第五章　灾难恢复与业务连续性

本章提纲

§1 概述

§2 数据备份

§3 灾难恢复

§4 业务连续性

§1 概述

灾难的定义

- 灾难(Disaster) 是导致重大损失的突发的不幸事件

§1 概述

灾难的危害

- Gartner分析报告:
  - 2/5公司经历大灾难后再也不能恢复运作
  - 1 /3公司经历大灾难后在2年内倒闭
- 明尼苏达大学研究:
  - 两周内不能恢复运作， 75%企业完全停顿
  - 两周内不能恢复运作， 43%企业再无法恢复

§1 概述

- 灾难
  - ✓ 具有破坏性的突发事件
  - ✓ 发生原因：自然灾害、技术故障、人为因素等
- 灾难恢复
  - ✓ 指当系统崩溃时为将其恢复到正常运行状态所需的操作
  - ✓ 目的：减轻灾难对单位和社会带来的不良影响，保证信息系统关键业务功能在灾难发生后能及时恢复和继续运作

§1 概述

灾难备份

- 定义：为灾难恢复而对数据、数据处理系统、网络系统、基础设施、技术支持与运行管理能力等进行备份的过程
- 关系：是灾难恢复的基础
- 类别：软件级备份、硬件级备份

数据备份

- 定义：为达到数据恢复和重建目标所进行的一系列备份步骤和行为
- 关系：灾难发生后，利用数据备份实现主系统的还原恢复，是灾难恢复的有效手段

§1 概述

➢ 业务连续性

- ✓ 定义：指组织为了维持其生存，一旦发生突发事件或灾难后，在其所规定的时间内必须恢复业务功能的强制性要求
- ✓ 关系：灾难恢复是在灾难发生时确保组织正常经营保持连续性的过程
- ✓ 业务连续性管理：对单位潜在风险加以评估分析，确定其可能造成的威胁，并建立完善的管理机制以防止或减少灾难事件给单位带来的损失

本章提纲

§1 概述

§2 数据备份

§3 灾难恢复

§4 业务连续性

§ 2. 数据备份

§ 2.1 备份策略

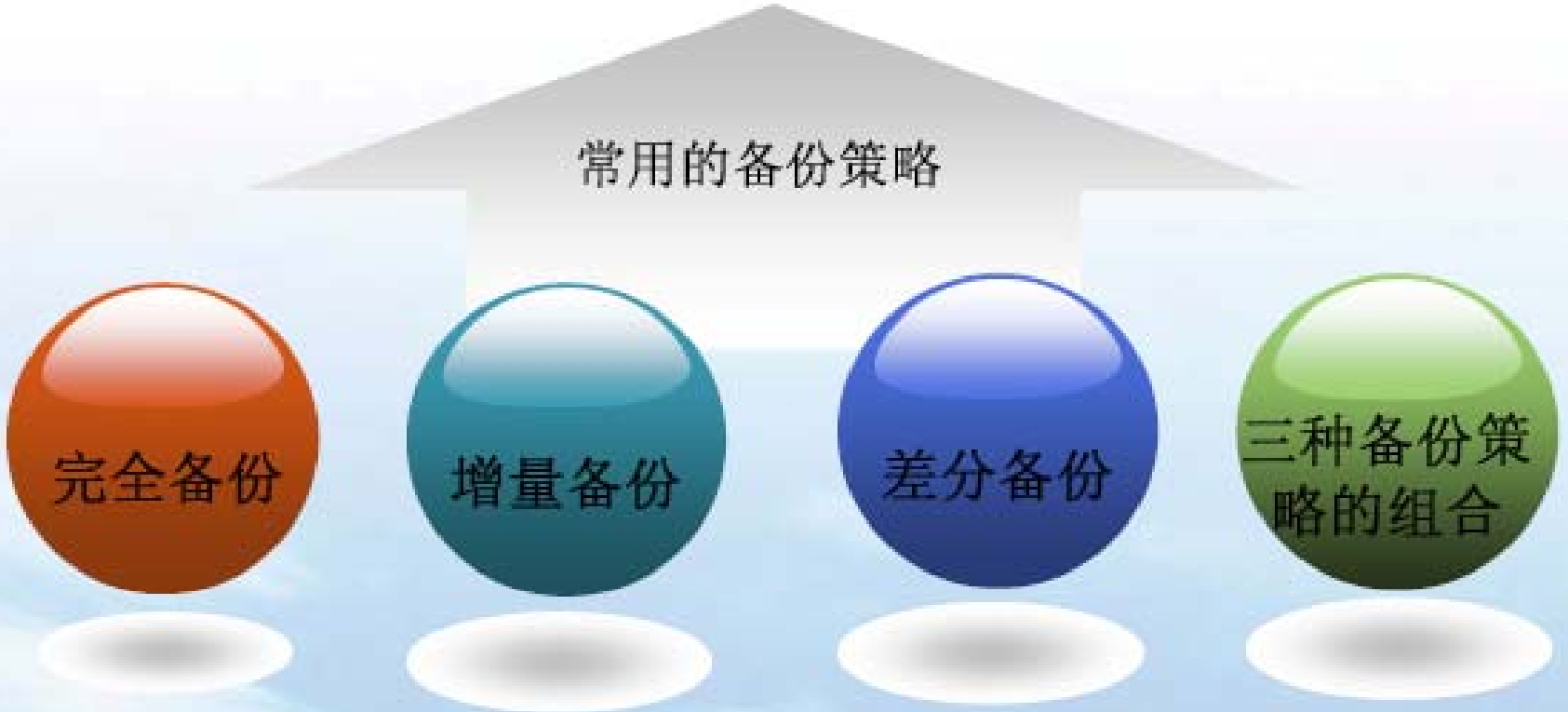
§ 2.2 备份分类

§ 2.3 备份技术

§ 2.4 数据恢复工具

§2.1 备份策略

确定需要备份的内容、备份方式以及备份介质。



完全备份

- **要求：**每天对系统进行完全备份，例如，每天用不同盘磁带对系统进行备份

✓ 优点

- 灾难恢复方便

✓ 缺点

- 备份的数据量大，成本增加
- 备份所用时间较长

增量备份

- **要求：**在周日进行一次完全备份，接下来的六天里只对当天新的或被修改过的数据备份

✓ 优点

- 节省存储，缩短备份时间

✓ 缺点

- 灾难恢复麻烦
- 可靠性差

差分备份

- **要求：**在周日进行一次完全备份，接下来的六天里，对当天所有与周日不同的数据（新的或修改过的）备份

✓ 优点（继承了前两种策略的优点）

- 节省存储，缩短备份时间
- 灾难恢复方便

✓ 缺点

- 避免了前两种策略的缺陷

综合型完全备份

- 要求：从前三种备份中读取信息，创建一个新的完全备份
- ✓ 优点（继承了前两种策略的优点）
  - 离线进行，不减低系统性能或妨碍网络用户
  - 当备份时间较短时进行

备份策略选择

- 决定采用何种备份方式取决于两大因素：

✓ 备份窗口

- 完成一次给定备份所需的时间
- 由数据总量和处理速度决定

✓ 恢复窗口

- 恢复整个系统所需的时间
- 取决于网络负载和磁带库性能及速度

备份策略选择

- 实际应用中，决定采用何种备份方式须依据
  - ✓ 备份窗口的大小
  - ✓ 恢复窗口
  - ✓ 数据量
- 通常，采用完全备份结合差分备份的方式较为适宜

§2.2 备份分类

- 按备份策略分类
  - ✓完全备份
  - ✓增量备份
  - ✓差分备份
  - ✓综合型完全备份

§2.2 备份分类

- 按备份状态分类
  - ✓物理备份
    - 指将实际物理数据从一处复制到另一处的备份
    - 冷备份：脱机备份，指正常关闭数据库，对数据库所有文件备份
    - 热备份：联机备份，指在数据库打开和用户对数据库进行操作的状态下进行的备份
  - ✓逻辑备份
    - 将某个数据库的记录读出并将其写入到一个文件中

§2.2 备份分类

- 按备份层次分类
  - ✓硬件备份
    - 指通过硬件冗余实现的备份
    - 现有的硬件冗余技术有：双机容错、磁盘阵列（RAID）、磁盘镜像等
  - ✓软件备份
    - 理想的备份系统：使用硬件容错来防止硬件故障，使用软件备份和硬件容错相结合方式解决软件故障或人为误操作造成的数据丢失

§2.2 备份分类

- 按备份地点分类
  - ✓本地备份
    - 备份的数据存放在本地
    - 缺点：抗重大灾害的能力差
  - ✓异地备份
    - 数据异地存放
    - 优点：安全性较高
    - 缺点：成本较高

§2.2 备份分类

- 按灾难恢复的层次分类
  - ✓数据级备份
    - 用以对主系统关键业务数据进行备份
  - ✓系统级备份
    - 除进行业务数据备份外，对信息系统的系统数据、运行场景、参数设置等信息进行备份，以恢复整个系统
  - ✓应用级备份
    - 同时进行业务数据和业务应用的异地备份，以向用户提供不间断的应用服务

§2.3 备份技术

- 数据复制技术
  - ✓数据复制方式
    - 同步方式、异步方式
    - 保证数据完整性和一致性
  - ✓数据复制形式
    - 卷、文件、数据库
  - ✓数据复制层次
    - 硬件级、操作系统级、数据库级、业务数据流级等四种类型的数据复制

§2.3 备份技术

- **冗余技术**：通过硬件设备冗余实现备份，通过配备与主系统相同的硬件设备保证系统和数据的安全性
  - ✓现有的硬件冗余技术
    - 双机容错
    - 磁盘双工
    - 磁盘阵列
    - 磁盘镜像：在两个或多个磁盘或磁盘子系统上产生同一个数据的镜像视图的信息存储过程

§2.4 数据恢复工具

- FinalData
  - ✓强大的数据恢复功能
    - 针对误删除、物理故障、磁盘格式化等均可恢复
    - 甚至部分覆盖后亦可能恢复
  - ✓操作简便易用
    - 无需培训即会使用
  - ✓网络恢复功能
    - 对网络上其他计算机丢失文件进行恢复

§2.4 数据恢复工具

- EasyRecovery
  - ✓专为硬盘恢复准备的数据恢复工具
    - 从格式化的硬盘恢复数据
    - 分区损坏恢复
    - 多次格式化的硬盘数据恢复
  - ✓恢复软盘中删除的文件
  - ✓用户日常PC的基础工具

§2.4 数据恢复工具

- ExcelRecovery
  - ✓专门修复Excel电子表格数据的文件
    - 支持多种格式的Excel文件
    - 恢复损坏的表格单元数据
    - 修补受损的多重分页文件结构

本章提纲

§1 概述

§2 数据备份

§3 灾难恢复

§4 业务连续性

§3 灾难恢复

§3.1 确定需求

§3.2 制定策略

§3.3 实现策略

§3.4 等级划分

§3.1 确定需求

风险分析

- ✓标示信息系统的资产价值
- ✓识别信息系统面临的自然和人为威胁
- ✓识别信息系统的脆弱性
- ✓分析各种威胁发生的可能性，并定量或定性描述可能发生的损失
- ✓通过技术和管理手段，防范或控制信息系统的风险

业务影响分析

- 分析业务功能和相关资源配置
  - ✓对各项业务功能及其之间的相关性进行分析
  - ✓确定支持各种业务功能的相应信息系统资源及其他资源
  - ✓明确相关信息的保密性、完整性和可用性要求
- 评估中断影响
  - ✓定量分析：评估直接和间接经济损失
  - ✓定性方法：运用归纳与演绎、分析和综合以及抽象和概括等方法，评估业务功能中断可能给组织带来的非经济损失，包括组织声誉、社会影响等

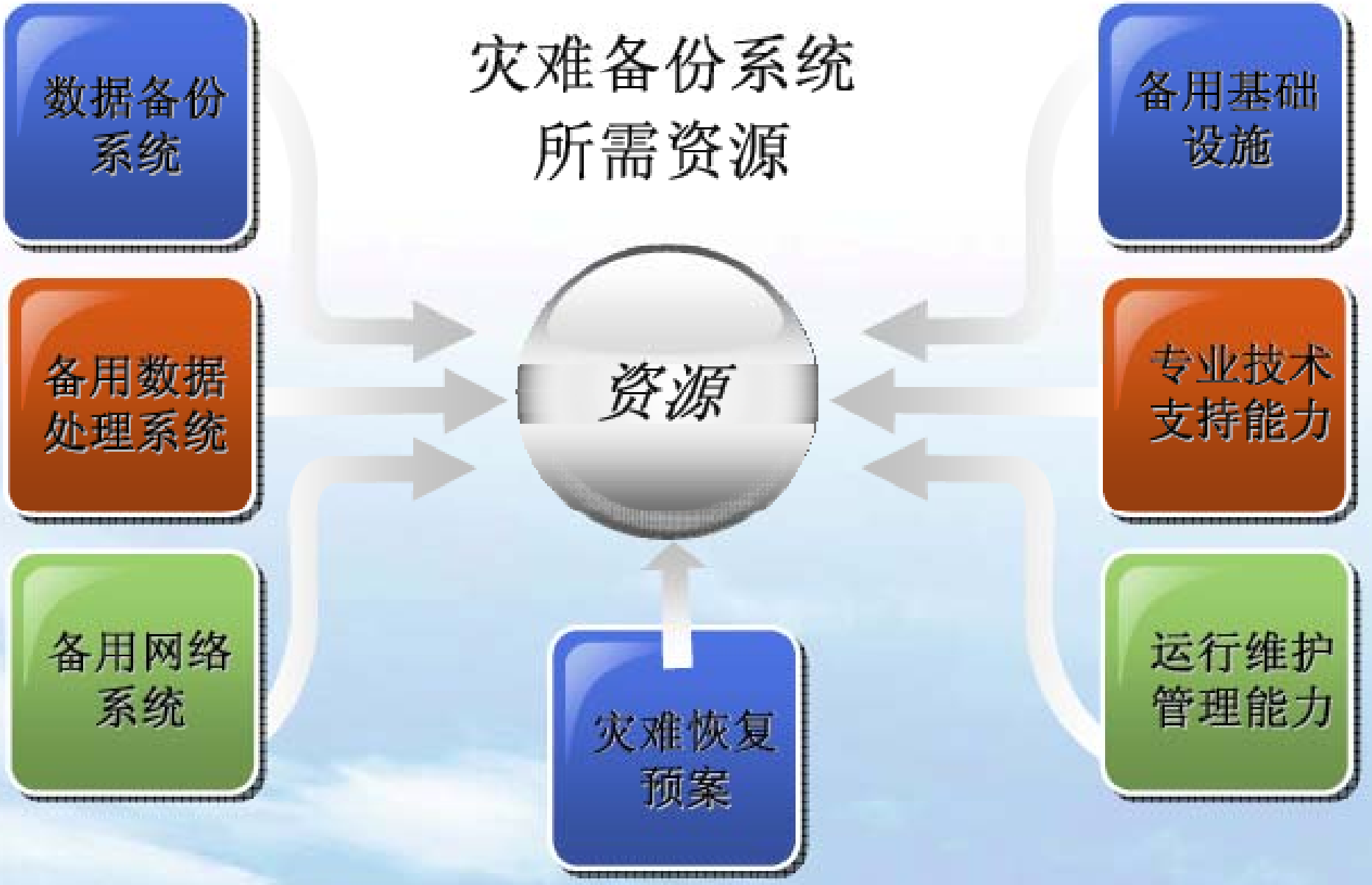
确定灾难恢复目标

- 根据风险分析和业务影响分析的结果，确定灾难恢复目标，包括：
  - ✓关键业务功能及恢复的优先顺序
  - ✓灾难恢复时间范围

§3.2 灾难恢复策略的制定

- 灾难恢复策略包括：
  - ✓灾难恢复资源的获取方式
  - ✓灾难恢复等级各要素的具体要求

§3.2 制定策略


灾难备份系统
所需资源
数据备份系统
备用数据处理系统
备用网络系统
资源
灾难恢复预案
备用基础设施
专业技术支持能力
运行维护管理能力

数据备份系统

- 概念
  - ✓一般由数据备份的硬件、软件和数据备份介质组成，如果是依靠电子传输的数据备份系统，还包括数据备份线路和相应的通信设备
- 资源获取方式
  - ✓可自行建设，也可通过租用其他机构的系统而获取
- 资源要求
  - ✓数据备份的范围
  - ✓数据备份的时间间隔
  - ✓数据备份技术及介质
  - ✓数据备份线路的速率及相关通信设备的规格和要求

备用数据处理系统

- 概念
  - ✓ 指备用的计算机、外围设备和软件
- 资源获取方式
  - ✓ 事先与厂商签订紧急供货协议
  - ✓ 事先购买所需的数据处理设备并存放在灾难备份中心或安全的设备仓库
  - ✓ 利用商业化灾难备份中心或签有互惠协议的机构已有的兼容设备
- 资源要求
  - ✓ 数据处理能力
  - ✓ 与主系统的兼容要求
  - ✓ 平时处于就绪还是运行状态

备用网络系统

- 概念
  - ✓ 最终用户用来访问备用数据处理系统的网络，包含备用网络通讯设备和备用数据通信线路
- 资源获取方式
  - ✓ 备用网络通信设备可通过与获取备用数据处理系统相同的方式获取
  - ✓ 备用数据通信线路可使用自有数据通信线路或租用公用数据通信线路
- 资源要求
  - ✓ 选择备用数据通信的技术和线路带宽，确定网络通信设备的功能和容量，保证灾难恢复时，最终用户能以一定的速率连接到备用数据处理系统

备用基础设施

- 概念
  - ✓ 灾难恢复所需的、支持灾难备份系统运行的建筑、设备和组织，包括介质场外的存放场所、备用的机房及灾难恢复辅助设施，以及容许灾难恢复人员连续停留的生活设施
- 资源获取方式
  - ✓ 由组织所有或运行
  - ✓ 多方共建或通过互惠协议获取
  - ✓ 租用商业化灾难备份中心的基础设施
- 资源要求
  - ✓ 与主中心的距离要求
  - ✓ 场地和环境要求
  - ✓ 运行维护和管理要求

专业技术支持能力

- 概念
  - ✓ 对灾难恢复系统的运转提供支撑和综合保障的能力，以实现灾难恢复系统的预期目标。包括硬件、系统软件和应用软件的问题分析和处理能力、网络系统安全运行管理能力、沟通协议能力等
- 资源获取方式
  - ✓ 灾难备份中心设置专职技术支持人员
  - ✓ 与厂商签订技术支持或服务合同
  - ✓ 由主中心技术支持人员兼任
- 资源要求
  - ✓ 确定灾难备份中心在软件、硬件和网络等方面的技术支持要求，包括技术支持的组织架构、各类技术支持人员的数量和素质等要求

运行维护管理能力

- 概念
  - ✓包括运行环境管理、系统管理、安全管理和变更管理等
- 资源获取方式
  - ✓自行运行和维护
  - ✓委托其他机构运行和维护
- 资源要求
  - ✓确定灾难备份中心运行维护管理要求，包括运行维护管理组织架构、人员的数量和素质、运行维护管理制度等要求

灾难恢复预案

- 概念
  - ✓ 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，用于指导灾难恢复
- 资源获取方式
  - ✓ 由组织独立完成
  - ✓ 聘请具有相应资格的外部专家指导完成
  - ✓ 委托具有相应资格的外部机构完成
- 资源要求
  - ✓ 整体要求
  - ✓ 制定过程的要求
  - ✓ 教育、培训和演练的要求
  - ✓ 管理要求

§3.3 灾难恢复策略的实现

- 1. 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
- 2. 灾难备份中心的选择和建设
  - ✓选址原则
  - ✓基础设施的要求
- 3. 技术支持能力的实现
- 4. 运维管理能力的实现
- 5.灾难恢复预案的实现

§3.4 灾难恢复的等级划分

- 依据灾难恢复的系统和数据的完整性要求及时间要求等要素将灾难恢复划分为6个等级
  - ✓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：电子传输和完整设备支持
  - ✓第5级：实施数据传输和完整设备支持
  - ✓第6级：数据零丢失和远程集群支持

本章提纲

§1 概述

§2 数据备份

§3 灾难恢复

§4 业务连续性

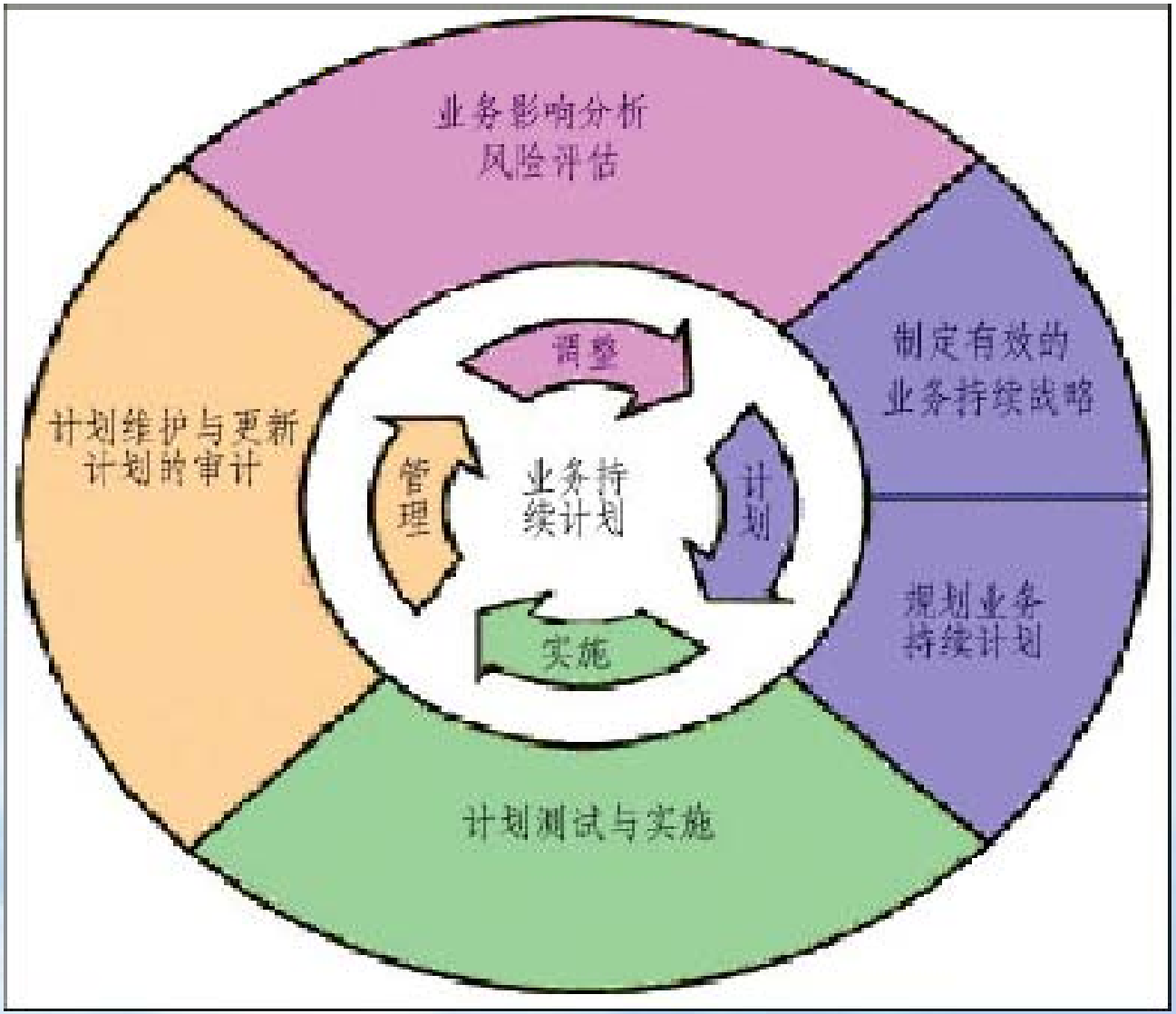
业务连续性管理

- 业务连续性管理（Business Continuity Management，缩写为BCM）是一个全面、持续的过程， 包括：
  - ✓识别威胁组织的潜在影响
    - 保证数据完整性和一致性
  - ✓提供一个框架
    - 用于指导组织提升应对灾难和持续运营的能力
    - 用于保障组织的主要股东利益，以及公司的声誉、品牌和其他创造价值的活动

业务连续性管理

- BCM目标
  - ✓提升组织的持续运营能力。通过事先发现组织中由各种突发业务中断所造成的潜在影响，协助组织排定各种业务恢复先后顺序，最终实现各领域业务的持续运营

BCM过程



BCM生命周期

BCM过程

- BS7799所描述的BCM主要有以下要点：

  - ◆业务持续计划首先是组织高层管理人员的首要职责，因为他们被委任保护公司的资产及公司的生存；
  - ◆制定和实施一个完整的业务持续计划应从理解自身业务开始，进行业务影响分析和风险评估；
  - ◆由组织高层管理者形成本企业的业务持续性战略方针，然后规划业务持续性计划；
  - ◆进行计划的测试与实施；
  - ◆进行计划的维护与更新，通过审计保证计划不断改进和完善。

业务影响性分析

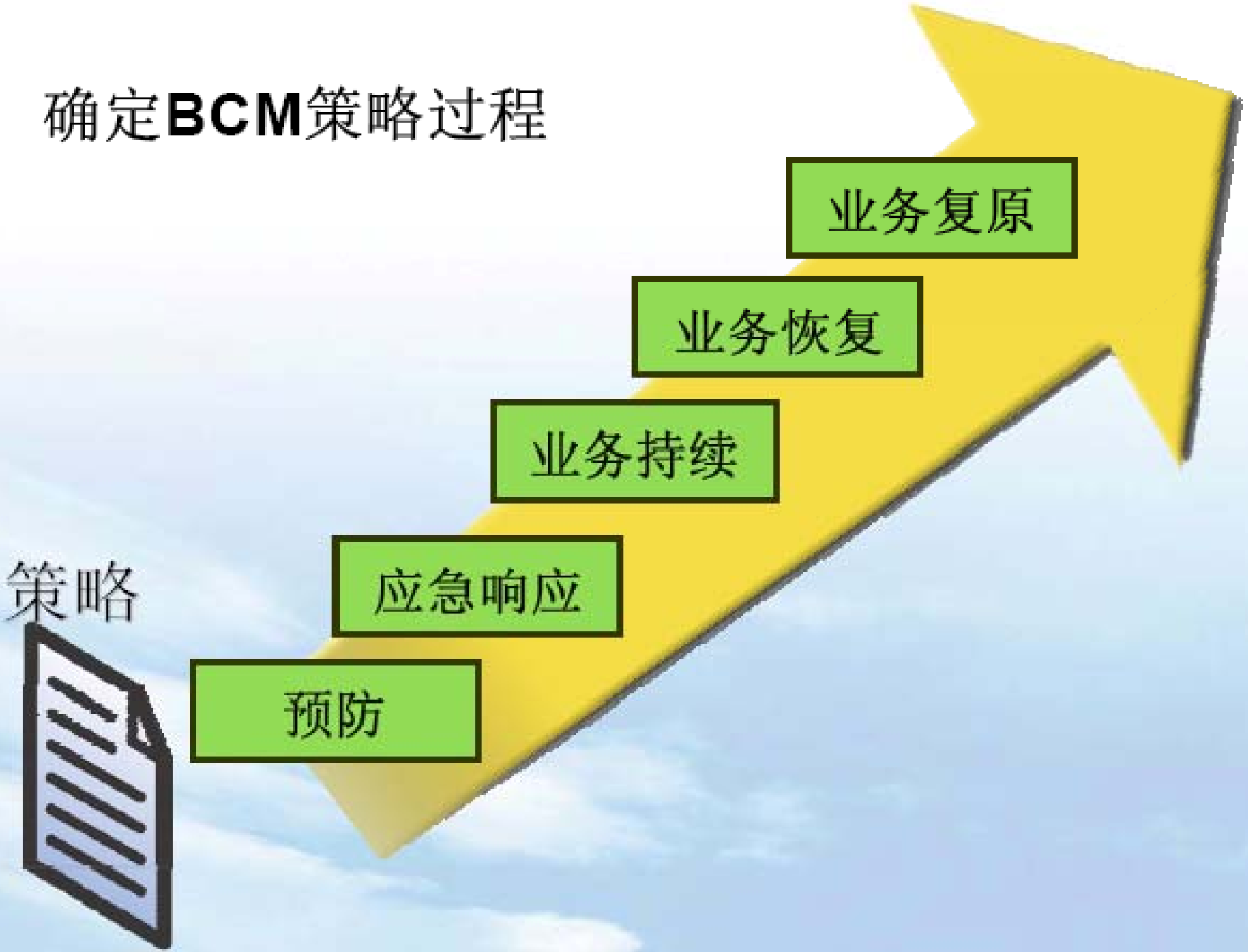
- 业务影响分析（Business Impact Analysis, BIA）
  - ✓实质上是对关键性的企业功能，以及当这些功能一旦失去作用时可能造成的损失和影响的分析
  - ✓BIA是整个BCM流程的工作基础
- BIA的作用
  - ✓识别关键的业务功能及其支持方面的不足
  - ✓分析中断事件造成的影响
  - ✓分析业务功能的中断忍受程度和恢复的优先顺序

业务影响性分析

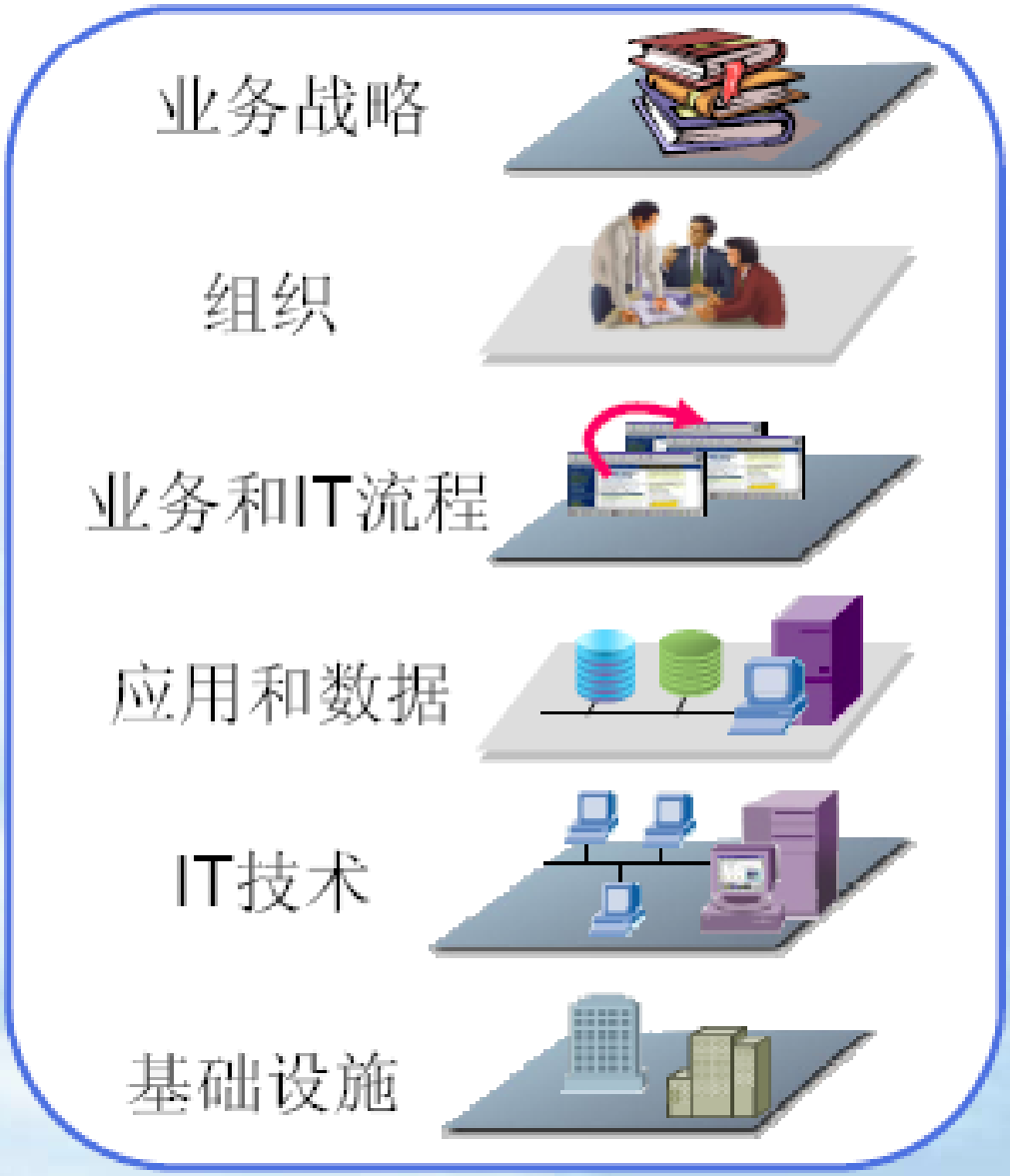
BIA过程

- 确定信息收集技术
  - 讨论（Discussion)）
  - 调查问卷（questionnaires）
  - 访谈（Interview）
- 选择受访者
- 识别关键业务功能及其支持资源
- 确定最大允许中断时间（ MTD）
- 识别弱点和威胁
- 分析风险
- 向管理层汇报BIA结果
  - 存在的问题
  - 应对建议

确定BCM策略过程



BCM建设思路



- 制定BCM建设战略
- 增加人员BCM意识

- 建立BCM组织
- 确定角色和职责

- 确定业务和IT流程
- 建立恢复流程和恢复计划

- 实时或定期备份数据和程序
- 定期检查备份数据的有效性

- 构建灾难备份系统
- 应用高效存储设备

- 建立灾备中心
- 营建灾备IT基础环境

BCM计划制定

BCM计划

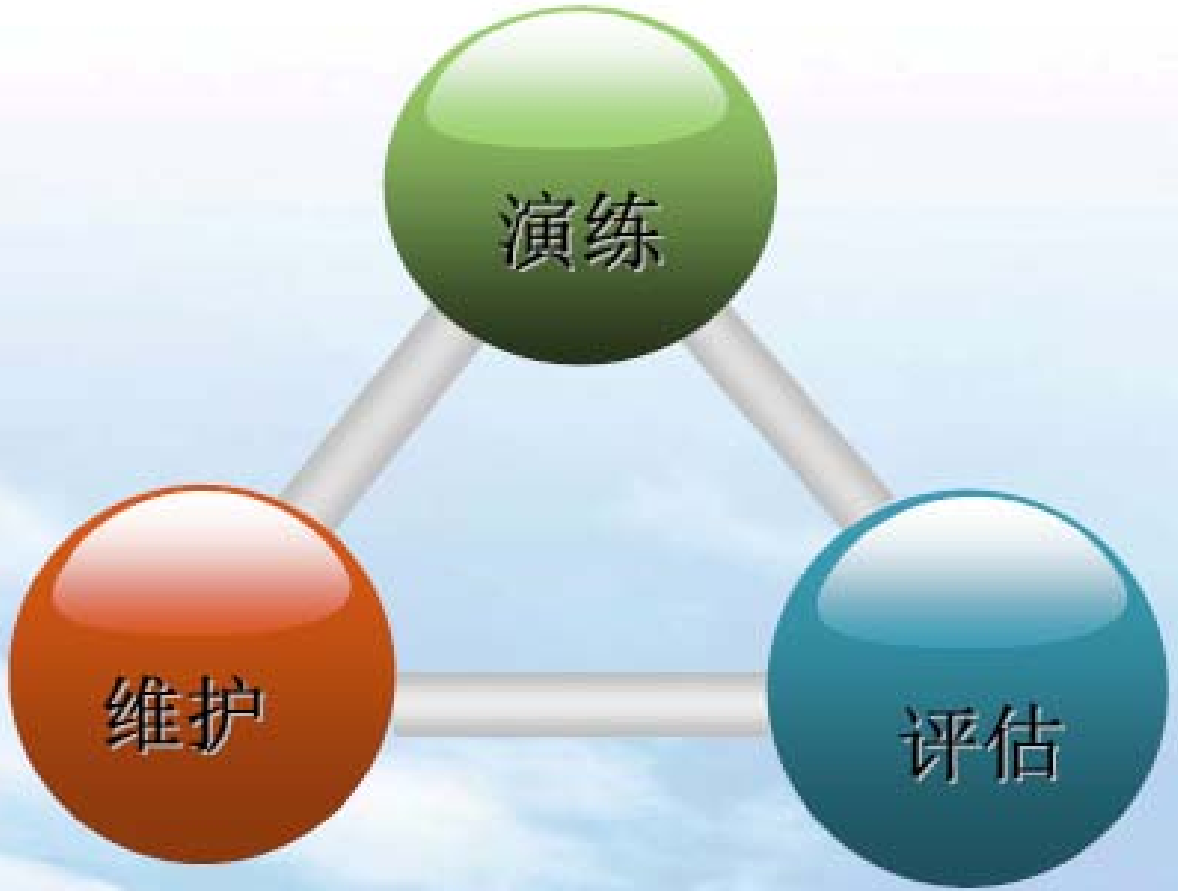
- 通知/启动阶段
- 恢复阶段
- 重建阶段
- 计划的附录

BCM团队

- 服务器恢复小组
- L AN/WAN恢复小组
- 数据库恢复小组
- 网络运行恢复小组
- 应用程序恢复小组
- 电信恢复小组
- 硬件拯军救小组
- 测试小组
- 行政支持小组
- 运输布置小组
- 媒体公关小组
- 法律事务小组
- 物理/人员安全小组
- 采购小组

BCM演练、维护与评估

通过演练、维护和评估，确保组织的 BCM 策略、预案和契约安排的高效性，并保持更新到最新状态。



BCM演练、维护与评估

演练

- 只有经过演练验证后，才能确认 BCM 的水平及能力。
- 演练有多种形式，包括技术测试、桌面演练和实战演练等。
- 演练所需的时间和资源是演练工作的重要组成部分。

维护

- 大部分的组织都处于变化的环境之中，为了保证组织的 BCM 能力适应自身的特性，必须满足及时性、正确性、完整性等要求。
- 须制定业务持续性管理制度，以保障所有利益相关方都能得到与其相关的 BCP 内容。

评估

- 内部审计。
- 外部审计。
- 自我评估。

小结 —— 灾难恢复

- 计算机系统经常会因各种原因不能正常工作，会损坏或丢失数据，甚至整个系统崩溃。为了不影响工作，将损失减少到最低程度，我们一般通过备份技术保留用户甚至整个系统数据，当系统不正常时可以通过该备份恢复工作环境
- 数据备份
  - ✓备份策略、备份分类、备份技术、数据恢复工具
- 灾难恢复
  - ✓确定需求、制定策略、实现策略、等级划分

小结 —— 业务连续性

- 业务连续性是指组织为了维持其生存，一旦发生突发事件或灾难后，在其所规定的时间内必须恢复关键业务功能的强制性要求

  - ✓BCM概述
  - ✓业务影响分析
  - ✓BCM制定和实施
  - ✓BCM演练和维护