

3.1 业务连续性计划

- 业务连续性计划(BCP): 对组织各种过程的风险评估，发生风险的情况下为了使风险对组织的影响降至最小而定制的各种计划
- BCP和DRP首先考虑的人不受到伤害，然后再解决IT恢复和还原问题
- BCP的主要步骤：
 - i. 项目范围和计划编制
 - ii. 业务影响评估
 - iii. 连续性计划
 - iv. 批准和实现

3.2 项目范围与计划

3.2.1 业务组织分析

- 负责BCP计划编制的人员，首要职责之一就是进行业务组织分析

3.2.2 BCP团队的选择

- BCP的团队至少包括下列人员
- 核心服务部门代表
- 重要支持部门代表
- 技术专长的IT代表
- 了解BCP的安全代表
- 法律代表
- 高层管理

3.2.3 资源要求

BCP不同阶段所需资源

- BCP开发：实施BCP过程的四个要素(项目范围和计划编制、业务影响评估、连续性计划、批准和实现)
- BCP测试、培训和维护
- BCP实现：实现BCP需要大量资源，包括大量人力资源

3.2.4 法律和法规要求

- 许多行业受到联邦政府、州和地方法律或法规的限制
- 许多国家、金融机构和公司在处理数据时，会受到政府和国际银行与证券制度的严格控制
- BCP过程中，将组织的法律顾问添加进来是非常重要的

3.3 业务影响评估 (BIA)

3.3.1 确定优先级

- 每个参与者创建一个优先级列表，从而创建一个优先级主列表
- 最大允许中断时间(MTD)：某个业务功能出现故障但是不会对业务产生无法弥补的损失的最大终端时间
- 恢复时间目标 (RTO)：恢复时间目标
- BCP过程的目标确保RTO小于MTD

3.3.2 风险识别

- BIA过程的风险识别部分是纯粹的定性分析

3.3.3 可能性评估

- 可能性评估通常使用年发生比率(ARO)表示

3.3.4 影响评估

- 定量分析影响评估: $ALE = SLE * ARO$
- 定性分析影响评估: 丧失的声誉、员工的流失、社会/道德责任、消极的公共影响

3.3.5 资源优先级划分 (BIA)

- BIC的最后一个步骤是位不同风险所分配的业务连续性资源的优先级
- 合并定量和定性优先级列表

3.4 连续性计划

3.4.1 策略开发

- 策略开发：决定需要缓解的风险和每种缓解任务将被交付的资源级别

3.4.2 预备和处理

- 在这个过程中BCP团队设计具体的过程和机制，将在策略开发阶段缓解被认为不可接受的风险

- 通过BCP预备和处理保护的资产人、建筑物/设备、基础设施
- 人：认识最有价值的资产，人的安全必须始终优于公司的商业目的
- 建筑物/设备：
 - 强化预备措施，采取措施保护设施抵御策略开发阶段定义的风险
 - 预备场所：确定业务活动可以立即回复的预备场所
- 基础设施：
 - 强化系统：引入保护性措施为系统抵御风险
 - 预备系统：引入冗余性保护

3.4.3 计划批准和实现

- 完成BCP文档设计阶段，申请获得高级管理层的批准

3.4.4 计划实现

- 高级管理员实批准后，BCP团队共同开发一个实现计划

3.4.5 培训和教育

- 对具体的BCP任务评估，确保灾难发生时能有效完成其任务，人员的冗余性

3.5 BCP文档化

- 确保BCP有一个连续性的书面文档，甚至资深BCP团队成员不在场可参考
- 提供BCP过程的历史记录
- 促使团队成员将他们的想法记录到纸上

3.5.1 连续性计划的目标

- 计划应当描述BCP团队和高级管理员提出的连续性计划目标

3.5.2重要性声明

- 重要性声明反应了BCP对于组织继续生存能力的关键程度

3.5.3优先级声明

- 优先级声明是业务影响评估的优先级确定阶段的直接产物

3.5.4 组织责任声明

- 来自高管，重申组织对业务连续性计划的承诺

3.5.5 紧急程度和实现声明

- 参数实现BCP的关键性，并概述上层管理者同意的实现时间表

3.5.6 风险评估

3.5.7 可接受的风险/风险缓解

3.5.8 重大记录计划

3.5.9 影响紧急事件的指导原则

3.5.10 维护

持续维护BCP文档和计划

3.5.11 测试和演习