第9章　业务连续性与灾难恢复

信息安全管理

主讲　李章兵

内容

- 9.1 业务连续性管理BCM
  - 9.1.1 BCM概念与规划
  - 9.1.2 业务影响分析BIA
  - 9.1.3 应急响应
  - 9.1.4 确定BCM策略
  - 9.1.5 BCM开发和实施
  - 9.1.6 BCM演练和维护
- 9.2 灾难恢复

教学目标

- 本章的重点是
  - 业务连续性管理
  - 数据备份与容灾
  - 灾难恢复

9.1 BCM概念与过程

- 9.1.1 BCM概念与规划
  - 业务连续性管理BCM
    - Business Continuity Management
    - 业务连续性管理是对机构或组织的潜在风险加以评估分析，确定其可能造成的威胁，并建立一个完善的管理机制来防止或减少灾难事件给组织带来的损失。
    - 是一个全面、持续的过程， 包括：
      - 识别威胁组织的潜在影响；
      - 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。

9.1 BCM概念与过程

- 9.1.1 BCM概念与规划
  - 业务连续性管理BCM
    - 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，最终实现各业领域的业务持续运营。

9.1 业务连续性管理BCM

- 9.1.1 BCM概念与规划
  - BCM好处
    - 确保组织及时响应生死攸关的灾难性事件；
    - 提升组织风险意识、同时满足规范和应对特殊风险的要求；
      - 合理计划BCM 。
    - 提升组织自身竞争力；
      - 通过BCM争取新的客户、提高利润， 并且能增加"客户关怀度" 。
    - 最大限度发现低效的业务和平时无法揭露的隐患；
    - BCM预防措施成本低。
      - 提前采取要比临时采取措施所花费用低。

9.1 业务连续性管理BCM

- **9.1.1 BCM概念与规划**
  - **BCM过程： BS7799描述**
    - 业务持续计划是组织高层管理人员的首要职责；
      - 组织高层管理人员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。

9.1 业务连续性管理BCM

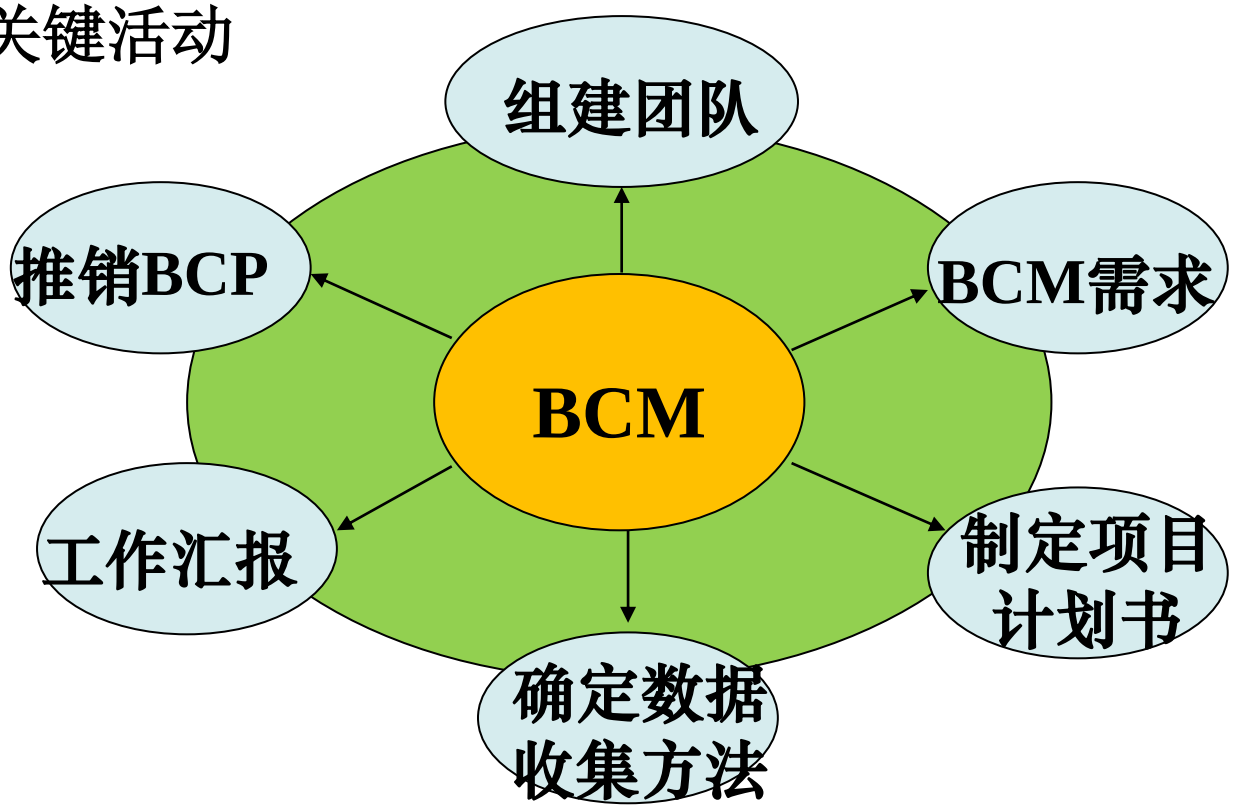
- 9.1.1 BCM概念与规划
  - BCM生命周期

9.1 业务连续性管理BCM

- 9.1.1 BCM概念与规划
  - BCM规划
    - 业务持续计划BCP
      - "天要塌了，我们如何照常运转"
      - 业务
      - 持续(Continuity)
    - 灾难恢复计划DRP
      - "天已经塌了，我们如何恢复原貌"
      - IT
      - 恢复(Recovery)
    - BCP VS DRP

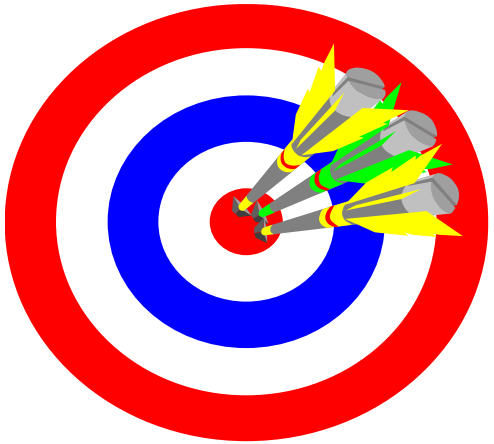
9.1 业务连续性管理BCM

- 9.1.1 BCM概念与规划
  - BCP项目准备
    - 关键活动



9.1 业务连续性管理BCM

- 9.1.1 BCM概念与规划
  - BCP项目准备
    - BCM策略要求



BCM策略要求

- 目的
- 范围
- 需求
- 基本原则
- 指导方针
- 职责
- 责任
- 关键环节的原则要求
- 得到高级管理层的正式批准

9.1 业务连续性管理BCM

- 9.1.1 BCM概念与规划
  - BCP项目准备

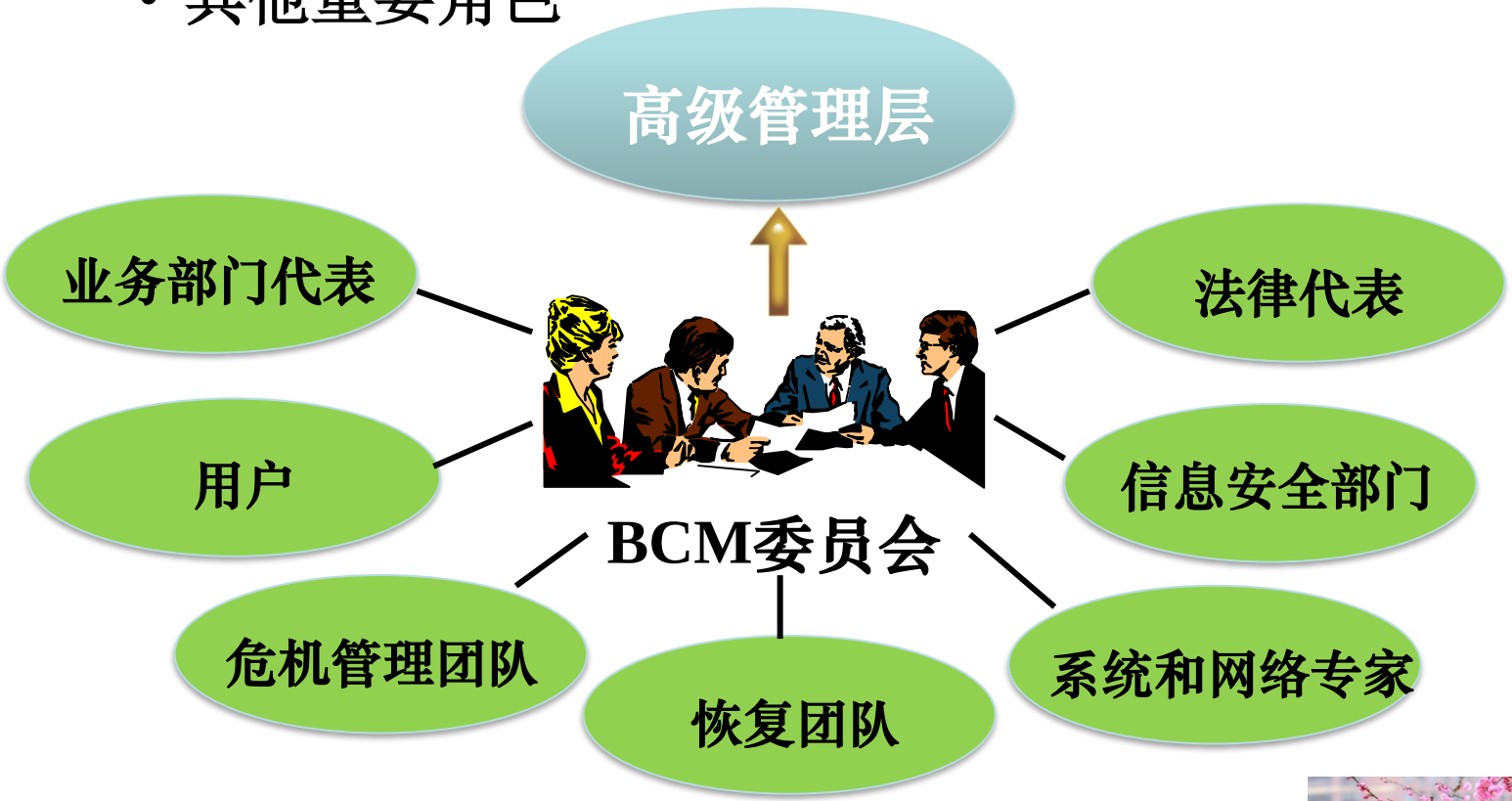
项目计划
- 目标与任务（Objective-to-task mapping）
- 任务与资源（Resource-to-task mapping）
- 里程碑
- 预算
- 成功因素
- 关键环节的原则要求

9.1 业务连续性管理BCM

- 9.1.1 BCM概念与规划
  - BCP角色和职责
    - BCM项目负责人
      - 全面负责项目的规划、准备、培训、协调等各项工作。
        - » 接触高级管理层
        - » 影响高级管理层的决策
        - » 与管理层的沟通和联络
        - » 组建和领导BCM委员会
        - » 与计划相关所有人员进行直接接触和沟通
        - » 了解机构业务使命和高级管理层的意图
        - » 充分了解中断对机构业务的影响
        - » 熟悉机构的需求和运作，有能力平衡相关部门的不同需求

9.1 业务连续性管理BCM

- 9.1.1 BCM概念与规划
  - BCP角色和职责
    - 其他重要角色



9.1 业务连续性管理BCM

- 9.1.2 业务影响分析BIA
  - Business Impact Analysis
    - 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；
      - 确定业务功能之间的依赖关系
    - 分析中断事件造成的影响。
      - 定量(Quantitative)分析、定性(Qualitative) 分析
    - 分析业务功能的中断忍受程度和恢复的优先顺序
      - 确定业务功能的最大允许中断时间（MTD）
      - 确定恢复点目标（RPO)

9.1 业务连续性管理BCM

- 9.1.2 业务影响分析BIA
  - 业务中断的影响
    - 收入的损失
    - 延迟收入的损失
    - 生产力的损失
    - 营运成本的增加
    - 声誉和公众信任的损失
    - 竞争力的损失
    - 违约责任
    - 违背法律法规

9.1 业务连续性管理BCM

- 9.1.2 业务影响分析BIA
  - 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

9.1 业务连续性管理BCM

- 9.1.2 业务影响分析BIA
  - 信息收集
    - 开会讨论：能够加速得出分析结论，同时要和各个部门进行激烈的争论，最终达成一致的BIA结论。
    - 调查问卷：能提供大量的BIA分析数据
      - 问卷设计：问卷设计针对性要强，问题要具体；
      - 问卷填写：填写不完整，会降低调查信息的质量。
    - 访谈：能提供很好的真实信息
      - 访谈目标必须明确，问题具体；
      - 选择合适的访谈对象，也许需要心理学支持；
      - 比较费时间，得到的信息的格式和详细程度变化较大。

9.1 业务连续性管理BCM

- ## 9.1.2 业务影响分析BIA
  - ### 信息收集--调查问卷设计
    - 根据企业文化、管理风格、自身特点设计适合于受访者的BIA问卷。
    - 问卷内容可包括：
      - 受访者基本信息(姓名、部门、职位、联络方式、受访时间等)
      - 业务功能概况(名称、规模、运行时间、员工数量、客户数量、重要的时间段、高峰业务量、法规要求、与其它业务或支持系统的关系等)
      - 业务中断对业务成本或收入的影响(增加开支租用额外设备或人员等)
      - 业务中断可能承担的法律责任(合同违约、违反相关规定等)
      - 业务中断对业务运作的影响(无法提供服务等)
      - 业务中断对声誉的影响(失去客户信任、客户流失等)
      - 依赖于哪些技术系统(如硬件、软件、数据、网络等)
      - 存在哪些弱点和威胁(火灾、地震、罢工等)
      - 现有的应对措施(应急预案等)

9.1 业务连续性管理BCM

- **9.1.2 业务影响分析BIA**
  - 支持资源的确定
    - 人力资源（ **Human resources** ）
      - 如操作员、专家、系统用户等
    - 处理能力（ **Processing capability** ）
      - 如数据中心、备份中心、网络、小型机、工作站、个人计算机
    - 物理基础设施（**Physical infrastructure** ）
      - 如办公室、家具、环境控制系统、电力、上下水、物流服务等
    - 基于计算机的服务(**Computer-based services**)
      - 如语音和数据通信服务、数据库服务、公告服务等
    - 应用和数据（ **Application and Data**）
      - 计算机设备上运行的各种程序和存储的数据
    - 文档和票据（**Documents and papers** ）
      - 如合同、票据、操作程序等文件、文档和资料

9.1 业务连续性管理BCM

- 9.1.2 业务影响分析BIA
  - 确定最大允许中断时间MTD
    - Maximum Tolerable Downtime
      - 中断时间超过MTD将造成业务难以恢复；
      - 越是关键的功能或资源，MTD应该越短：
        - 关键：1 小时之内
        - 紧急： 24小时
        - 重要：72 小时
        - 一般：7天
        - 非必要：30天
  - 确定恢复顺序
    - 根据MTDs排定关键业务功能及其支持资源的恢复顺序

9.1 业务连续性管理BCM

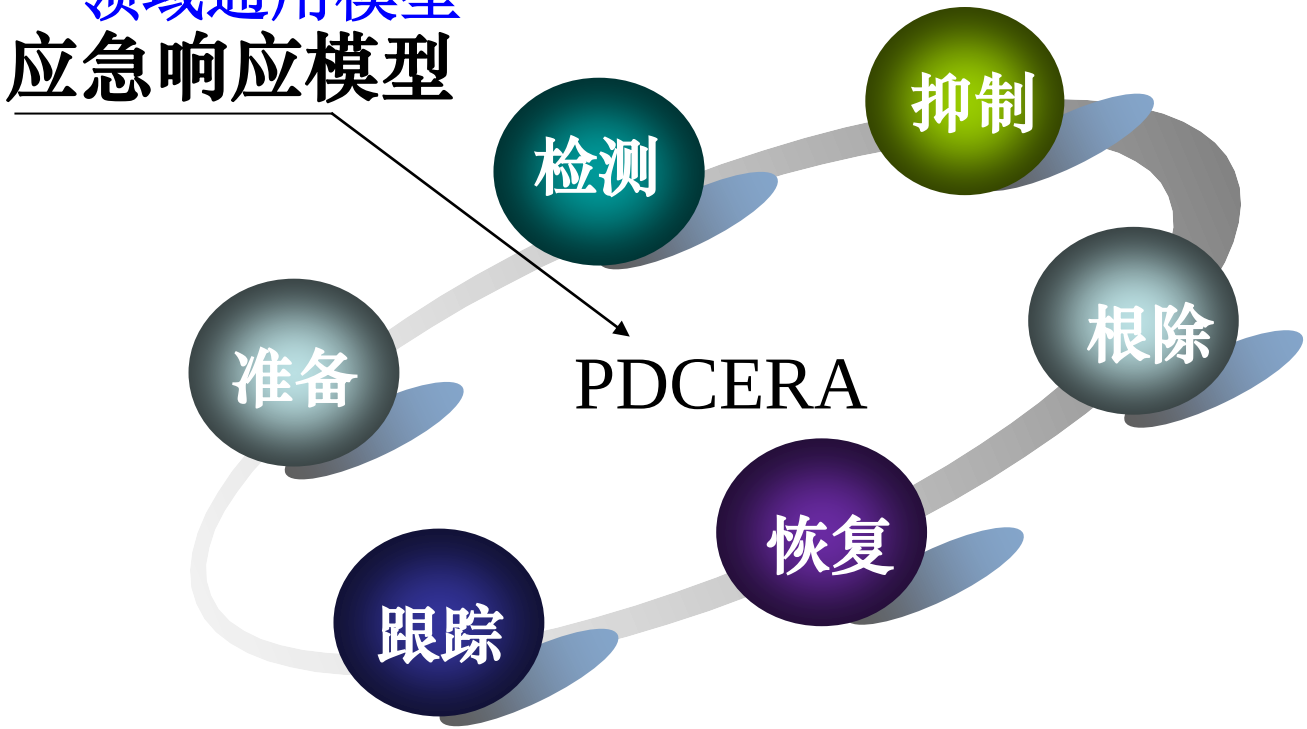
- **9.1.2 业务影响分析BIA**
  - 风险分析
    - 电力中断
    - 火灾、洪水、风暴、地震
    - 系统设备故障和软件故障
    - 丧失基础设施功能（如电信等）
    - 测试和变更造成的中断
    - 关键人员缺席
    - 恐怖袭击、爆炸、罢工
    - 传染病

9.1 业务连续性管理BCM

- 9.1.3 应急响应
  - 应急响应
    - 指一个组织为了应对各种意外事件的发生所做的准备以及在事件发生初期所采取的措施。
    - 目的：避免、降低危害和损失，以及从危害和损失中恢复。
  - 应急响应的必要性
    - 网络安全保护的困难；
    - 大量的安全漏洞；
    - 攻击系统和网络的程序的存在；
    - 实际的和潜在的财务损失；
    - 不利的媒体曝光的威胁；
    - 对效率的需求；
    - 当前入侵检测能力的局限性。

9.1 业务连续性管理BCM

- 9.1.3 应急响应
  - 应急响应方法学
    - 领域通用模型



9.1 业务连续性管理BCM

- 9.1.3 应急响应
  - 应急响应方法学—准备P
    - 即在安全事件发生前为应急响应做好准备。
    - 这一阶段极为重要，因为安全事件多数都比较复杂，事先准备是必须的。
    - 准备工作包括：
      - 基于威胁建立一组合理的防御／控制措施。
      - 建立一组尽可能高效的安全事件处理程序。
      - 获得处理问题必须的资源和人员。
      - 建立一个支持应急响应活动的基础设施。

9.1 业务连续性管理BCM

- 9.1.3 应急响应
  - 应急响应方法学—检测(Detection)
    - 弄清是否出现了恶意代码、文件和目录是否被篡改或者出现其他的安全事件特征；如果是的话，问题在哪里，影响范围有多大。
    - 检测包括软件检测和人工检测。
    - 软件检测
      - 面对种类繁多复杂的攻击，检测软件(如杀毒软件、入侵检测软件、完整性校验软件等)对应急响应工作的成功是非常必要的。
      - 许多软件可以迅速地检测桌面系统和邮件服务器的病毒、秘密安装的后门木马程序。

9.1 业务连续性管理BCM

- 9.1.3 应急响应
  - 应急响应方法学—检测(Detection)
    - 人工检测
      - 用不活跃或系统缺省账号登录。
      - 在非工作时间有系统活动。
      - 出现了不是由系统管理员创建的账号。
      - 出现了不熟悉的文件或程序。
      - 用户权限的提升或超级用户权限的使用，但对此无法解释。
      - Web服务器主页或其他页面被修改。
      - 系统日志出现一段时间的空白或擦除。
      - DNS表、路由器或防火墙规则中的无法说明的变化。
      - 系统性能变慢。

9.1 业务连续性管理BCM

- 9.1.3 应急响应
  - 应急响应方法学—抑制(Containment)
    - 抑制是限制攻击的范围，同时也就限制了潜在的损失和破坏。
      - 只有在第2阶段观察到事件的确已经发生的基础上才能进行抑制。
    - 可能的抑制措施
      - 关闭所有系统。
      - 断开网络。
      - 修改所有防火墙和路由器的过滤规则，拒绝来自看起来是发起攻击的主机的所有的流量。
      - 封锁或删除被攻破的登录账号。
      - 提高系统或网络行为的监控级别。
      - 设置诱饵服务器作为陷阱，如“蜜罐”等。
      - 关闭存在漏洞的服务。
      - 反击攻击者的系统。

9.1 业务连续性管理BCM

- 9.1.3 应急响应
  - 应急响应方法学—根除(Eradication)
    - 在安全事件被抑制以后，应该找出事件根源并彻底根除。
    - 根除手段：
      - 工具软件。比如，防病毒软件可以消灭大多数感染小系统的(甚至大系统的)病毒以及特洛伊木马程序。
      - 对于单机上的事件，主要可以根据各种操作系统平台的具体的检查和根除程序进行操作。
      - 大规模爆发的带有蠕虫性质的恶意程序的根除相对复杂。
      - 手工根除。经验丰富的管理员检查和根除恶意程序。

9.1 业务连续性管理BCM

- 9.1.3 应急响应
  - 应急响应方法学—恢复(Recovery)
    - 在安全事件的根源根除以后，恢复阶段定义下一阶段的行动。
    - 恢复的目标是把所有被攻破的系统和网络设备彻底地还原到它们正常的任务状态。

9.1 业务连续性管理BCM

- 9.1.3 应急响应
  - 应急响应方法学—跟踪(Follow-up)
    - 跟踪是最后一个阶段。
    - 总体目标是回顾并整合发生事件的相关信息。
    - 跟踪的重要性：
      - 有助于事件处理人员吸取经验教训，提高他们的技能，以应付将来发生的同样的事件。
      - 有助于评判和管理一个组织机构的应急响应能力。
      - 所吸取的任何教训都可以当作应急响应工作组新成员的培训教材。
      - 可以当作应急响应工作组建设的基础。
      - 能够产生在法律行为中有用的信息。

9.1 业务连续性管理BCM

- 9.1.3 应急响应
  - 应急响应预案
    - 是被设计用于在信息安全突发事件中维持或恢复包括计算机运行在内的业务运行的策略和规程。
    - 应该有系统完整的设计、标准化的文本文件、行之有效的操作程序和持续改进的运行机制。
    - 基本原则
      - 集中管理、统一指挥、规范运行、标准操作、反应迅速和响应高效。
    - 目标
      - 控制紧急事件的发展并尽可能消除，将事故对人、财产和环境的损失和影响减小到最低限度。

9.1 业务连续性管理BCM

- 9.1.3 应急响应
  - 应急响应预案制定过程
    - 初稿制订：
      - 参照应急响应预案框架，按照IT系统风险分析和业务影响分析所确定的应急内容，根据应急响应等级的要求，结合组织其它相关的应急计划，撰写出应急响应预案的初稿。
    - 初稿的评审：
      - 组织应对应急响应预案初稿的全面性、易用性、明确性、有效性和兼容性进行严格的评审。
      - 评审应有相应的流程保证。
    - 初稿的修订：
      - 根据评审结果，对预案进行修订，纠正在初稿评审过程中发现的问题和缺陷，形成预案的修订稿。

9.1 业务连续性管理BCM

- 9.1.3 应急响应
  - 应急响应预案制定过程
    - 预案的测试：
      - 应预先制订测试计划，在计划中说明测试的案例。
      - 测试应包含基本单元测试、关联测试和整体测试。
      - 测试的整个过程应有详细的记录，并形成测试报告。
    - 预案的审核和批准：
      - 根据测试的记录和报告，对预案的修订稿进一步完善，形成预案的报批稿；
      - 预案报批稿由应急响应领导小组审核和批准，确定为预案的执行稿。

9.1 业务连续性管理BCM

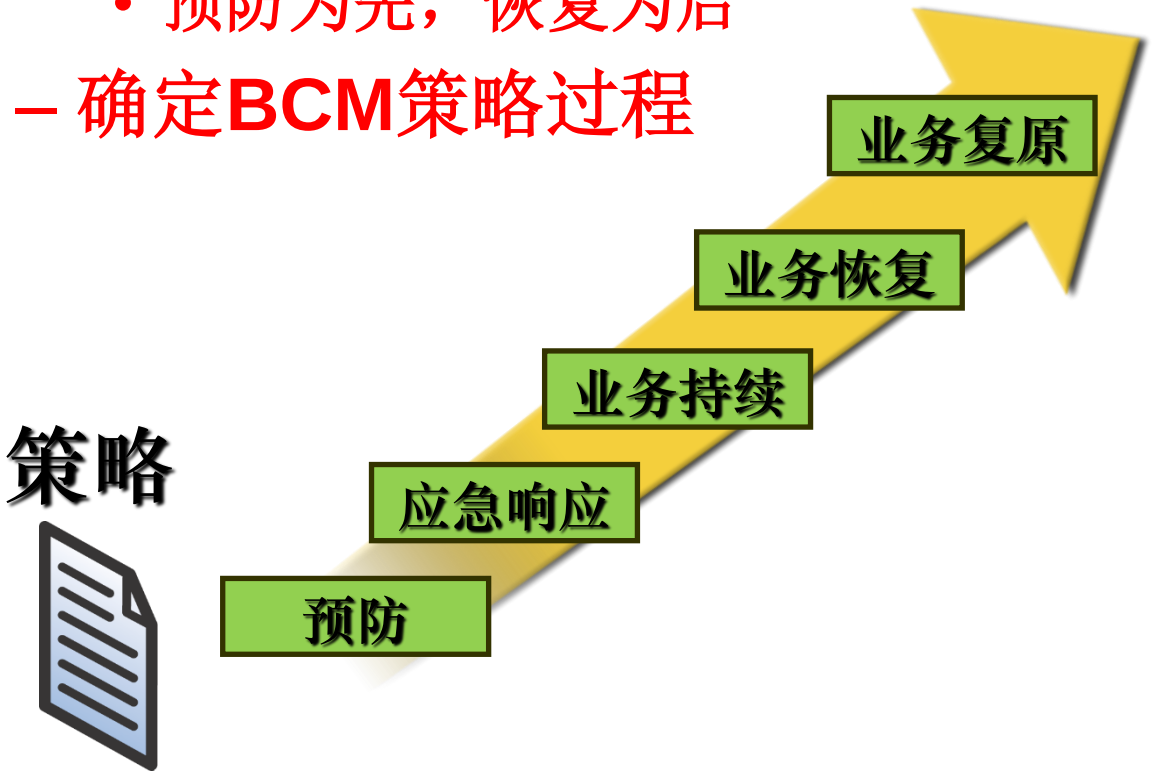
- 9.1.3 应急响应
  - 应急响应组
    - 应急响应领导小组是信息安全应急响应工作的组织领导机构，由管理、业务、技术和行政后勤等人员组成。组长应由组织最高管理层成员担任。
      - 一般可设为应急响应领导小组、应急响应实施小组和应急响应日常运行小组等。
    - 领导小组职责
      - 领导和决策信息安全应急响应的重大事宜，主要如下：
        - a）审核并批准经费预算；
        - b）审核并批准恢复策略；
        - c）审核并批准应急响应预案；
        - d）批准应急响应预案的执行。

9.1 业务连续性管理BCM

- 9.1.3 应急响应
  - 应急响应组
    - 应急响应实施小组的主要职责：
      - a）应急响应的需求分析；
      - b）确定应急策略和等级；
      - c）应急策略的实现；
      - d）编制应急响应预案文档；
      - e）组织应急响应预案的测试和演练。
    - 应急响应日常运行小组的主要职责：
      - a）协助灾难恢复系统实施；
      - b）备份中心日常管理；
      - c）备份系统的运行和维护；
      - d）灾难恢复的专业技术支持；
      - e）参与和协助应急响应预案的教育、培训和演练；
      - f）维护和管理应急响应预案文档；
      - g）信息安全突发事件发生时的损失控制和损害评估；
      - h）信息安全事件发生后信息系统和业务功能的恢复；

9.1 业务连续性管理BCM

- 9.1.4 确定BCM策略
  - BCM策略原则
    - 预防为先，恢复为后
  - 确定BCM策略过程



9.1 业务连续性管理BCM

- 9.1.4 确定BCM策略
  - BCM策略—预防
    - 预防为先
      - 通过遏制、探测或降低对系统影响的防御性措施予以消减或清除风险；
      - 达不到灾难级别的风险，采取预防措施规避或降低风险；
      - 灾难级别的风险，采取预防措施降低风险。
    - 恢复为后
      - 对于不可忍受的灾难，采取恢复措施。

9.1 业务连续性管理BCM

- 9.1.4 确定BCM策略
  - BCM策略—预防
    - 预防目的
      - 减少灾难发生的可能性
    - 预防策略
      - 制止控制：减少威胁的可能性。
      - 预防控制：保护企业的弱点区域，以防御危险的发生并降低其影响。

9.1 业务连续性管理BCM

- 9.1.4 确定BCM策略
  - BCM策略—预防
    - 预防措施
      - 设施采取加固材料(建筑、设备等)
      - 冗余服务器和通讯线路
      - 多方多路供电、配置UPS和发电机
      - 消防系统(火警发现、灭火)
      - 防水措施
      - 冗余供应商
      - 购买保险
      - 数据备份
      - 介质保护
      - 备用关键设备
      - 人员培训

9.1 业务连续性管理BCM

- 9.1.4 确定BCM策略
  - BCM策略—应急响应
    - 成立应急响应组
    - 设计应急响应预案并审批
    - 预案的测试和演练

9.1 业务连续性管理BCM

- 9.1.4 确定BCM策略
  - BCM策略—业务持续
    - 业务持续：只涉及时间敏感的业务流程，不是对所有业务的恢复。
      - 中断后立即持续；
      - 在可允许的一段时间中断后持续。
    - 业务持续预案
      - 主要关注业务的损坏、中断和丧失等突发事件，从初始应急响应开始到恢复至正常业务水平。
    - 激活BCP
      - 一旦BCP被激活，做出的第一个决策是：关键性业务的运营能否在日常的工作场所或者一个备选场所很快运营。

9.1 业务连续性管理BCM

- 9.1.4 确定BCM策略
  - BCM策略—业务持续
    - 备选场所分类：
      - 热站点（Hot Site）
      - 温站点（Warm Site）
      - 冷站点（Code Site）
      - 镜像站点（Mirrored Site）
      - 移动站点（Mobile Site）

9.1 业务连续性管理BCM

- 9.1.4 确定BCM策略
  - BCM策略—业务持续：备选场所
    - 热站点(Hot Site)
      - 配置了所需的基础设施、服务、系统硬件、软件、实时数据和支持人员，通常24小时有人值守；
      - 接到应急计划启动通知时只需要进行适当的路由转换和通知就可以提供主站点的关键应用服务。
    - 冷站点(Cold Site)
      - 通常具有充足空间和支持IT系统的基础设施和服务(电源、电信连接和环境控制)；
      - 不包含IT设备并且通常也不包含办公自动化设备如电话、传真机或复印机。

9.1 业务连续性管理BCM

- 9.1.4 确定BCM策略
  - BCM策略—业务持续：备选场所
    - 温站点(Warm Site)
      - 介于热站点和冷站点之间；
      - 配置部分IT资源，不包含实时数据；
      - 启用时需要安装部分设备和软件，还需要上载数据。
    - 镜像站点(Mirrored Site)
      - 具有完整和实时信息镜像的完全的冗余设施；
      - 镜像站点与主站点在所有的技术层面上都是一致的。
    - 移动站点(Mobile Site)
      - 内部配置适当电信装备和IT设备的可移动拖车；
      - 可以被机动拖放和安置在所需的备用场所。

9.1 业务连续性管理BCM

- 9.1.4 确定BCM策略
  - BCM策略—业务恢复
    - 是事件发生后为了继续支持关键功能所采取的行动，启动时间敏感度稍低一些的业务流程。
    - 业务恢复的开始时间要取决于接续时间敏感的业务流程所需要的时间。
    - 业务恢复策略的技术指标：
      - 恢复时间目标(Recovery Time Objectives. RTO)
      - 恢复点目标(Recovery Point Objectives. RPO)

9.1 业务连续性管理BCM

- 9.1.4 确定BCM策略
  - BCM策略—业务恢复
    - 不同层次的恢复策略

业务恢复
Business Recovery

↓

设施恢复
Facility Recovery

↓

支持和技术恢复
Supply and Technical Recovery

↓

用户环境恢复
User Environment Recovery

↓

数据恢复
Date Recovery

9.1 业务连续性管理BCM

- 9.1.4 确定BCM策略
  - BCM策略—业务恢复：基础设施和电力的恢复
    - 基础设施的恢复考虑
      - 备用站点和离站存储设施；
      - 主站点到备用站点的设备和人员运输问题。
    - 电力的恢复考虑
      - 不间断电源(UPS)
      - 双电源(DPS)
      - 双回路供电系统
      - 备用发电机

9.1 业务连续性管理BCM

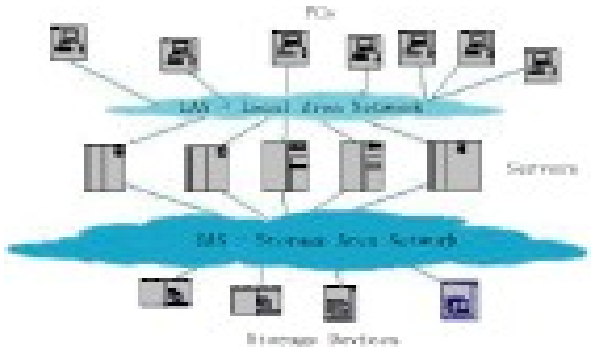
- 9.1.4 确定BCM策略
  - BCM策略—业务恢复：支持与技术的恢复
    - 支持服务的恢复考虑
      - 服务水平协议(Service Level Agreement. SLA)，与服务提供商签订的服务协议中应考虑到在紧急情况下提供服务的问题
    - 应用程序和数据的恢复考虑
      - 常规备份和离站(off-site) 存储；
      - 备份频率和备份介质的运输；
      - 备份方式: 全备份(Full Backup) 、差异备份(Differential) 、增备份(Incremental)。
    - 文档和票据的恢复考虑
      - 重要的文件、资料包括应急计划本身应该有离站存储。

9.1 业务连续性管理BCM

- 9.1.4 确定BCM策略
  - BCM策略—业务恢复：环境与设备的恢复
    - 设备更换的考虑
      - 供应商协议(Vendor Agreements)
        - » 与硬件、软件和支持供应商签订紧急维护服务的服务水平协议
      - 设备存货(Equipment Inventory)
        - » 预先采购所需的设备并将其存储到安全的离站地点
      - 现有的兼容设备(Existing Compatible Equipment)
        - » 现在库存的设备、租用的热站点中使用的设备以及部门中其它机构使用的设备

9.1 业务连续性管理BCM

- 9.1.4 确定BCM策略
  - BCM策略—业务恢复：环境与设备的恢复
    - 网络的恢复考虑
      - 双电缆布线和预留额外的数据插口
      - 关键网络设备的冗余或容错
      - 冗余的远程通信链路
      - 冗余网络服务提供商(Network Service Providor, NSP)
      - 由NSP或互联网服务提供商(Internet Service Provider, ISP)提供冗余
      - 与NSP或ISP签订的服务水平协议



9.1 业务连续性管理BCM

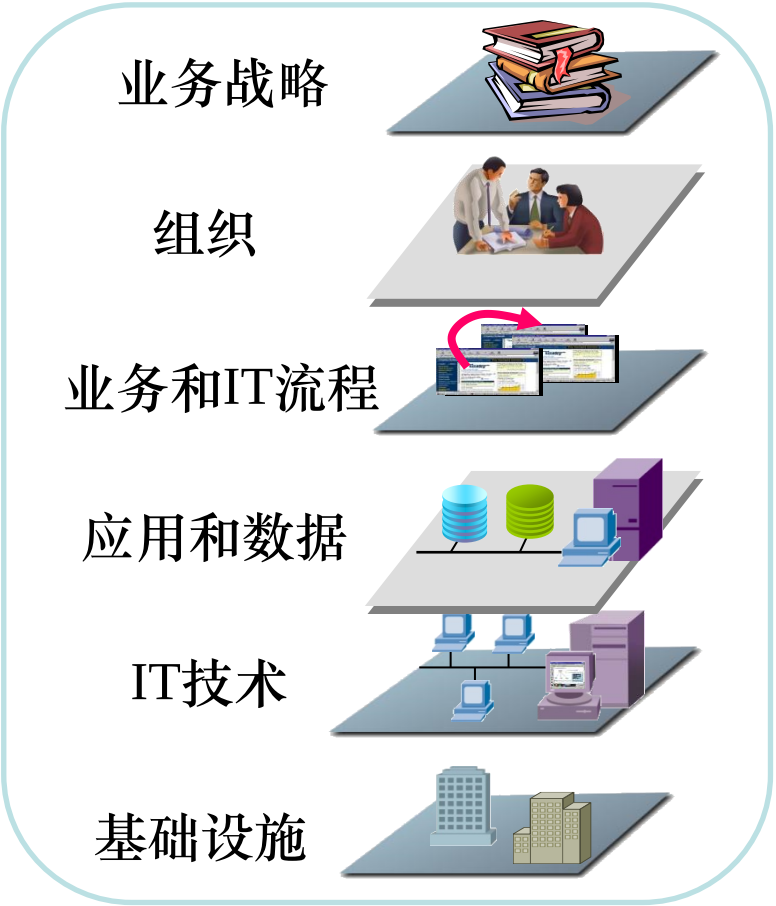
- **9.1.4 确定BCM策略**
  - **BCM策略—业务恢复：人员与用户的恢复**
    - 人力资源的考虑
      - 在灾难发生后，保护人的生命是第一要务
      - 员工培训和应急指引
      - 人员备份和轮岗
      - 雇佣额外或临时工作人员

9.1 业务连续性管理BCM

- 9.1.4 确定BCM策略
  - BCM策略—业务复原
    - 业务复原
      - 是事件发生后为了恢复到正常运行状态所采取的行动。
      - 主要是修复并恢复主要的运营场所。
      - 其最终目的是要在原有的场所或者一个全新的场所完全恢复所有的业务流程。
      - 进行复原时，必须确保该复原场所配备必要的基础设施、设备、硬件、软件和通信设备。而且要对该场所能否处理全部的业务流程进行测试。

9.1 业务连续性管理BCM

- **9.1.5 BCM开发和实施**
  - **BCM开发建设思路**



- 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

9.1 业务连续性管理BCM

- 9.1.5 BCM开发和实施
  - BCM计划制定
    - 通知/启动阶段
    - 恢复阶段
    - 重建阶段
    - 计划的附录

9.1 业务连续性管理BCM

- 9.1.5 BCM开发和实施
  - BCM计划制定--通知/启动阶段
    - 损害评估
      - 紧急情况的原因、损失情况、影响范围、需更换的项目、预计恢复所需的时间等
    - 启动标准
      - 预警级别
      - 触发条件
    - 启动通知
      - 工作时间和非工作时间的通知方法
      - 呼叫树
      - 通知可能受影响的外部机构或互联的伙伴系统
      - 通知中所传递的信息类型应该在计划中载明

9.1 业务连续性管理BCM

- 9.1.5 BCM开发和实施
  - BCM计划制定--恢复阶段
    - 恢复顺序
      - 系统允许的中断时间(Allowable Outage Time)
      - 系统之间的依赖关系
    - 恢复规程
      - 按照直接和逐步的风格书写
      - 不能假定规程的步骤
      - 不能忽略规程的步骤
      - 准备检查列表

9.1 业务连续性管理BCM

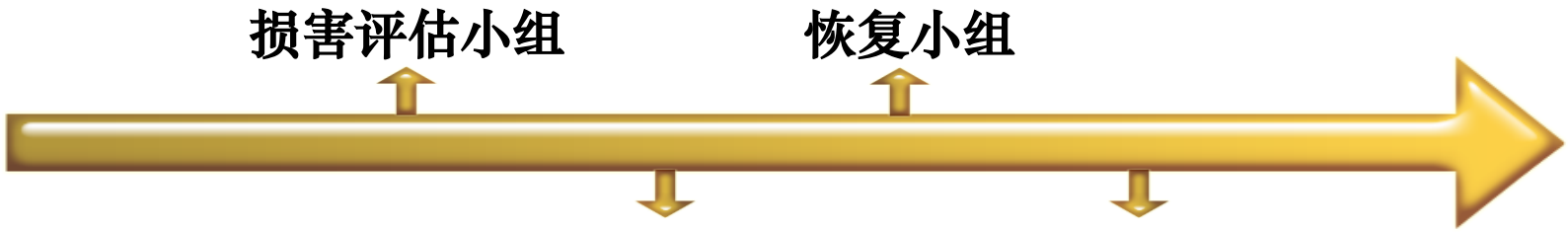
- 9.1.5 BCM开发和实施
  - BCM计划制定--重建阶段
    - 恢复原站点
      - 确保充足的基础设施支持，如电源、供水、电信、安全、环境控制、办公设备和用品
      - 安装系统硬件、软件和固件
      - 准备和使用恢复阶段类似的详细恢复规程
    - 测试系统
      - 对系统进行测试
      - 备份和上载应急系统中的运行数据
    - 终止操作
      - 关闭应急系统、终止应急操作
      - 保护、清除或重新配置应急站点
      - 恢复人员回到原设施

9.1 业务连续性管理BCM

- 9.1.5 BCM开发和实施
  - BCM计划制定--计划的附录
    - 计划的附录
      - BCM 团队成员的联络信息
      - 供应商联络信息，包括离站存储(Off-site Storage) 和备用站点(Alternate Site) 的联络点(Point Of Contact. POC)
      - 系统恢复的标准操作规程和检查列表
      - 支持系统所需的硬件、软件、固件和其它资源的设备和系统需求清单。每个条目应该包含详细内容，包括型号或版本号、规格说明和数量
      - 供应商SLA 、与其它机构的互惠协议
      - 备用站点的描述和说明
      - BIA报告（业务影响分析），包含系统各部分相互关系、风险、优先级别和影响的有价值的信息

9.1 业务连续性管理BCM

- 9.1.5 BCM开发和实施
  - BCM计划制定—团队与要求
    - 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

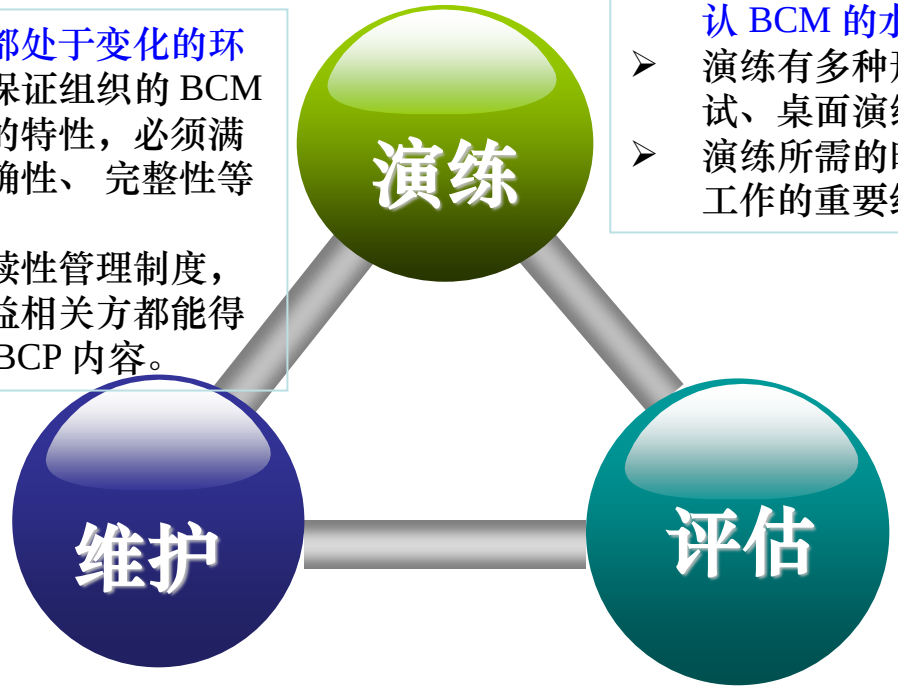
9.1 业务连续性管理BCM

- 9.1.5 BCM开发和实施
  - BCM计划制定—团队与要求
    - BCM 团队要求
      - 团队成员选择
        - » 技能(Skills)
        - » 知识(Knowledge)
      - 团队建设
        - » 充分的培训，至少一年一次
        - » 新员工上岗之前应该接受BCM培训
        - » 能够随时开展工作
        - » 小组应该具有足够规模，不存在人员单点
        - » 继任序列(Line of Succession Planning)

9.1 业务连续性管理BCM

- **9.1.6 BCM演练、维护和评估**
  - 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。

- 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。



- 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。

- 内部审计。
- 外部审计。
- 自我评估。

9.1 业务连续性管理BCM

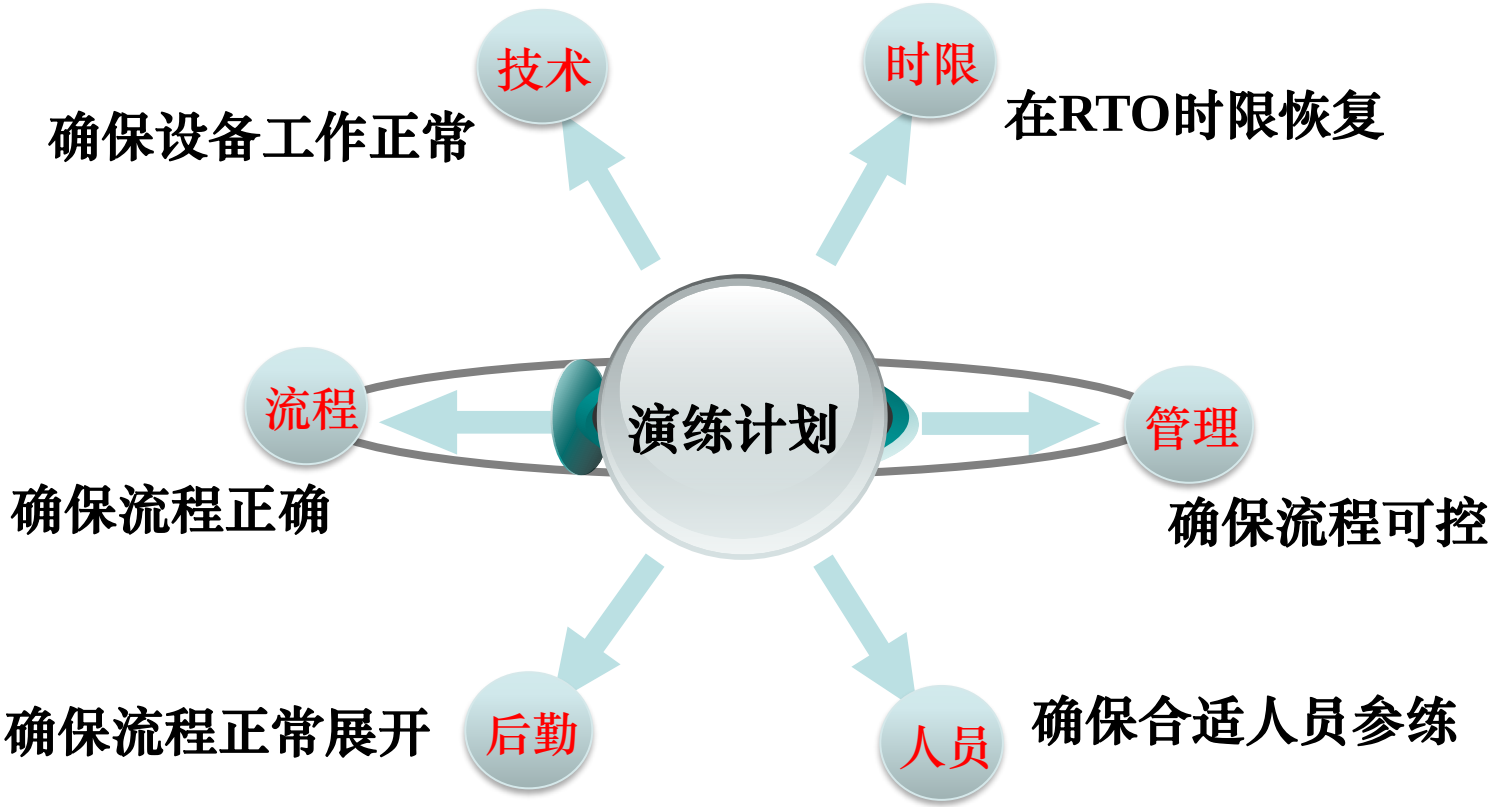
- 9.1.6 BCM演练、维护和评估
  - BCM演练要求
    - 制定演练计划
      - 明确的演练目标(Test Objectives)
      - 成功标准(Standard for Success)
      - 演练计划应该包括 BCM 策略规定的所有方面
    - 演练总结
      - 演练结果和学习到的经验应该记录到文档
      - 在演练中和演练后收集到的有助于提高计划效率的信息应该修订BCP计划

9.1 业务连续性管理BCM

- 9.1.6 BCM演练、维护和评估
  - 演练规划流程
    - 绘制所有恢复流程列表
    - 确定每个恢复流程的具体演练方式
    - 列出每个恢复流程中涉及的人员或团队
    - 制定演练活动计划表，确保演练活动涵盖所有预案的中人员、流程。

9.1 业务连续性管理BCM

- 9.1.6 BCM演练、维护和评估
  - 演练规划



9.1 业务连续性管理BCM

- 9.1.6 BCM演练、维护和评估
  - 演练规划
    - 演练分级和类型

测试类型	流程	参与者	演练周期	复杂程度
桌面检查	检察预案，确保完整	预案制定者、部门主管	高	低
过程演练	确保交互、协调能力	预案制定者、主要参与者	↑	↑
模拟演练	综合各项预案 场地预案 应急通讯预案	主要参与者、观察员、协调员	↕	↕
模拟、实战演练	将工作转移到备用场地，重建业务功能	业务部门员工、场地服务商、观察员、协调员	↓	↓
实战演练	完全关闭主场地，重新部署、恢复业务	所有员工、场地服务商、观察员、协调员	低	高

9.1 业务连续性管理BCM

- 9.1.6 BCM演练、维护和评估
  - BCM演练预案
    - 预案演练目的
      - 评估组织当前的BCM能力。
      - 发现BCM 的不足，持续改进。
      - 检查预案场景假设的不足之处。
      - 为演练参与者提供信息，增强信心。
      - 提高团队工作能力。
      - 全面提升组织的BCM意识水平。
      - 测试恢复流程的有效性、所花费时间等。

9.1 业务连续性管理BCM

- 9.1.6 BCM演练、维护和评估
  - BCM演练预案
    - 预案演练要求：实现测试的有效性
      - 严谨周密
        - » 应该尽一切可能开展演练， 并且尽可能采用与现实环域中相同的流程和方法。
      - 结合实际
        - » 如果场景假设不合理， 那么测试的效果也会大打折扣。
      - 最小破坏
        - » 将造成业务中断的风险控制到最小程度。业务部门需要理解、同意接受测试的潜在风险。

9.1 业务连续性管理BCM

- 9.1.6 BCM演练、维护和评估
  - BCM演练方式
    - 测试：
      - 主要针对技术流程/业务流程的检验活动，经常用目标时间来衡量测试水平。在这种情况下，结果或者是"通过" 或者是"失败" (结果是针对BCP流程而不是人员) 。
      - 举例: 基于备份磁带，重新配置服务器。
    - 排演：
      - 是指包含一系列特殊的流程，通过剧本/手册等传达相关的知识和技能。 举例：火灾排演。
    - 演练：
      - 通常是基于场景的，用于检验决策能力。
      - 举例：针对某个重大事故举行桌面演练。

9.1 业务连续性管理BCM

- 9.1.6 BCM演练、维护和评估
  - BCM演练方式
    - 技术测试流程
      - 确定技术测试的目标和范围。
      - 确定技术测试的费用预算。
      - 指定专人负责技术测试。
      - 为技术测试假设一个基本场景。
      - 对技术测试开展风险评估，将测试对实际生产造成的影响降到最低。
      - 开展测试并记录测试结果。
      - 评估和汇报测试结果。
      - 解决在测试中发现的任何问题。

9.1 业务连续性管理BCM

- 9.1.6 BCM演练、维护和评估
  - BCM演练方式
    - 场景演练流程
      - 高层管理确认并同意场景演练的目的和范围。
      - 确定场景测试的费用预算。
      - 与相关部门达成一致。
      - 准备真实、 恰当和详细的模拟场景。
      - 调查相关信息。
      - 确保可以调用演练参与者。
      - 通知有关演练活动的信息和简报。
      - 开展演练。
      - 立刻举行简短的演练总结。
      - 举行正式、详细的演练总结。
      - 制定演练报告和整改建议。
      - 报告在演练中发现的不足。
      - 发布演练报告。
      - 制定演练整改计划， 指导演练报告中的整改措施。

9.1 业务连续性管理BCM

• 9.1.6 BCM演练、维护和评估

– BCM演练输出

- 验证业务持续性策略的有效性；
- 应急团队成员、普通员工在应对突发事件中熟悉各自的职责、义务和权力， 提高人员BCM 的意识及技能；
- 测试业务持续预案中技术、后勤和管理等；
- 测试恢复设施中应急指挥中心、工作场地、技术和通信等的资源恢复情 况；
- 演练人员的可用性、人员调配；
- 在事后演练报告中记录演练结果，供高层管理、审计者、保险公司、监管机构及其他组织参考和使用；
- 记录和处理在演练中暴露的不足；
- 提升人员关于应急流程的意识；
- 提升人员关于BCM重要性的意识；
- 发现组织的不足，提高业务持续性能力。

9.1 业务连续性管理BCM

- 9.1.6 BCM演练、维护和评估
  - BCM预案维护
    - 确保组织在激烈的变化环境中，仍然保持应对各种突发事件的能力。
    - 要使BCM维护程持续有效，应该将其融入到组织的日常管理流程中，而不是单独设置而遭遗忘。
    - BCM维护目的
      - 确保组织在自身和外部环境变化的情况下， 仍然保持有效的BCM 能力。
    - BCM 维护前提
      - 有效的变更管理；
      - 定期检查组织的内部变更：人员、业务流程、技术。

9.1 业务连续性管理BCM

- 9.1.6 BCM演练、维护和评估
  - BCM预案维护
    - 检查触发条件
      - 如果变更流程发生重大变化，或者在演练总结报告和审计报告中有重大发现事项，需要立即检查。
    - 检查对象
      - 检查BIA报告中的假设内容，分析业务的时间敏感度是否发生变化。
      - 检查组织在不同时期所需的外部服务是否充分、 可用。
      - 检查与关键业务相关的供应商的安排事宜。
      - 评估是否需要变更和改善培训、 意识和沟通。
      - 供适当的培训、意识和沟通培训。
      - 依据正式文档变更(版本)控制流程，向各利益相关方发布更新、修订和变更的BCM政策、策略、解决方案、流程和计划。

9.1 业务连续性管理BCM

- 9.1.6 BCM演练、维护和评估
  - BCM预案维护输出成果
    - BCM监控和维护工作的文档；
    - 内容清晰的BC文档维护报告(包括整改建议)，并且由相应的高级管理层确认和批准；
    - 内容清晰的BCM维护报告的行动计划， 并且由相应的高级管理层确认和审批；
    - 维护业务持续预案(BCP)、策略和解决方案的有效， 保持最新版本。

9.1 业务连续性管理BCM

- 9.1.6 BCM演练、维护和评估
  - BCM预案演练评估
    - 评估方法
      - 内部审计、外部审计、自我评估
    - 评估目的
      - 检验组织 BCM 的竞争力和能力。
      - 将组织 BCM 现状和审计标准对比，提出正式、规范的审计报告。
      - 另外，BCM 的审计周期会影响到组织的 BCM 能力水平。

9.1 业务连续性管理BCM

- 9.1.6 BCM演练、维护和评估
  - BCM预案演练评估
    - BCM审计过程需要与业务、技术领域的管理和操作岗位人员进行广泛的交流沟通。
    - BCM的保证流程
      - 定义BCM工作的岗位职责、权力和义务。
      - 定义BCM工作的KPI (关键性能指标) 目标、衡量的尺度和标准。
      - 定义BCM工作的成功要素。
      - 将KPI (关键性能指标)纳入内部、外部合同和年度考核工作中。
      - 根据事先预定的KPI(关键性能指标)，评估和检查实际的执行效果。
      - 提供后续整改计划。

9.1 业务连续性管理BCM

- 9.1.6 BCM演练、维护和评估
  - BCM预案演练评估
    - BCM 审计流程
      - BCM审计计划。
      - 定义审计范围。
      - 确定需要审计涉及到组织的区域/部门/场地。
      - 通过BCM审计活动，检查和收集信息。
      - 整理、汇总相关的文挡。
      - 分析收集到的信息的内容和水平。
      - 收集和比较相关文档。
      - 参考其他信息。
      - 恨据审计目的要求，出具审计结论。
      - 提供审计草案
      - 提供一个双方协商一致的审计意见报告。
      - 提供一个双方协商一致的后续整改计划。
      - 提供一个BCM审计的监控流程。

9.1 业务连续性管理BCM

- 9.1.6 BCM演练、维护和评估
  - BCM预案演练评估
    - 评估方法
      - 定量评估、定性评估；
      - 由执行BCM 审计的人员决定采用。
    - 评估方法：定性评估
      - 分析和检查文档；
      - 访谈员工和其他利益相关方。

9.1 业务连续性管理BCM

- 9.1.6 BCM演练、维护和评估
  - BCM预案演练评估
    - 评估方法：定量评估
      - 从最近一次演练到现在的间隔时间(月份)；
      - 从最近一次演练到现在， 还未解决所发现问题的数量；
      - BC计划文档的完整程度；
      - 从最近一次业务影响分析到现在的间隔时间(月份)；
      - 从最近一次业务影响分析到现在， 还未解决所发现问题的数量；
      - 在BC管理/计划中包含的新IT应用的评估内容；
      - 在BC管理/计划中包含的新业务或业务变更；
      - 恢复团队动态数据的完整性、可用性， 例如团队成员、联系电话、通知/供应商列表， 恢复站点/工作站的配置等；
      - 确定实施和维护BCM 的费用预算；
      - 控制费用的使用；
      - 自我评估保证记分卡。

9.1 业务连续性管理BCM

- 9.1.6 BCM演练、维护和评估
  - BCM预案评估输出
    - 独立的BCM 审计报告：由高层管理者同意和批准；
    - 后续整改行动计划：由高层管理者同意和批准；
    - BCM执行水平较低将：
      - 内部审计部门所认可的BC计划是“ 不适当” 的， 需要进一步完善。
      - 需要由BC专家协助组织重新检查BC， 提升组织相关团队的水平。

9.2 灾难恢复

- 9.2.1 灾难(Disaster)
  - 灾难是导致重大损失的突发的不幸事件。
    - 任何导致机构关键业务功能(Critical Business Functions) 在一定时间内无法进行的事件都被视为灾难。
  - 灾难（GB/T 20988-2007）
    - 由于人为或自然的原因，造成信息系统严重故障或瘫痪，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。
    - 导致信息系统需要切换到灾难备份中心运行。

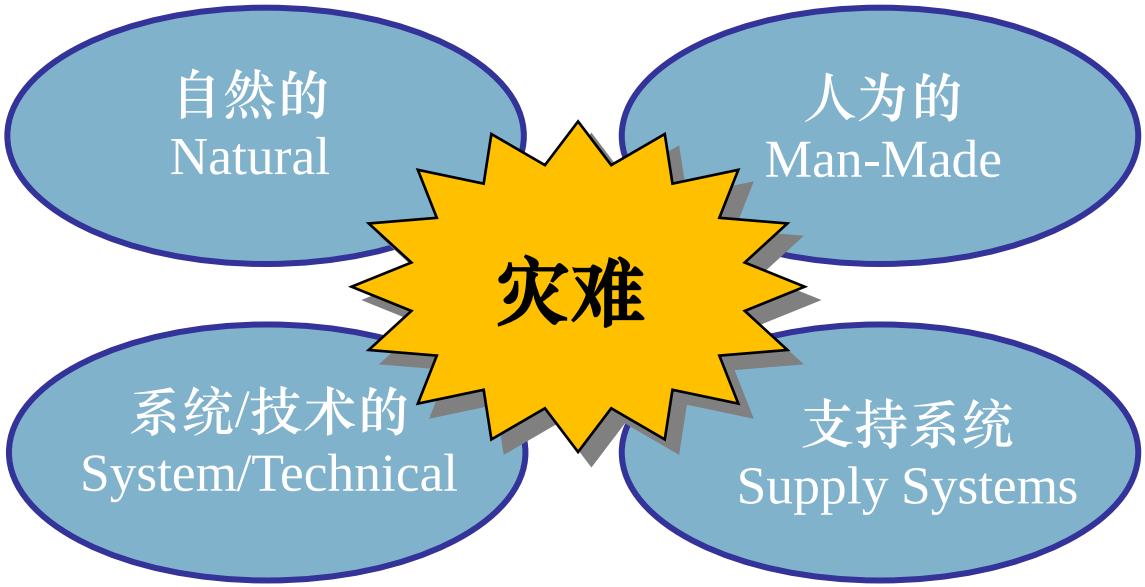
9.2 灾难恢复

- 9.2.1 灾难(Disaster)
  - 灾难案例
    - 世贸大厦
      - 世界上最大、最快的电梯
      - 南楼共有99座电梯
      - 每个电梯最多容纳55人
      - 45秒内由78层到地面
      - 大楼备用电源， 应急灯
      - 3个楼梯
      - 楼梯扶手、天花板、楼道门上涂荧光漆，指示疏散线路
      - 安装扬声器、疏散指挥系统
      - 大楼设救火指挥所，每楼层有火警监督员，定期演练

    - 飞利浦芯片厂火灾
      - Nokia：危机是你改进的机遇！
      - Ericsson：我们根本没有所谓的危机处理方案！

9.2 灾难恢复

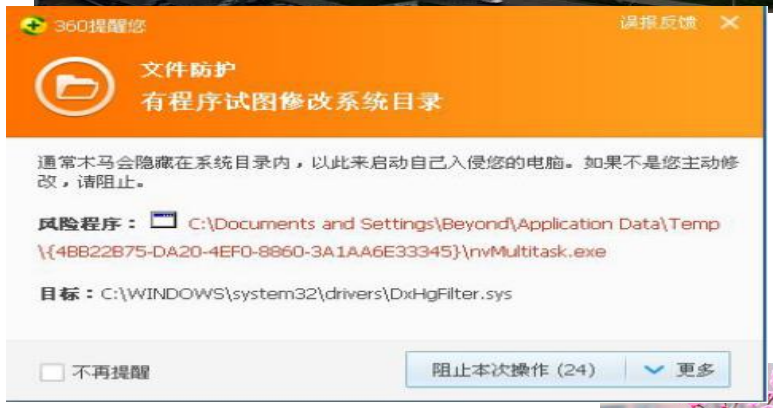
- 9.2.1 灾难(Disaster)
  - 灾难事件分类
    - 典型的灾难事件包括自然灾害、技术风险和提供给业务运营所需服务的中断以及人为的因素等。
      - 自然：火灾、洪水、地震、飓风、龙卷风和台风等。
      - 人为：操作员错误、植入有害代码和恐怖袭击等。



9.2 灾难恢复

- 9.2.1 灾难(Disaster)
  - 灾难事件分类
    - 自然灾害

    - 人为因素



9.2 灾难恢复

- 9.2.1 灾难(Disaster)
  - 灾难事件分类
    - 技术故障
      - 如设备故障、软件错误导致系统停止运行

    - 业务支持服务中断
      - 业务运营所需服务，如电力、通信、网络、运输等支持服务中断

9.2 灾难恢复

- 9.2.1 灾难(Disaster)
  - 机构灾难的表现特点：
    - 计划之外的服务中断；
    - 超期的服务中断；
    - 中断无法通过平常的事件管理程序得到解决；
    - 中断造成重大损失。
  - 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

9.2 灾难恢复

- 9.2.2 灾难恢复
  - 灾难恢复(GB/T 20988-2007)
    - 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。
    - 是指当系统崩溃时为将其恢复到正常运行状态所需的操作。
  - 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。

9.2 灾难恢复

• 9.2.2 灾难恢复(GB/T 20988-2007)

– 灾难恢复系统

- 为了保障计算机系统和业务发生灾难的情况下能够迅速的得以恢复而建立的一整套完整系统。
  - 包括备份中心、计算机备份运行系统、可根据需要重置路由的数据通信线路、电源以及数据备份等。
  - 还应包括对该系统的测试和对人员的培训。

– 灾难恢复的必要性

- 业务连续性需求。
  - 灾难恢复是业务连续性的基本保障。
  - 制定灾难恢复系统的最终目的是以最合理的代价保护应用数据的完整性与安全性，在灾难发生后尽快的恢复运行，减少业务停顿时间，使灾难造成的损失降到最小。
- 法律要求。
  - 一些发达国家对某些行业，灾难恢复系统是法律要求的，公司必须承诺严格执行。

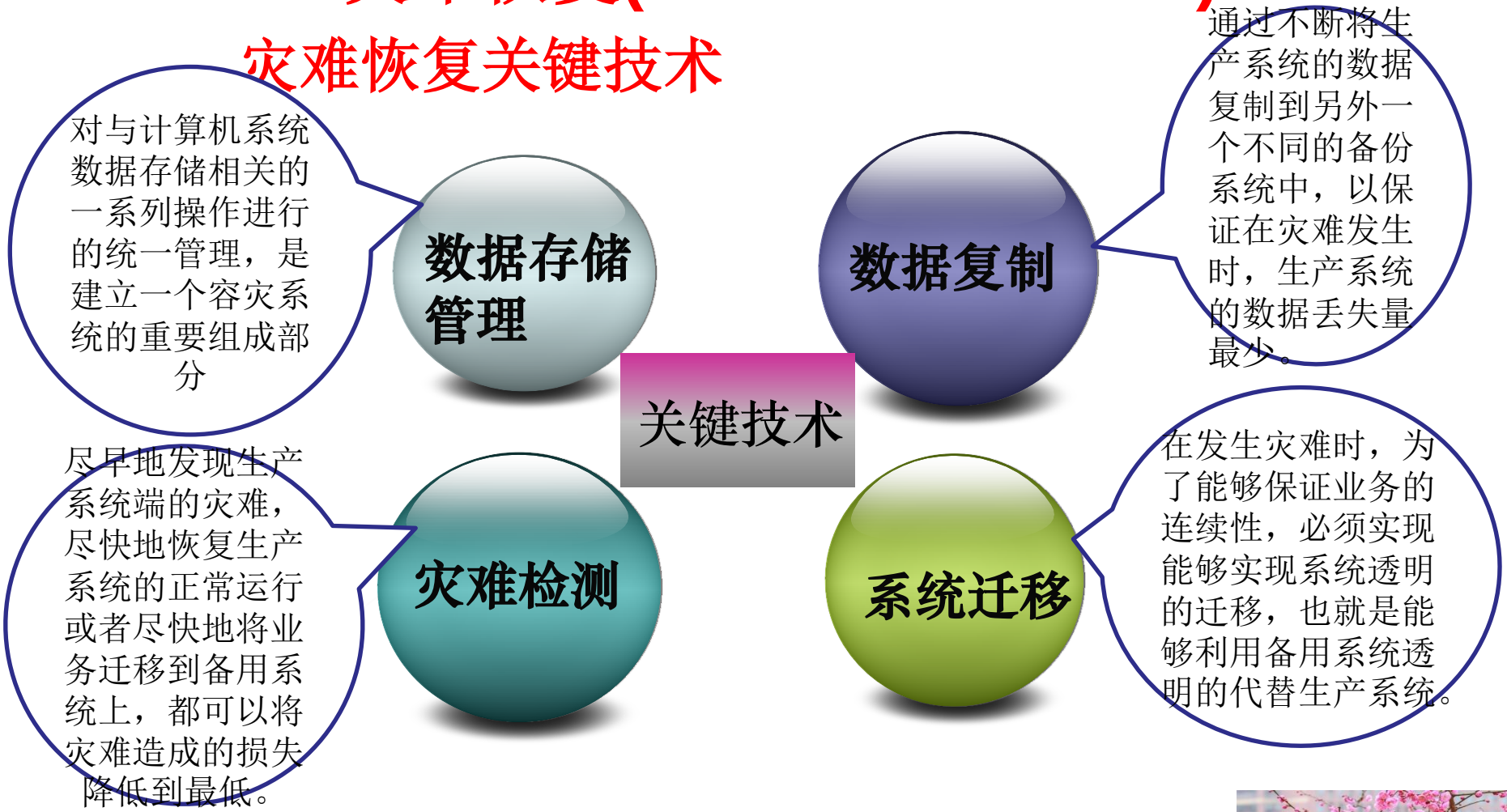
9.2 灾难恢复

- 9.2.2 灾难恢复(GB/T 20988-2007)
  - 灾难恢复的种类
    - 1）全盘恢复。
      - 一般应用在服务器发生意外灾难导致数据全部丢失、系统崩溃或是有计划的系统升级、系统重组等，也称为系统恢复。
    - 2）个别文件恢复。
      - 利用网络备份系统的恢复功能，很容易恢复受损的个别文件。
    - 3）重定向恢复。
      - 重定向恢复是将备份的文件恢复到另一个不同的位置或系统上去。其可以是整个系统恢复，也可以是个别文件恢复。

9.2 灾难恢复

- 9.2.2 灾难恢复(GB/T 20988-2007)

灾难恢复关键技术



9.2 灾难恢复

- 9.2.2 灾难恢复(GB/T 20988-2007)
  - 灾难备份
    - 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，称为灾难备份。
      - 为了维持业务连续性，应通过预防和灾难恢复控制措施相结合的模式将灾难和安全事件引起的业务中断和系统破坏减少到可以接受的程度，保护关键业务过程免受故障或灾难的影响。
      - 在灾难发生前通过建立灾难备份系统，对主系统进行备份并加强管理保证其完整性和可用性；
      - 在灾难发生后，利用备份数据，实现主系统的还原恢复。这是灾难恢复的有效手段。
    - 备份包括软件级备份和硬件级备份。

9.2 灾难恢复

- 9.2.2 灾难恢复(GB/T 20988-2007)
  - 数据备份与灾难恢复的关系
    - 数据备份是灾难恢复的前提和基础，而灾难恢复是在此基础之上的具体应用。
    - 灾难恢复的目标与计划决定了所需要采取的数据备份策略。而灾难恢复策略也应该依据数据备份的情况来制定。

9.2 灾难恢复

- 9.2.3 容灾
  - 容灾
    - 就是减少灾难事件发生的可能性以及限制灾难对关键业务流程所造成的影响的一整套行为。
  - 容灾目的
    - 保持信息系统的业务持续性，将灾难损失降到可容忍的范围。
  - 容灾方案考虑要点：
    - 灾难的类型
    - 恢复时间
    - 恢复程度
    - 实用技术
    - 成本

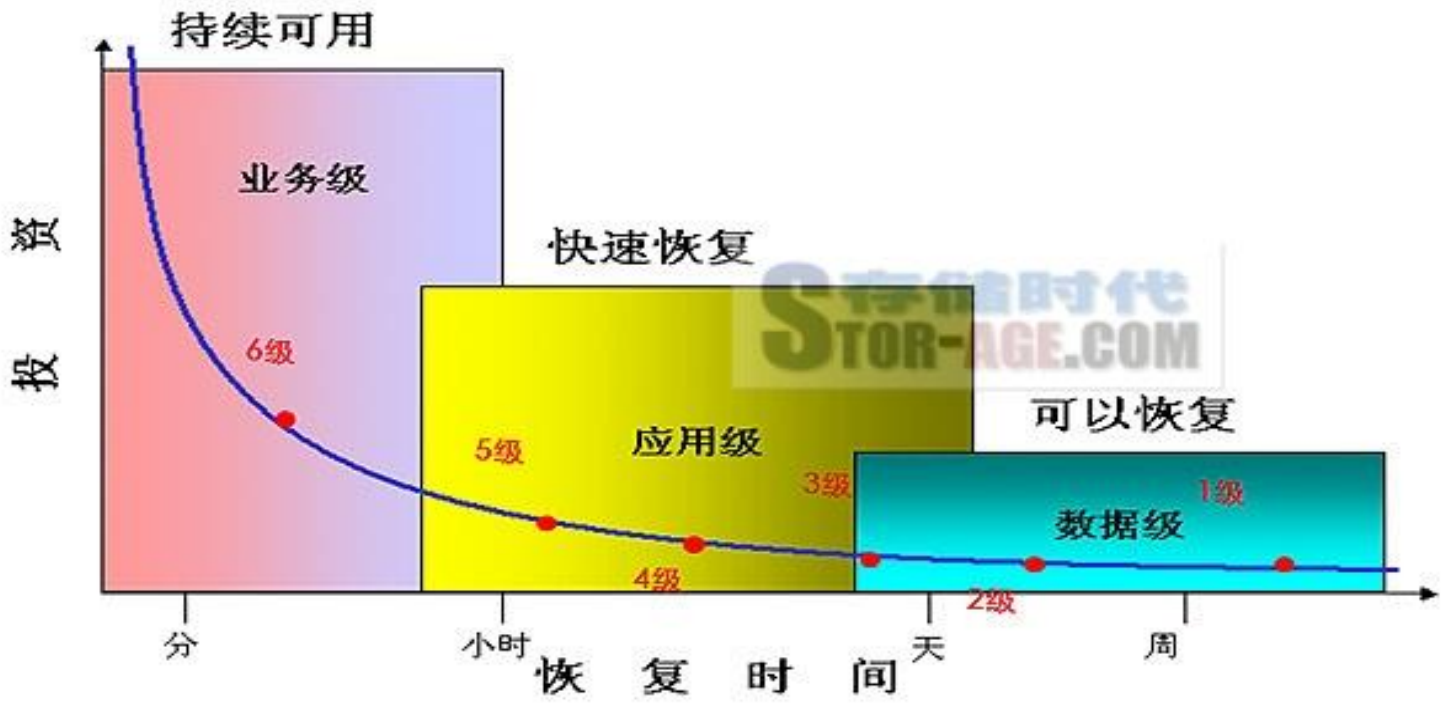
9.2 灾难恢复

- 9.2.3 容灾
  - 容灾分类
    - 按照所保障的内容可以分为：
    - 数据级容灾
      - 通过采取一定的措施确保用户数据的完整性、可靠性、安全性和一致性，但信息系统提供的实时服务在灾难发生时可能会中断，用户的应用服务请求不能得到及时响应。
    - 应用级容灾
      - 在保证用户数据的完整性、可靠性、安全性和一致性的前提下，提供不间断的应用服务，让客户的应用服务请求能够透明地毫无察觉灾难发生地继续运行。
    - 业务级容灾
      - 保证业务持续性

9.2 灾难恢复

- **9.2.3 容灾**
  - **– 容灾分类**

灾备级别与投资的关系



9.2 灾难恢复

- 9.2.3 容灾
  - 容灾分类
    - 按照容灾功能实现的距离远近可分为：
    - 本地容灾
      - 主要手段是容错：基本思想是在系统体系结构上精心设计，利用外加资源的冗余技术来达到屏蔽故障，自动恢复系统或安全停机的目的。
        - » 外加资源的容错方法：主要包括硬件冗余、时间冗余、信息冗余和软件冗余。
        - » 容错技术的采用使得容灾系统能恢复大多数的故障。
    - 异地容灾
      - 指在相隔较远的异地，建立两套或多套功能相同的IT系统。当主系统因意外停止工作时，备用系统可以接替工作，保证系统的不间断运行。
      - 主要方法是数据复制：目的是在本地与异地之间确保各系统关键数据和状态参数的一致。
      - 异地容灾的地址选择：要确保两地不会同时遭受相同类型的灾害，以使得主系统和备份系统同时遭受破坏。

9.2 灾难恢复

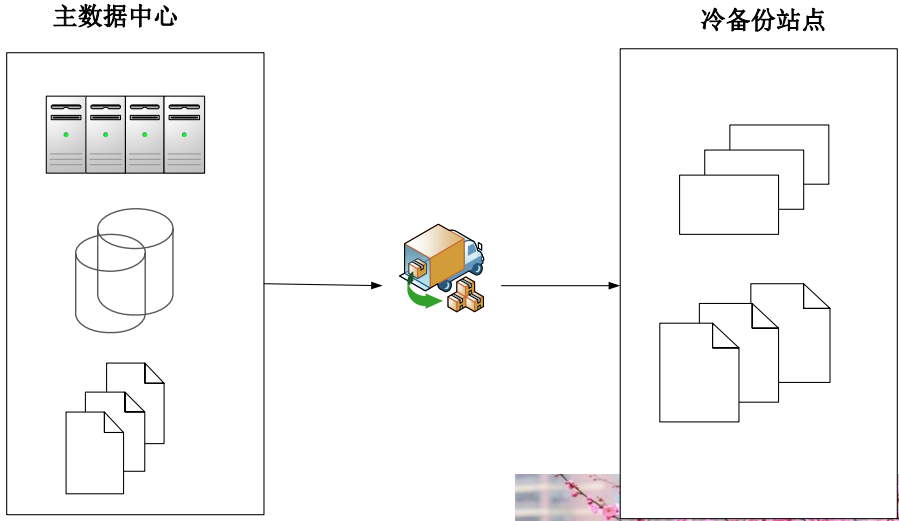
- 9.2.3 容灾
  - 容灾等级划分
    - 第0级——本地冗余备份
      - 投资少，技术简单，但原始数据和备份数据可能一起被毁
    - 第1级——数据介质转移
      - 数据异地存放，安全保管，但无备用系统，会丢失部分数据
    - 第2级——应用系统冷备
      - 数据异地存放，有备用系统，系统硬件冷备份，会丢失部分数据
    - 第3级——数据电子传送
      - 使用网络传输技术，自动异地备份，提高备份频率
    - 第4级——应用系统温备
      - 备份系统处于活动状态，数据恢复达到小时级
    - 第5级——应用系统热备
      - 系统镜像，同步更新，灾难发生时需要人工切换，数据恢复达到分钟级
    - 第6级——数据零丢失
      - 在线实时镜像，作业动态分配，自动切换

9.2 灾难恢复

- 9.2.3 容灾
  - 容灾等级划分
    - 1992年美国SHARE 78 标准：将容灾系统分为七层，分别适用于不同的规模和应用场合。
    - 第0 级—没有异地数据(No Off-site Data)
      - 没有信息存储的需求，不需要建立备援硬件平台或发展应急计划。
      - 0 级容灾系统事实上并不具有灾难恢复的能力，因为它的数据仅在本地进行备份和恢复，并没有被送往异地保存。

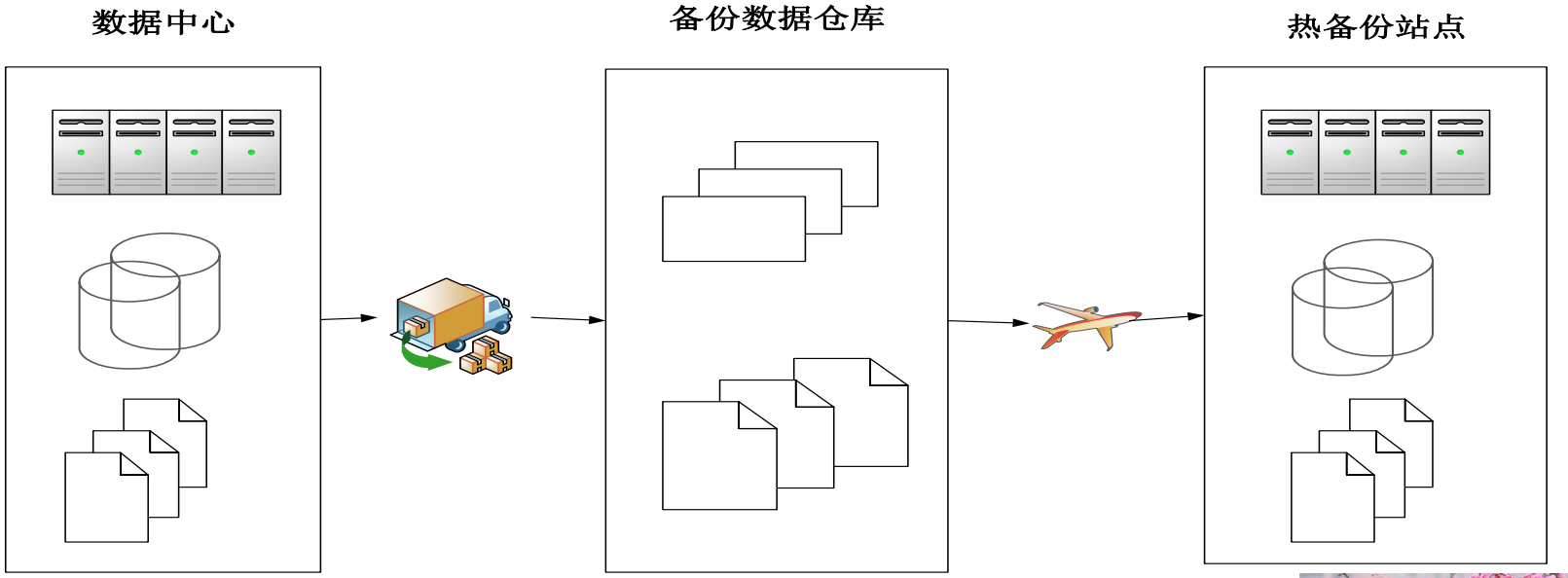
9.2 灾难恢复

- 9.2.3 容灾
  - 容灾等级划分
    - 第1 级—PTAM (Pickup Truck Access Method, 卡车运送访问方式)
      - 要求设计一个灾难恢复方案，根据该方案在平时备份所需要的信息并将它运送到异地保存，灾难发生时将根据需要，有选择地搭建备援的硬件平台并在其上恢复数据。
      - 典型恢复时间1周左右。



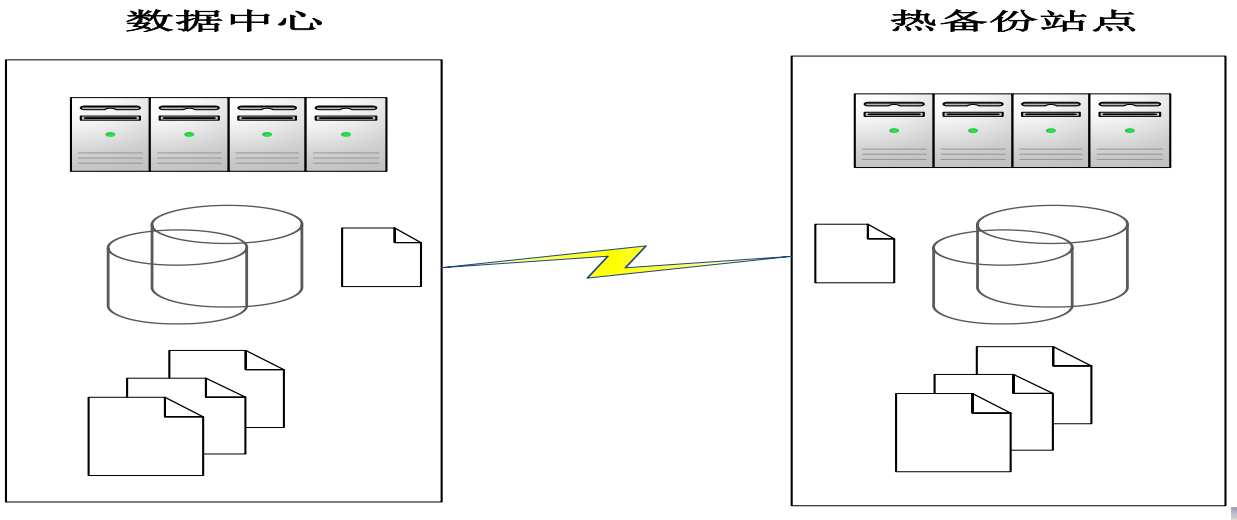
9.2 灾难恢复

- 9.2.3 容灾
  - 容灾等级划分
    - 第2 级—PTAM + 热备份站点
      - 在第1 级的基础上增加了一个热备份站点；
      - 典型恢复时间1天左右。



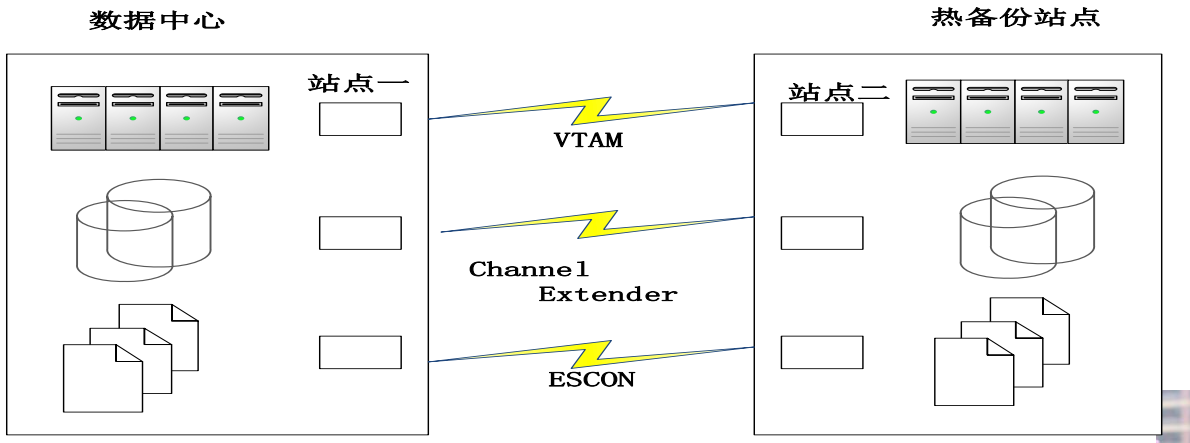
9.2 灾难恢复

- 9.2.3 容灾
  - 容灾等级划分
    - 第3 级—电子链接(Electronic Vaulting)
      - 在第2 级的基础上用电子链路取代了卡车进行备份数据传送的容灾系统，直接建立热备份站点；
      - 典型恢复时间在一天以内的小时级。



9.2 灾难恢复

- 9.2.3 容灾
  - 容灾等级划分
    - 第4 级—活动状态的备援站点(Active Secondary Site)
      - 要求地理上分开的两个站点同时处于工作状态,并相互管理彼此的备份数据。该系统自最近一次数据复制以来的业务数据将会丢失,其它非关键应用也将需要手工恢复。
      - 关键应用的灾难恢复时间降低到了小时级或分钟级。



9.2 灾难恢复

- 9.2.3 容灾
  - 容灾等级划分
    - 第5 级—双站点,两步提交(Two-Site , Two-Phase Commit)
      - 与第4 级的结构类似,在满足第4 级所有功能要求的基础上,进一步提供了两个站点间的数据互作镜像(数据库的一次提交过程会同时更新本地和远程数据库中的数据) 。
      - 恢复的时间被降低到了分钟级。

9.2 灾难恢复

- 9.2.3 容灾
  - 容灾等级划分
    - 第6 级—零数据丢失(Zero Data Loss)
      - 灾难恢复的最高级别：实现零数据丢失。
        - » 只要用户按下ENTER 键向系统提交了数据,那么不管发生了什么灾难性事件,系统都能保证该数据的安全。
        - » 所有的数据都将在本地和远程数据库之间同步更新,当发生灾难事件时,备援站点能通过网络侦测故障并立即自动切换,负担起关键应用。
      - 容灾系统中最昂贵的方式，也是速度最快的恢复方式。

9.2 灾难恢复

- 9.2.4 灾难恢复需求
  - 灾难恢复计划要点
    - 确定灾难恢复的需求
    - 寻求解决方案
    - 执行计划
    - 维护计划

9.2 灾难恢复

- **9.2.4 灾难恢复需求**
  - 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

9.2 灾难恢复

- 9.2.4 灾难恢复需求
  - 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：以量化方法，评估业务功能的中断可能给组织带来的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，包括组织的声誉、客户的忠诚度、员工的信心、社会和政治影响等。

9.2 灾难恢复

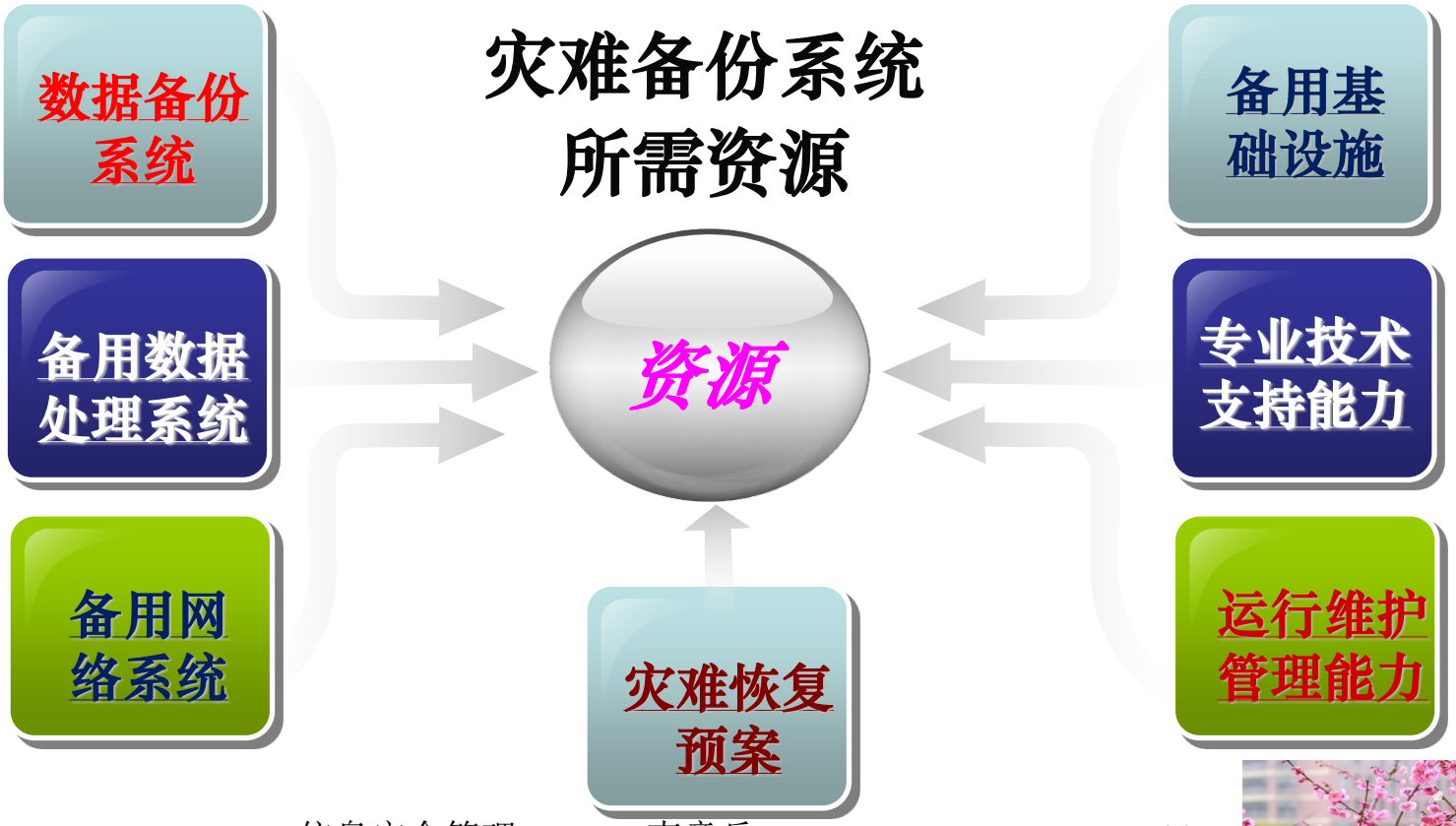
- 9.2.4 灾难恢复需求
  - 确定灾难恢复目标
    - 根据风险分析和业务影响分析的结果，确定灾难恢复目标
      - 关键业务功能及恢复的优先顺序；
      - 灾难恢复时间范围。
  - 制定灾难恢复计划

• 获得管理层的支持 • 选定负责人 • 组成一个跨部门的小组	• 进行业务影响分析 • 明确优先次序 • 评估可能的业务连续性战略	• 为灾难恢复小组选择成员并明确分工 • 制定灾难恢复文档 • 经常对计划测试 • 每次测试之后进行经验总结

9.2 灾难恢复

• 9.2.5 灾备系统资源

– 国标GB/T 20988-2007将支持灾难恢复各个等级所需的资源（以下简称“灾难恢复资源”）分为7个要素，制定灾难恢复策略时，应根据灾难恢复需求确定灾难恢复等级，并依照灾难恢复等级要求确定各资源要素的具体要求。



9.2 灾难恢复

- 9.2.5 灾备系统资源
  - 数据备份系统
    - 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

9.2 灾难恢复

- 9.2.5 灾备系统资源
  - 备用数据处理系统
    - 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

9.2 灾难恢复

- 9.2.5 灾备系统资源
  - 备用网络系统
    - 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。

9.2 灾难恢复

- **9.2.5 灾备系统资源**
  - **备用基础设施**
    - 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

9.2 灾难恢复

- **9.2.5 灾备系统资源**
  - **– 专业技术支持能力**
    - 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**
      - 灾难备份中心在软件、硬件和网络等方面的技术支持要求；
      - 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。

9.2 灾难恢复

- 9.2.5 灾备系统资源
  - 运行维护管理能力
    - 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
      - 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。

9.2 灾难恢复

- 9.2.5 灾备系统资源
  - 灾难恢复预案
    - 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

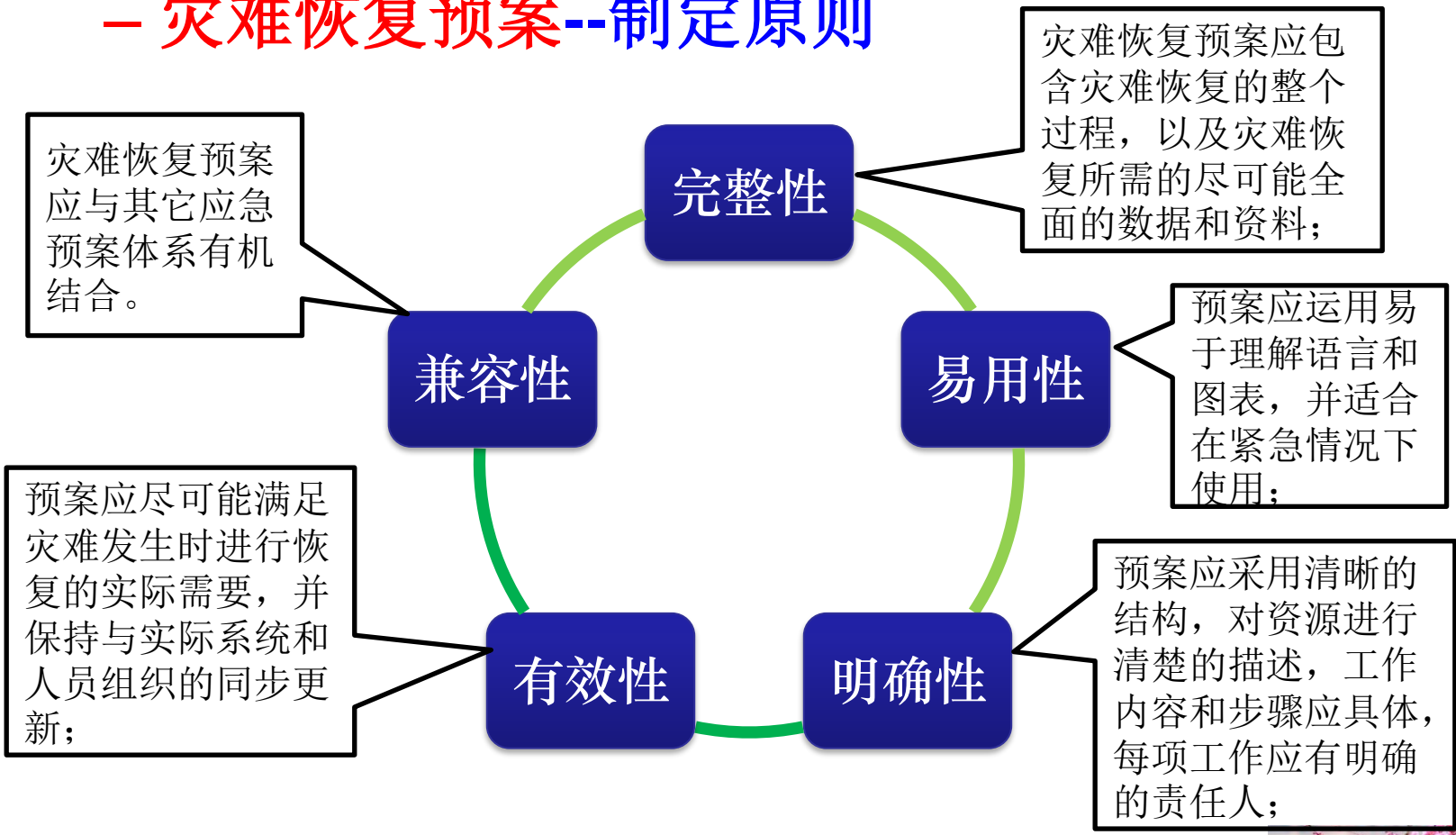
9.2 灾难恢复

- 9.2.6 灾难恢复预案与实现关键
  - 灾难恢复预案
    - 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。
    - 组织应在风险分析和业务影响分析的基础上，按照成本风险平衡原则，制定灾难恢复预案，并加强灾难恢复预案的教育培训、演练和管理。

9.2 灾难恢复

• 9.2.6 灾难恢复预案与实现关键

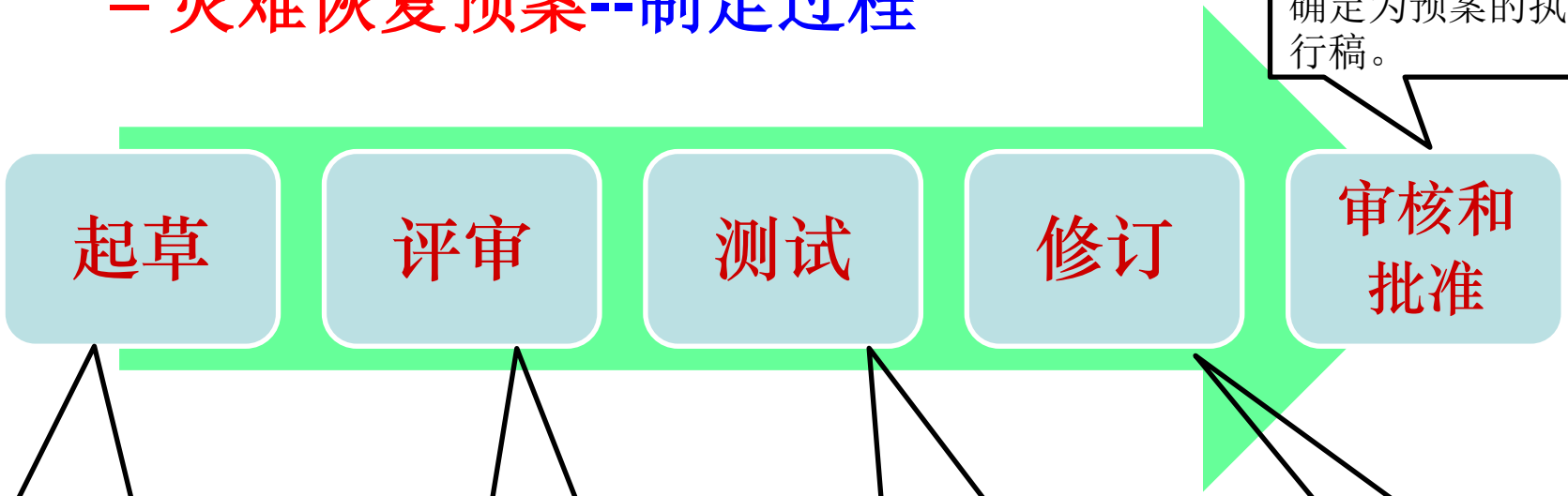
– 灾难恢复预案--制定原则



9.2 灾难恢复

• 9.2.6 灾难恢复预案与实现关键

– 灾难恢复预案--制定过程



参照灾难恢复预案框架，按照风险分析和业务影响分析所确定的灾难恢复内容，根据灾难恢复等级的要求，结合组织其它相关的应急预案，撰写出灾难恢复预案的初稿。

组织应对灾难恢复预案初稿的完整性、易用性、明确性、有效性和兼容性进行严格的评审。评审应有相应的流程保证。

应预先制定测试计划，在计划中说明测试的案例。测试应包含基本单元测试、关联测试和整体测试。测试的整个过程应有详细的记录，并形成测试报告。

根据评审和测试结果，对预案进行修订，纠正在初稿评审过程和测试中发现的问题和缺陷，形成预案的报批稿。

由灾难恢复领导小组对报批稿进行审核和批准，确定为预案的执行稿。

9.2 灾难恢复

- 9.2.6 灾难恢复预案与实现关键
  - 灾难恢复实现关键--灾难检测
    - 心跳技术
      - 又称为拉技术，就是每隔一段时间都要向外广播自身的状态（通常为“存活”状态）。
      - 心跳检测的时间和时间间隔是关键问题，如果心跳检测的太频繁，将会影响系统的正常运行，占用系统资源；如果间隔时间太长，则检测就比较迟钝，影响检测的及时性。
    - 检查点技术
      - 又称为主动检测，就是每隔一段时间周期，就会对被检测对象进行一次检测，如果在给定的时间内，被检测对象没有响应，则认为检测对象失效。
      - 检测点技术也受到检测周期的影响，如果检测周期太短，虽然能够及时发现故障，但是给系统造成很大的开销；如果检测周期太长，则无法及时的发现故障。

9.2 灾难恢复

- 9.2.6 灾难恢复预案与实现关键
  - 灾难恢复实现关键--系统迁移
    - 在发生灾难时，为了能够保证业务的连续性，必须实现能够实现系统透明的迁移，也就是能够利用备用系统透明的代替生产系统。
      - 对于实时性要求不高的容灾系统，通过DNS或者IP地址的改变来实现系统迁移；
      - 对于可靠性、实时性要求较高的系统，就需要使用进程迁移算法；在分布式系统和集群中得到了广泛的运用。
        - » 进程迁移算法的好坏对于系统迁移的速度有很大影响。
        - » 进程迁移算法在目前主要有贪婪拷贝算法、惰性拷贝算法和预拷贝算法。

9.2 灾难恢复

- 9.2.6 灾难恢复预案与实现关键
  - 灾难恢复实现关键--灾备中心的选择和建设
    - 灾难备份中心
      - 是用于灾难发生后接替主系统进行数据处理和支持关键业务功能运作的场所，可提供灾难备份系统、备用的基础设施和技术支持及运行维护管理能力，此场所内或周边可提供备用的生活设施。
    - 选址原则
      - 应根据风险分析的结果，避免与主中心同时遭受同类风险。
      - 应具有方便灾难恢复人员或设备到达的交通条件，以及数据备份和灾难恢复所需的通信、电力等资源。
      - 应根据资源共享、平战结合的原则，合理地布局。
    - 基础设施的要求
      - 新建或选用灾难备份中心的基础设施时，计算机机房应符合有关国家标准的要求，工作辅助设施和生活设施应符合灾难恢复目标的要求。

本章小结

作业

- 1.什么是业务连续管理BCM？其策略过程如何？
- 2.什么是BIA？
- 3.什么是应急响应？目的如何？应急响应分类和级别？
- 4.什么是灾难和灾难恢复？