效和规范的灾难恢复评估模型、方法和相应的评估工具，在未经历灾难的情况下客观地评估信息系统的灾难恢复能力，并据此建立更好的信息系统灾难恢复体系是保障国家信息安全的一项重要内容，也是信息化发展建设不可或缺的步骤。然而，目前国内外对信息系统的灾难恢复能力评估和评测的研究仍在起步阶段，缺乏成熟的评估理论、方法和相应工具。

本书介绍了灾难恢复系统在灾难恢复规划设计、建设实施和运营维护三方面的能力要求、技术方案以及评估方法。读者可以利用书中的知识和方法去解决实际应用中的常见问题。通过阅读本书，能够较为全面地了解灾难恢复系统的建设和评估，掌握常用的灾难恢复策略与解决方案。

本书共分六章。第1章“绪论”介绍信息系统灾难恢复的基础知识和部分基本理论，阐述信息系统灾难恢复的含义和目标、特点，国内外的发展现状，信息系统灾难恢复能力评估标准和评估方法。本章可使读者较为全面地了解信息系统灾难恢复体系建设和评估的发展和现状。

第2章“灾难恢复体系规划设计”介绍在灾难恢复规划设计阶段的技术要求和能力要求，包括灾难恢复需求分析、策略制定、技术体系规划、资源规划。

第3章“灾难恢复体系建设与实施”讲述在建设实施阶段的技术要求和能力要求，包括灾难恢复资源建设、灾难恢复系统实施及灾难恢复预案的制定。

第4章“灾难恢复体系运营维护”阐述在运营维护阶段的技术要求和能力要求，包括灾难恢复系统的日常运维管理和发生灾难事件后的应急与灾难恢复管理。

第5章“灾难恢复能力评估”按规划设计、建设实施和运维管理三个阶段，从技术、资源和管理三个维度建立评估指标体系，并阐述评估模型和评估方法。

第6章“灾难恢复成本效益评估”指出灾难恢复策略的制定应当满足成本效益分析的原则，阐明了成本效益评估的指标体系、工作流程。

本书主要由刘建毅、王枞和关继铮执笔编写，古恒、傅群超、张思悦、雷鸣涛、朱小陆、于俊和吕涛等同学也参加了本书的部分编写工作。

灾难恢复工作是一项综合性强、技术复杂度高、协调配合难度大的系统工程，涉及的知识面广、发展迅速，加之作者的水平有限，书中的错误在所难免，若有不当之处，敬请指正。

希望本书能对读者有所裨益。

目　录

第1章 绪 论

1.1 信息系统灾难恢复

1.1.1 灾难恢复的含义和目标

灾难恢复是指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。它的目的是减轻灾难对企业和社会带来的不良影响，保证信息系统所支持的关键业务功能在灾难发生后能及时恢复和继续运作。

灾难恢复工作包括灾难发生后的应急响应与处置、信息系统在灾难备份中心的恢复和重续运行、生产系统的灾后重建和回退工作。

信息系统的灾难恢复应与生产系统相适应，并能满足发生灾难时接替生产运行的要求，随着企业的业务发展和信息系统的变化，灾难恢复工作也将随之而变化，因此灾难恢复工作是一个周而复始、持续改进的过程。

构建企业灾难恢复体系包括灾难恢复规划设计、建设实施和运维管理三个阶段，其中：灾难恢复规划设计包括灾难恢复的需求分析、策略制定、技术方案设计；灾难恢复的建设实施包括灾难恢复资源建设、灾难恢复系统实施及灾难恢复计划的制订；灾难恢复的运维管理包括灾难恢复系统的日常运维管理和发生灾难事件后的应急与灾难恢复管理。因此灾难恢复工作是一项综合性强、技术复杂度高、协调配合难度大的系统工程。

1.1.2 灾难恢复的特点

鉴于灾难恢复的目标和定义，灾难恢复工作主要体现出以下几个特点：

(1) 平战结合：灾难的发生是一种风险高的小低概率事件，在一般情况下，灾难恢复资源处于闲置状态，为确保灾难发生时的信息系统恢复和业务的持续运行，应加强对灾难恢复资源的日常管理和应急管理，确保灾难发生时灾难恢复系统可接替生产系统运行。

(2) 成本高：为确保灾难发生时，灾难恢复系统能够接替生产系统运行，需构建一个完整、可靠，并与生产系统相适应的灾难恢复体系，这套体系不仅包括灾难恢复的场所、灾难恢复系统、灾难恢复线路，还包括灾难恢复的人员、管理机制，因此灾难恢复体系所要求的建设成本和运行维护成本都比较高。

(3) 专业性强：灾难恢复体系与企业的业务系统有着非常密切的关系，因此无论是灾难恢复体系的规划设计、建设实施及运行维护，都需要高素质、多学科、懂业务的专业技术人员相互协调和配合才能完成。

（4）规范性强：灾难恢复的过程需要多方人员相互配合，灾难恢复的时间直接关系到企业经济损失和社会影响，因此无论在日常运行维护还是在发生灾难时的应急处置及灾难恢复中，都需要在建立有效的信息系统灾难恢复技术体系的同时，建立规范的灾难恢复管理制度和流程，以提升灾难恢复的效率，确保信息系统能在业务部门所能容忍的时间内恢复运行。

1.1.3 灾难恢复与业务连续性

灾难恢复是对企业的信息系统进行相应的冲击分析及风险评估并将其量化，以确定信息系统面对灾难事故时的预防和恢复策略，开发并制定相应的数据和系统恢复计划、管理方法和流程，以缓解灾难对于信息系统造成的不利影响。

业务连续规划（Business Continuity Planning）就是灾难事故的预防和反应机制，是一系列事先制定的策略和规划，确保企业在面临突发的灾难事故时，关键业务功能的有效发挥和业务的持续运行。业务连续规划不仅仅包括对信息系统的恢复，更重要的是要考虑人员安全、资源保障和业务恢复。

对于信息化依赖程度高的企业，灾难恢复是其业务连续规划的重要组成部分。灾难恢复是业务持续运行的基础性必要条件。

业务连续性管理（Business Continuity Management）是针对企业现有资源所面临的潜在风险进行评估分析，制定完善有效的管理制度以防范灾难事件的发生，并减少灾难事件造成的损失。业务连续性管理是一项综合管理流程，它使企业在识别潜在风险的基础上制定业务连续性计划，提高企业的风险防范与抵御灾害的能力，降低灾难事件对企业的生产经营、市场形象、客户信誉及监管要求等方面造成的不良影响，确保业务的持续运行。因此业务连续性规划是实现业务连续性管理的基础环节和重要保证，二者之间的关系如图1.1所示。

图1.1 业务连续管理和业务连续规划的关系

构建业务连续性管理体系，不仅需要着眼于信息系统的备份与恢复，更重要的是构建业务连续性管理目标、策略、制度、组织和资源。业务连续性管理关注的内容包括：业务面临的威胁、灾难恢复资源需求、业务恢复策略和流程、灾难事件发生时的应急响应、接替生产运行、灾后重建、通知通告及危机管理，以及灾难恢复体系的运行、维护和验证。业务连续性管理的体系如图1.2所示。

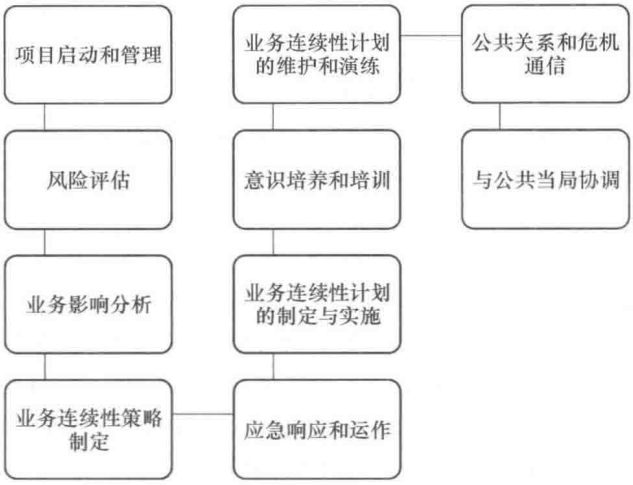

图1.2 业务连续性管理体系

1.1.4 灾难恢复的意义

(1) 必要性

随着集团化、跨地域经营，构架于IT系统之上的统一管理、统一决策、统一运营成了必然趋势。IT系统已成为企业的中枢系统，而作为承载IT系统运行的数据中心将作为企业业务数据存储和处理的核心系统，一旦出现数据丢失、网络中断、数据服务停止，将对企业的经营管理造成严重影响，并导致业务数据丢失、分支机构和业务网点的业务停顿，给企业带来的经济损失可能是无法挽回的。因此业务的重要程度越高，越有必要建立灾难恢复体系。

灾难恢复体系的建立，将为企业提供一个“保险”，一旦生产系统无法对外提供服务时，灾备系统将接管生产系统运行，当生产系统恢复后，灾备系统会将业务切换到生产系统运行。

随着科学技术的迅猛发展和信息技术的广泛应用，各行业对信息系统的依赖程度越来越高，特别是银行、电力、铁路、民航、证券、保险、海关、税务等行业的信息系统已经成为重要基础设施。信息系统的安全将直接影响到国民经济的正常运行，直接关系到社会稳定和人民群众的生活。但我国的信息安全防护能力还比较薄弱，安全保障能力还有待提高，目前仍有大部分企业没有建立灾难恢复体系，因此企业的信息安全和灾难恢复工作已刻不容缓。

(2) 重要性

随着近年来信息安全事件的发生给企业造成的损失，信息系统安全和灾难恢复工作已

经引起了国家、社会、企业的高度重视。信息安全和灾难恢复已成为企业管理者的重要职责，也是企业长期可持续发展的必然要求；信息安全与灾难恢复已逐渐纳入企业风险管理的范畴，并作为企业可持续发展的重要手段。

• 灾难恢复时保持业务连续运作和长期可持续发展的需要。

研究表明：未建立灾难恢复体系的企业比已建立灾难恢复体系的企业所面临的风险要高得多。以下是几组调查数据：

美国得克萨斯州大学的调查显示："只有 6%的公司可以在数据丢失后生存下来，43%的公司会彻底关门，51%的公司会在两年之内消失。"

美国明尼苏达大学的研究也表明，没有灾难恢复计划的企业在遭遇灾难时，有超过60%的企业在两到三年后退出市场。而随着企业对信息系统依赖程度的提高，此比例还有上升的趋势。

国际调查机构 Gartner Group 的调查显示：在经历大型灾难而导致系统停运的公司中有 2/5 再也没有恢复运营，剩下的公司中也有 1/3 在两年内破产。

企业的灾难恢复的能力是战略经营计划中极为重要的环节。灾难恢复体系的建设也是国际先进企业业务策略中的关键环节之一，是保证业务持续稳定运行的基础。灾难恢复体系建设的实质就是为企业的核心业务运作购买一份保险，保险公司只能为您现有的资产提供保险，但是灾难恢复大大提高了数据大集中后的风险防范能力，为企业的发展提供了有力的保障。

• 灾难恢复是加强风险管理，提高企业市场竞争力的重要手段。

树立稳健的、谨慎的、成熟的企业形象，是企业经营发展的重要命题。一个成熟的负责任的企业不但应当考虑到盈利能力和盈利手段，也应该考虑到未来面临的风险和风险防范能力。防范这些风险就意味着企业对业务伙伴和客户的长期承诺。灾难恢复不仅是为了企业业务数据保护和业务持续运行，也是对客户和合作伙伴的一种信心和信用的保证，是参与市场竞争的重要手段，在国际上有很多先进的理念和经验可以借鉴。美国 2002 年 7 月发布了 Sarbanes-Oxley 法案，对所有在美国注册的公司及在美国上市的公司提出了业务连续性要求；而美国、英国、新加坡等国家和中国香港地区的金融监管单位对银行、证券等行业的灾难恢复和业务连续规划有明确的要求；随着世界性分工和供应链的形成，是否拥有灾难恢复和业务连续性规划已经成为众多国家的政府机构与企业选择合作伙伴或供应商的一个必要条件，越来越体现出其重要性和迫切性。

• 灾难恢复是行业监管的需要。

灾难对企业的影响也会严重波及行业的发展。灾难恢复不仅是企业发展的要求，更是行业监管的需要。为有效防范行业信息系统风险，保护行业客户的合法权益，许多行业监管部门都出台了信息系统灾难恢复的相关监管要求。

• 灾难恢复是保证国家安全、人民利益、社会稳定和经济发展的需要。

国内外一系列已经发生的事件给我们提供了一个又一个的警示：如果没有应对风险的准备和灾难防范能力，一旦发生突发事件，将严重影响国民经济的发展和社会的稳定。因此，信息系统的灾难恢复工作是保证国家安全、人民利益、社会稳定和经济发展需要，因此从 2004 年开始，国家出台了一系列信息系统灾难恢复的相关标准和规范，可见，灾难恢复已上升到国家安全、人民利益、社会稳定和经济发展的高度。

(3) 新形势下的信息系统灾难恢复

随着网络技术和存储技术的发展，基于客户/服务器体系结构和浏览器/服务器体系结构的信息应用模式应运而生，高速信息交换、大容量数据存储等困扰IT人员多年的问题基本得到了解决。同时，过于分布的应用和数据所导致的日益昂贵的维护和运营费用，已经给单位的发展带来了束缚。数据的分散存储不利于资源的共享，与之相伴的是一个个存储和应用系统也成了孤岛，加大了管理难度，增加了成本。从中国工商银行20世纪90年代末的9991大集中工程开始，国内金融、电信、税务、海关等行业用户纷纷将数据进行整合，各地分公司的数据开始向总行或总部集中。实施数据大集中，可以消除信息孤岛，实现资源共享，加强对分支机构的监管和经营风险的管控，提高单位的经营管理能力。于是，数据大集中已经成为当前信息化领域中的一个热门的话题。

以银行为例，目前，银行信息化发展正逐步由信息资源建设阶段向信息资源运营阶段演进，支持持续提升信息系统整体效能的各个组成部分，如信息资源安全、整合、开发、配置、管理等，成为银行信息化发展的新趋势。数据大集中，有利于银行深化经营管理体制改革，增强风险防范能力，提高核心竞争力和创新能力，因此，数据集中是我国银行信息化最具代表性的发展趋势。从“十五”初期开始，我国银行普遍开始了数据大集中的规划与工程实施，各银行将原来分散在全国中心城市的小型数据处理中心，逐步集中到省的处理中心甚至全国性的大型数据处理中心，集中处理业务数据，数据大集中工程由此拉开序幕。

数据大集中是我国信息化发展的必然结果，同时，随着数据的集中，为业务信息系统的运行搭建了统一的数据平台，从而减少了数据维护的成本，提高了数据管理的效率，使业务得到了集中，技术风险的可控性提高，但风险的集中也随之而来。首先是数据量激增，对用户原有存储系统的容量提出了更高要求，容量的扩展势在必行；其次是数据如何在异构环境中实现更好的整合；最后，数据集中到一起，安全性问题变得更为重要，自然灾害、人为误操作都可能给数据中心带来致命打击，后果不堪设想，灾难备份与恢复工作必须提上议事日程。可以说，数据集中是一把双刃剑。因此，数据大集中赋予了信息安全保障工作的新的特点和任务，实施数据集中必须充分考虑灾难恢复工作的开展。

1.1.5 灾难恢复的发展

1. 国外灾难恢复的发展

灾难备份和恢复于20世纪70年代中期在美国起步，源于美国中西部地区对计算机设施进行的备份。灾难备份行业的历史性标志是1979年在美国宾西法尼亚州的费城建立了专业的商业化的灾备中心并对外提供服务。在这以后的10年里，美国的灾难备份行业得到了迅猛发展，拥有超过100家灾难备份中心服务商。1989年以后的十年中，灾难备份服务供应商之间进行了大规模的合并和重组，到1999年市场上剩下31个灾难备份中心服务商，并以每年15%的速度增长。

从1982年到1998年的约15年间，灾难恢复预案经受了大型灾难的考验，业务连续规划（BCP）开始出现，美国灾难备份行业成功地完成了582宗灾难恢复，平均每年约40宗。在这些灾难恢复中，44%的案例是发生了区域性的灾难使多个灾难备份服务客户同时受到影响，而从来没有出现客户因灾难备份中心资源不够而无法恢复的情况。灾难发

生最常见的原因是停电，接着是硬件损坏和火灾等。这582宗灾难分别由遍布全美的25间灾难备份中心进行了成功的恢复，对比于用户自己建设灾难备份的做法，灾难备份行业充分显示了其在提供专业可靠、低成本灾难备份服务方面的优势。

“9·11”事件后，Globe Continuity Inc. 对美国、英国、澳大利亚及加拿大的共565个公司使用灾难备份中心的情况进行了调查，发现在拥有或租用了灾难备份中心的公司中，56%使用了商业化的灾难备份服务，29%使用自有的灾难备份中心，15%在商业化灾难备份服务的基础上同时拥有自己的备份设施。两项相加，使用灾难备份服务的比例达到了71%。

从用户的行业划分来看，灾难备份行业面向的主要客户还是金融业。事实上，有近一半的灾难备份中心是专门为金融行业服务的。据CPR（Contingency Planning Research）估计，美国灾难备份行业的年销售额中有45%来自金融行业。

国外的灾难备份行业经过二十多年的发展已相当成熟，对外提供的服务主要包括：

（1）备份数据中心服务

备份数据中心服务主要为用户提供信息系统灾难恢复的场所和环境，备份数据中心服务模式包括：

- 热备份中心：为客户提供包括机房运行环境、数据处理设备和通讯端口在内的资源，一旦客户宣告灾难可切换到热备份中心运行。
- 冷备份中心：只为客户提供具备运行环境的机房空间。客户在宣告灾难后的一段时间内将使用灾难备份中心的热备份中心服务，然后就需要转入冷备份中心运行。
- 电子数据备份：从客户端将生产数据实时备份到灾备中心。
- 移动中心：这种服务面向的是规模相对较小的客户或一些紧急的情况。移动中心提供与冷备份中心相同的环境，其服务有两种模式：一种是利用拖车将集装箱模式的数据中心运送到客户指定地点；另一种模式是利用模块化数据中心运送到客户指定地点后进行快速组装。

（2）灾难恢复和业务连续性规划咨询

灾难备份服务供应商会向它的客户提供灾难恢复计划制定、业务连续性规划、风险管理等方面的顾问服务，同时也可以分别作为单独的服务进行提供。

（3）OEM保险服务

提供有限度的计算机设备损坏后更换服务，其收费与设备维护费用有关。

（4）快速运达服务

第三方的设备租赁公司经常向客户提供此项服务，即在需要时在规定的时间内将规定的设备送达客户指定地点。

西方发达国家重要机构都在远离中央信息中心的地方拥有一个灾难恢复系统，如美国的Wells Fargo Bank、法国的法兰西银行、新加坡的Citibank等。对于信息系统依赖程度较高的公司往往需要拿出IT总预算的7%到15%用于灾难恢复，每月要支付5万美元到10万美元的费用，大公司甚至达到100万美元/月。

2. 国内灾难恢复的发展

在国内，各行业用户对信息安全系统的建设越来越重视，其投入也呈现稳定增长的态势，但就单位信息化来说，大部分单位还没有有效的灾难恢复策略，没有建立统一的业务

连续性管理机制。

20世纪90年代末期，一些企业在信息化建设的同时，开始关注对数据安全的保护，进行数据的备份，但当时，不论从灾难恢复理论水平、重视程度、从业人员数量质量，还是技术水平方面都还很不成熟。

2000年，“千年虫”事件引发了国内对于信息系统灾难的第一次集体性关注，但“9·11”事件才真正地引起了大家对灾难恢复的关注。随着国内信息化建设的不断完善、数据大集中的开展和国家对灾难恢复工作的高度重视，越来越多的单位和部门认识到灾难恢复的重要性和必要性，开展灾难恢复建设的时机已基本成熟。21世纪初，国内灾难恢复专业服务商的出现以及灾难恢复外包和咨询项目的开展标志着国内灾难恢复市场的起步。中国的灾难恢复建设在经历几年的探讨之后，正逐步进入实践阶段。各地方政府和行业监管部门也在积极行动，制定灾难恢复的指导性意见，各单位开始计划或正在建设灾难备份中心。

2003年，中共中央办公厅、国务院办公厅下发了《国家信息化领导小组关于加强信息安全保障工作的意见》，文件要求：要高度重视灾难备份工作。为贯彻落实中央的指示，国务院信息化工作办公室于2004年9月下发了《关于做好重要信息系统灾难备份工作的通知》，文件强调了“统筹规划、资源共享、平战结合”的工作原则。为进一步推动八个重点行业加快实施灾难恢复工作，国务院信息化工作办公室于2005年4月下发了《重要信息系统灾难恢复指南》，文件指明了灾难恢复工作的流程、灾备中心的等级划分及灾难恢复预案的制定，使得数据备份与容灾的建设迈上了一个新的台阶。

近年来，各行业为了提高IT系统的可靠性，已逐步开展了IT系统的数据备份与容灾建设。随着各单位对灾难恢复的重视程度的提高，相关管理办法和规范的出台，2004年起中国灾难恢复市场开始初具规模。目前，国家部委、地方政府、银行、海关、税务等行业已经开展了灾难备份的设计、规划与实施。

目前，很多城市已经开始建设城市级政务灾备中心，有关部委也启动了行业灾难恢复规划项目，建立了部委级灾备中心，并相继出台了省市级灾备中心的监管要求。

银行电子信息化系统的安全稳定运行是银行在市场竞争中的生存基础，灾难恢复建设在银行业得到了普遍重视。中国人民银行发布了关于加强银行数据集中安全工作的指导意见，要求实施数据集中的银行必须建立相应的灾难备份中心，制定业务连续性计划，保障业务连续性及有效性。目前，各行都有数据级的备份措施，绝大部分银行的备份数据都能做到异地存放。中国人民银行已在无锡自建了灾难应急备份中心；三家政策性银行也都有建设灾难备份中心的考虑；深圳发展银行租用第三方的灾备中心已稳定运行；中国工商银行、福建兴业银行等单位目前已建成灾备中心，国家开发银行、中国银行、建设银行、广东发展银行等单位正在研究自建灾备中心或租用第三方的灾备中心。

同时，国内的灾难恢复工作还存在一些问题。部分单位对灾难恢复建设还存在概念模糊、应付领导、形象工程等现象，没有站在企业风险管控和信息安全的高度看待灾难恢复工作；很多地方政府和企业在没有进行统筹规划的前提下自行建设灾难备份中心，造成资源重复建设、资源大量闲置等情况；而建立灾难恢复体系的企业也存在良莠不齐的现象，部分企业缺乏专业化能力和完整、科学的灾难恢复方案，致使建立的灾备中心并不具备保证抵御灾害的能力，也不具备接替生产运行的能力；大部分企业建立的灾备系统未经过真

实切换演练，未能发挥灾难恢复的作用。

1.2 信息系统灾难恢复能力评估

信息系统的灾难恢复能力集中体现在规划设计能力、建设实施能力和运行维护能力三个方面，其评估是针对整个灾难恢复过程，从合规性、安全性、技术可行性、可操作性及可持续性对信息系统灾难恢复能力进行全面、客观、准确、综合地评估，以保证灾难恢复体系能满足机构灾难恢复的要求。

灾难恢复能力评估指标体系是对机构灾难恢复体系在技术和管理能力方面进行评估的依据，它将全面反映机构在灾难恢复体系的规划设计、建设实施及运行维护阶段所涉及的需求分析、策略制定、架构规划、建设实施方法、应急管理机制和运行维护手段等方面的能力。

1.2.1 灾难恢复相关标准与规范

灾难恢复标准规范是灾难恢复评估的基础，研究灾难恢复标准规范现状将为后续信息系统灾难恢复能力评估指标的提取及指标体系的建立提供思想指导与理论依据。

1. 灾难恢复国际标准

灾难恢复国际标准主要有 Share78。Share 是一个成立于 1955 年的计算机技术研究组织，其合作伙伴包括 IBM 等众多公司，该组织目前提供各种信息技术类的培训和咨询等服务。而 Share78 是该组织于 1992 年 3 月在 Anaheim 举行的一次盛会的编号，会上制定了一个有关远程自动恢复解决方案的标准。之后业界一直将此标准作为灾难恢复标准，成为灾难恢复国际标准。该标准的主要内容包括：

（1）备份或恢复的涵盖范围

（2）灾难恢复计划的状态

（3）业务中心与灾备中心间距离

（4）业务中心与灾备中心间互连方式

（5）数据在两中心间传送方式

（6）数据允许丢失量

（7）如何保证数据一致性

（8）灾备中心进入灾备进程的能力

除 Share78，国际上还有一些应用较广泛的灾难恢复标准。例如国际灾难恢复协会（DRII，Disaster Recovery Institute International）的 *Generally Accepted Practices for Business Continuity Practitioners*，作为详细的过程等级文档，提供发展业务连续性项目的指导、建议和清单；ISO 24762《信息与通信技术灾难恢复服务指南》，通过向作为业务连续性管理的一部分的信息与通信技术灾难恢复（ICTDR）服务提供指南，来协助信息安全管理体系的运行；ASIS/BSI *Business Continuity Management Standard*，基于 BS 25599两个部分，定义了商业业务连续性管理系统等要求；ISACA Doc. G32 *IT Auditing Guideline*：*Business Continuity Plan*，针对信息技术审计和控制标准方面提供评估业务连续性计划审计指导等，这些标准均从业务连续性方面对灾难恢复实践及要求进行了

规定。

2. 灾难恢复国家标准

美国9·11事件发生后，灾难恢复在世界范围的受重视程度达到一个新的高度，各国立足本国实际情况出台的灾难恢复标准层出不穷，9·11事件之后几年发布的灾难恢复标准数量甚至超过9·11事件之前十几年的总和。各国的国家标准中比较具有代表性的有以下国家。

(1) 美国

NFPA 1600：2006 *Standard on Disaster/Emergency Management and Business Continuity Programs*，美国国家标准，针对应急管理和业务连续性的标准，包括对业务连续性详细的指导；美国国家标准和技术学会（NIST）信息技术实验室（ITL）制定的SP 800-12 *Contingency Planning Guide for Information Technology Systems*，针对信息技术灾难恢复的详细的指导和建议；美国联邦紧急事务管理局（FEMA）制定的FPC 65 *Federal Preparedness Circular*：*Federal Service Operation Continuity*，针对业务连续性提出详细要求。

(2) 英国

BS 25999-1：2006，BS 25999-2：2007 *Code of Practice and Specification for Business Continuity Practitioners*，英国国家容灾行业标准，为建立和管理一套业务连续性管理系统提供指导、建议及要求。

(3) 加拿大

加拿大标准协会制定的CAN/CSA-7731-M95 *National Standard Emergency Planning for Industry*，即工业紧急计划国家标准，侧重风险分析与紧急响应的要求等。

(4) 澳大利亚

澳大利亚国家审计局（ANAO）制定了针对业务连续性管理要求的 *Business Continuity Management*：*Keeping the wheels in motion*、针对商业连续性管理与应急管理的 *Business Continuity Management and Emergency Management in Centre link* 以及针对审计业务连续性管理要求的 *Business Continuity Management Follow-on Audit* 等。

(5) 新加坡

新加坡金融管理局制定了《业务应急计划指导方针》(Guidelines On Business Continuity Planning)，用于指导金融机构制定业务应急计划的原则。

在各国灾难恢复国家标准中，美国与英国出台的国家标准得到更广泛的关注与使用。

3. 国内灾难恢复标准与规范

信息系统灾难恢复建设在我国国内也得到了高度重视，政策支持逐级加深，其标准规范的发展历程简述如下。

(1)《国家信息化领导小组关于加强信息安全保障工作的意见》

2003年7月，温总理在国家信息化小组第三次会议上要求，重要系统建设要充分考虑抗毁性与容灾性，随后，于当年9月发布该文件。该文件提倡资源共享互备，加强信息安全应急服务队伍建设，鼓励社会力量参与灾难恢复建设，提高信息安全能力。

(2)《关于加强国家重要信息系统灾难备份工作的意见》

2004年9月，由国务院信息工作办公室下发，要求国家重要信息系统灾难恢复要坚