业务连续性和灾难恢复的具体操作

Agenda

- 业务连续性管理理论回顾
- 业务连续性管理的具体步骤
- 业务连续性演练方法
- Q&A

背景

- 日益频繁发生的灾难
  - 自911恐怖袭击、2003年的非典和2004年的印度洋大海啸后，尤其2008年我国发生的四川汶川大地震，使人们更加意识到灾难随时随地都可能发生， 直接威胁到公司的正常运营， 间接影响到公司的声誉、品牌、信誉， 甚至公司的存亡。
- 业务中断对企业的影响
  - 随着企业的业务对IT的依赖越来越高， IT如何面对灾难对业务造成的巨大损失、面对业务部门不断攀升的服务要求， 面对复杂的系统， 合理地把工作做在灾难发生之前，主动预防，成为IT管理者必须直面“永续运行”的课题。

基本概念

- **1风险**

发生某种威胁使资产损失或破坏的潜在可能

- **2事故**

可以或可能导致组织业务中断、损失的突发情况或事件

- **3灾难**

灾难是对组织产生灾害性影响的事故，或者大范围影响业务正常运行的事故

- **4业务中断**

预先计划的（如员工罢工、飓风）或者是非计划的（黑客入侵或地震）的事件，产生了与组织目标所期望的产品或服务的交付物产生了非计划的、负面的背离结果

基本概念

5灾难备份

灾难备份是指为了减少灾难发生的概率，以及减少灾难发生时或发生后造成的损失而采取的各种防范措施。

6灾难恢复

灾难恢复是一个在发生计算机系统灾难后，在远离灾难现场的地方重新组织系统运行和恢复营业的过程。

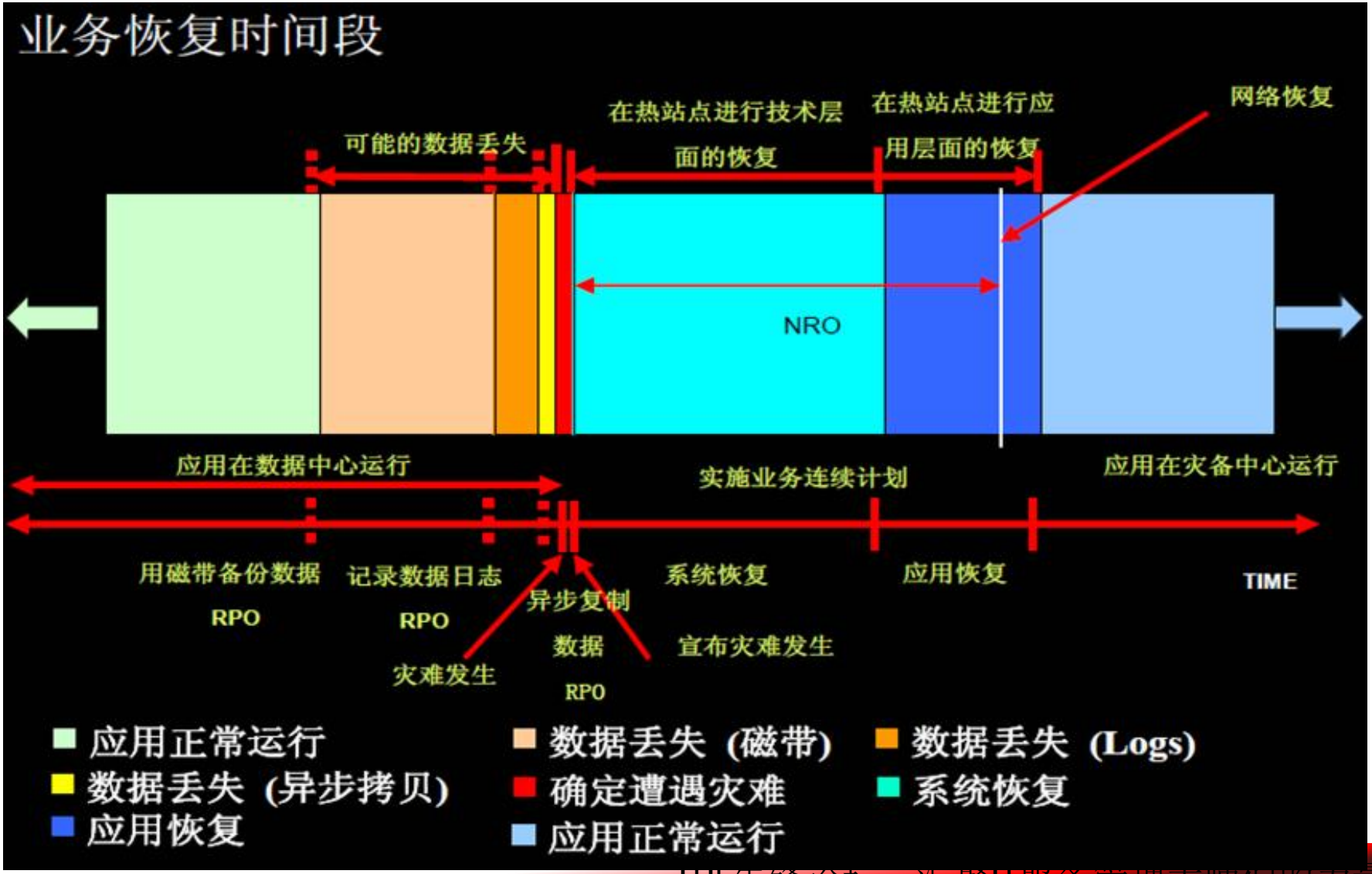
灾难恢复的目标是保护数据的完整性，使业务数据损失最少甚至没有业务数据损失。二是快速恢复营业，使业务停顿时间最短甚至不中断业务。

如何应对灾难—覆巢之下，亦有完卵

- 911恐怖袭击发生一年后统计，原来世贸大厦中的350家公司，重新开张的只有150家，200 家企业由于重要信息系统的破坏，关键数据的丢失而永远的关闭、消失了。

- 在世贸大厦租有25 层的金融界巨头摩根斯坦利公司，事发几个小时后，该公司宣布：全球营业部可以在第二天照常工作。

灾难恢复的生命周期



业务连续性管理的定义

业务持续管理是一个整体性的管理流程，它主要识别公司潜在的风险和提供一个建立快速恢复能力和有效反应能力的框架，从而减低灾难给业务带来的冲击以及确保公司关键业务的持续性，它旨在提高组织面对业务中断的复原力，以达到组织的关键目标；

- 当发生中断后，在业务可接受的时间内和服务水平下，提供给组织支持关键产品和服务的恢复能力；
- 交付验证管理业务中断能力，并保护组织的声誉和品牌；

BCM,ITSCM,IT DRP的关系和区别

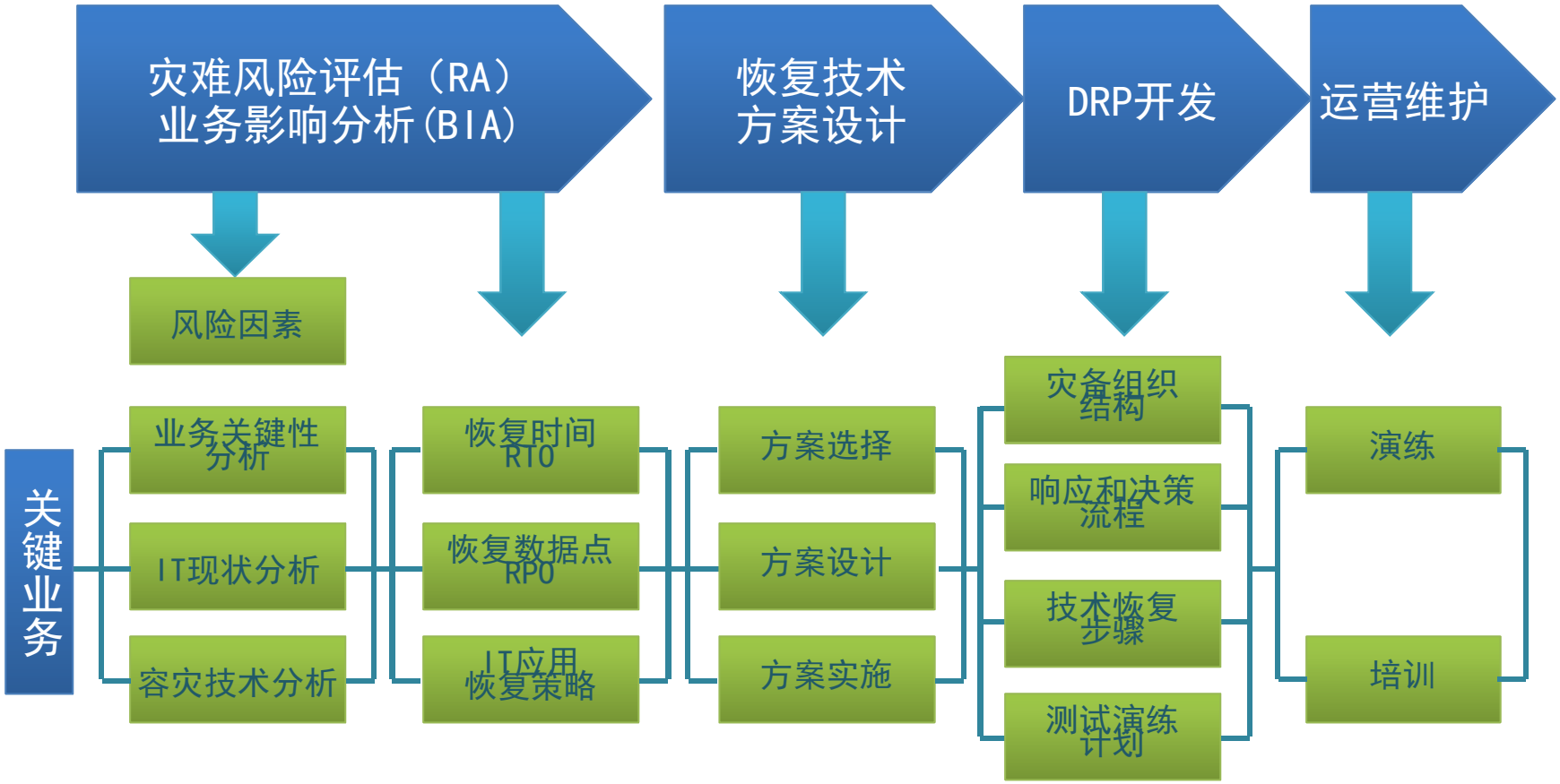
	业务连续性管理（BCM）	IT服务连续性管理（ITSCM）	IT灾难恢复计划（IT DRP）
主要目标	管理业务风险，确定业务可用性	当意外发生时在预先定义的服务水平上交付关键IT服务	当发生重大中断后恢复关键IT系统
范围	业务流程	IT服务	IT系统
职责角色	高管	CIO，CTO	IT运维经理

Agenda

- 业务连续性管理理论回顾
- 业务连续性管理的具体步骤
- 业务连续性演练方法介绍

- Q&A

业务连续性管理管理流程概览

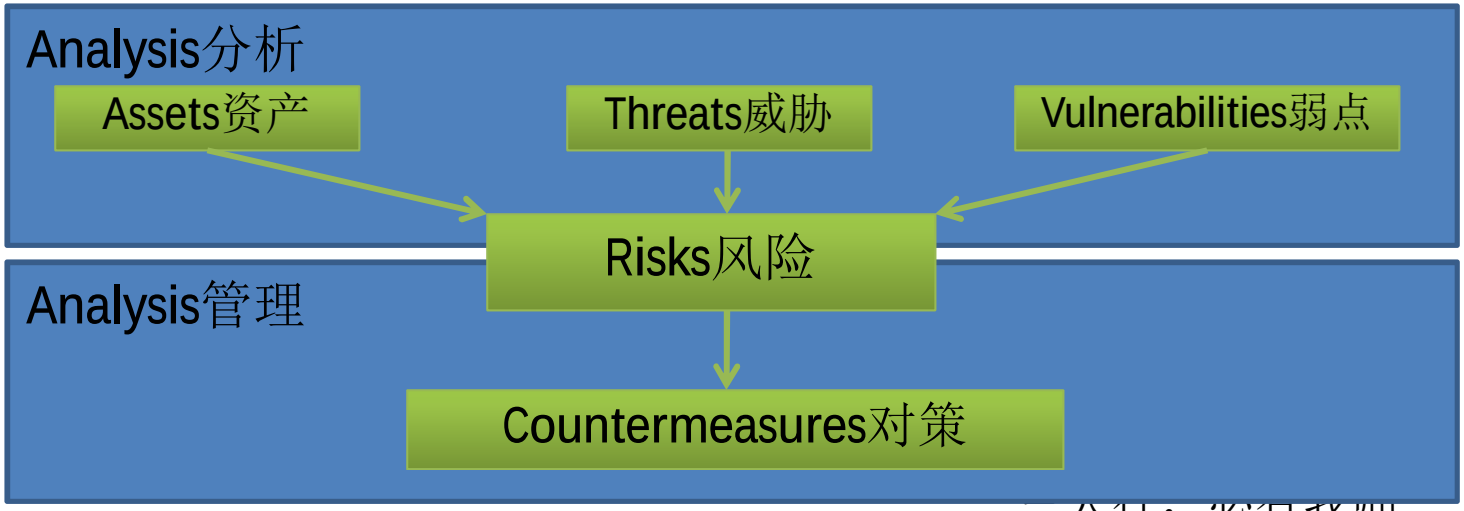


业务连续性管理的7大步骤

- 阶段一、风险分析
- 阶段二、业务影响分析
- 阶段三、企业容灾环境分析
- 阶段四、业务连续性策略制订
- 阶段五、容灾方案设计
- 阶段六、业务连续性流程设计
- 阶段七、业务连续性流程及方案管理和测试

阶段一：风险分析

- 识别支持关键IT服务的资产
- 评估威胁，或者任何可能导致服务中断的事件
- 评估自身的弱点
- 威胁对组织产生的影响
- 评估风险的可能性



信息系统资产

- 信息和数据
- 硬件
- 软件
- 服务
- 文档
- 人员

另外还有一些需要考虑的传统资产包括：建筑物、存货、资金和无形资产等。

信息系统可能受到的威胁

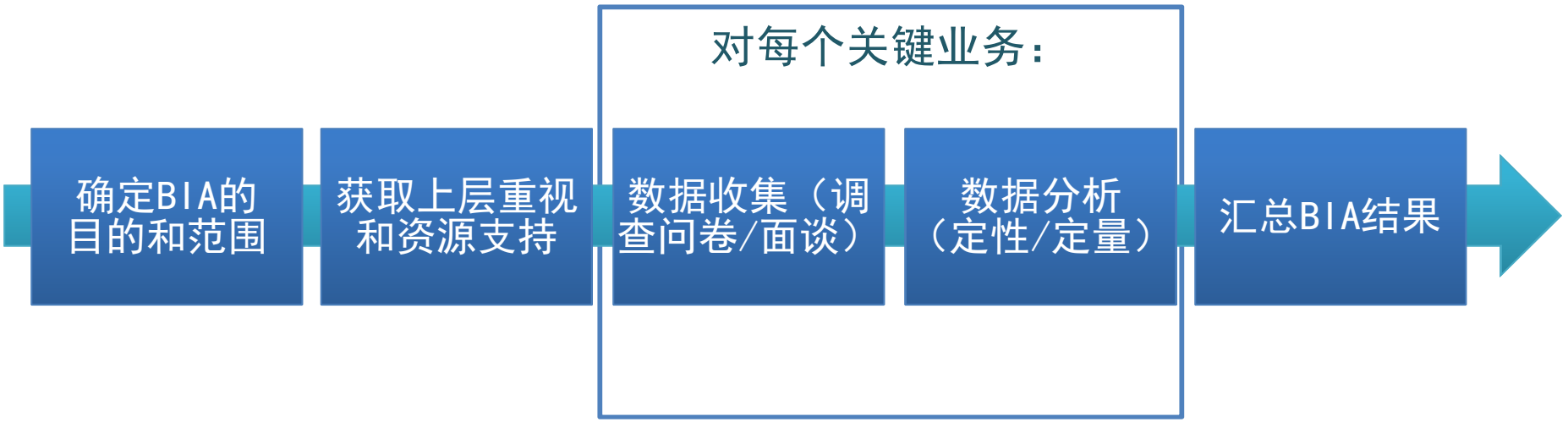
分类	特性	举例
自然灾害	受害程度高	地震，风灾，水灾，火灾等等
人为破坏	以破坏为主要目的	爆炸，恐怖袭击
意外故障	突发的非人为因素	系统故障，程序故障
人为失误	非故意的失误造成	输入数据差错，操作失误
侵犯	不正当存取，访问	黑客侵入，盗取数据

风险应对策略

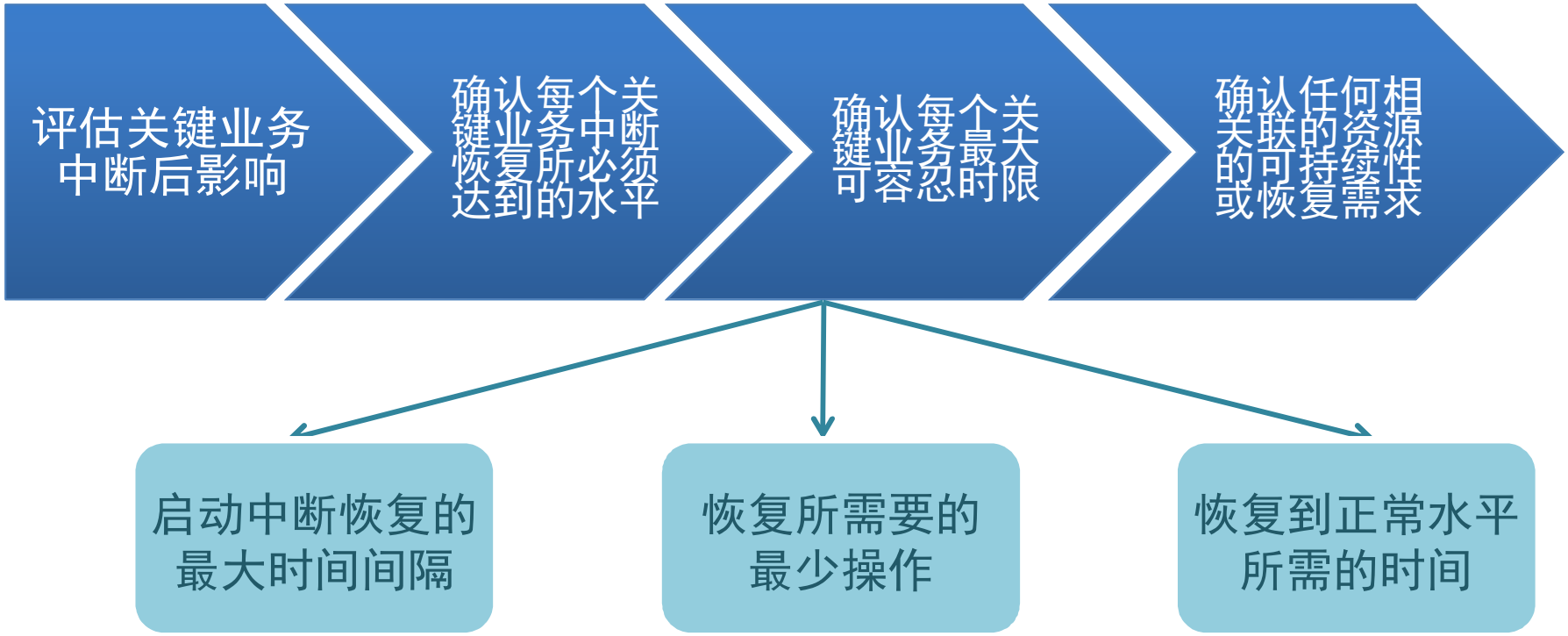
风险种类	应对策略	解释
高危低频	降低	利用政策或措施将风险降低到可接受的水平，如建设异地容灾心
高危高频	避免	避免受未来可能发生事件的影响而消除风险，如HA
低危高频	转移	将风险转移给资金雄厚的独立机构，如系统维护外包
低危低频	接受	维持现有的风险水平，如金融危机

阶段二：业务影响分析

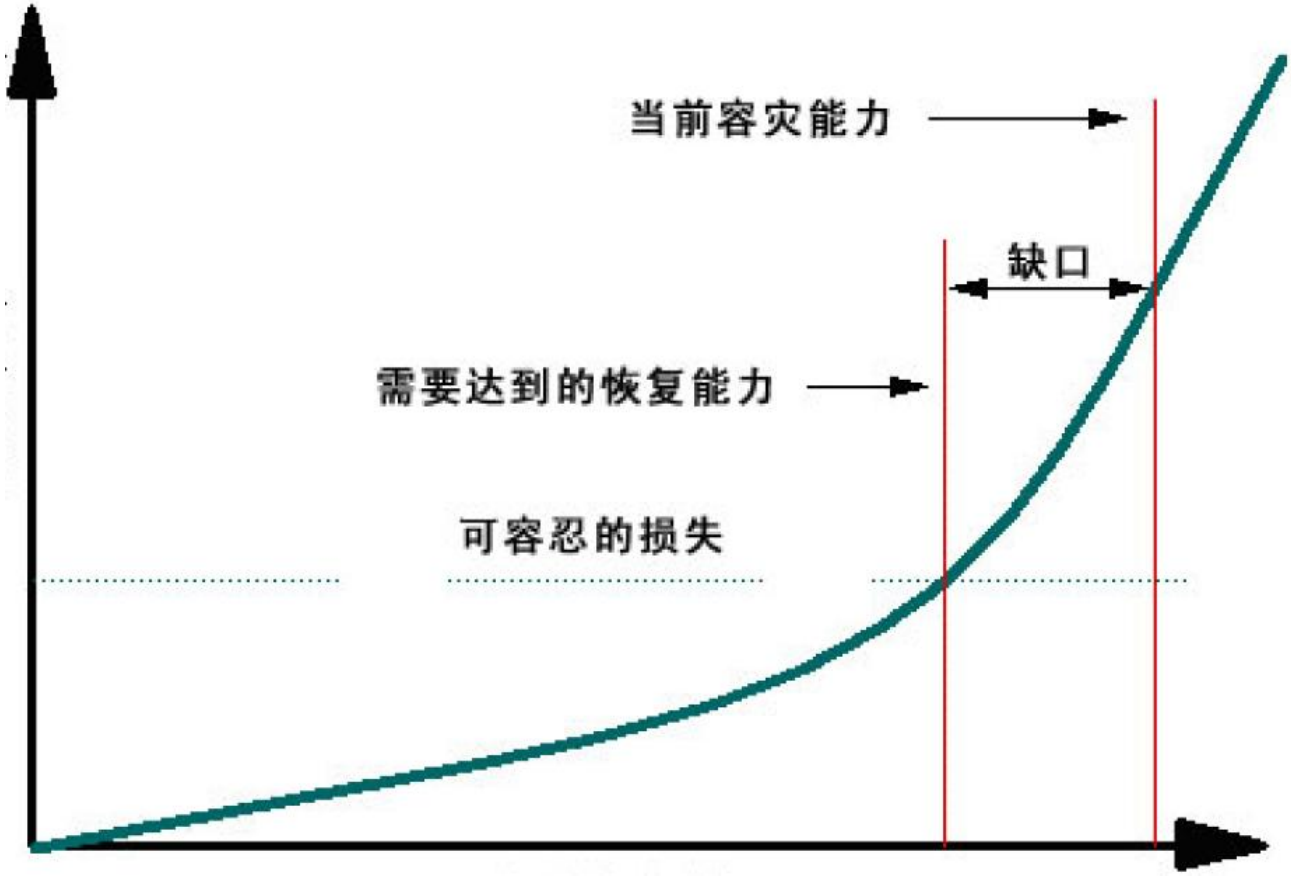
- 业务影响分析（BIA）：是组织评估和文档化业务活动中断对其所支持的关键产品和服务的影响
- BIA的工作流程



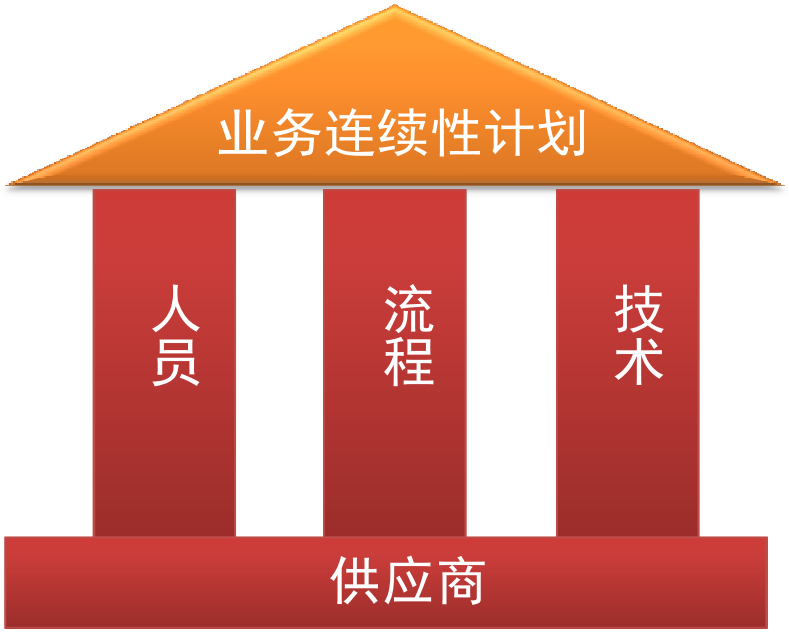
关键业务的影响分析


评估关键业务中断后影响
确认每个关键业务中断恢复所必须达到的水平
确认每个关键业务最大可容忍时限
确认任何相关联的资源性的可持续性或恢复需求
启动中断恢复的最大时间间隔
恢复所需要的最少操作
恢复到正常水平所需的时间

阶段三：企业容灾环境分析

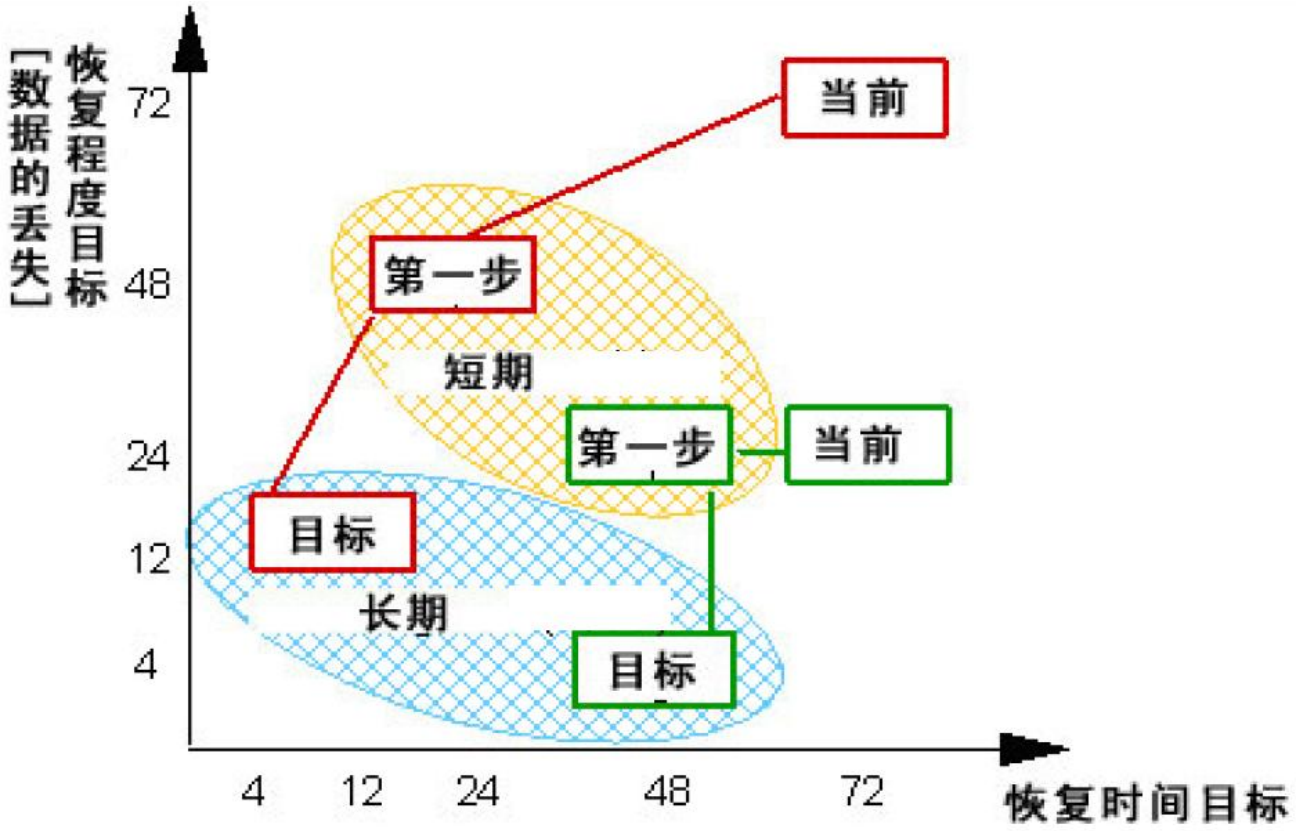


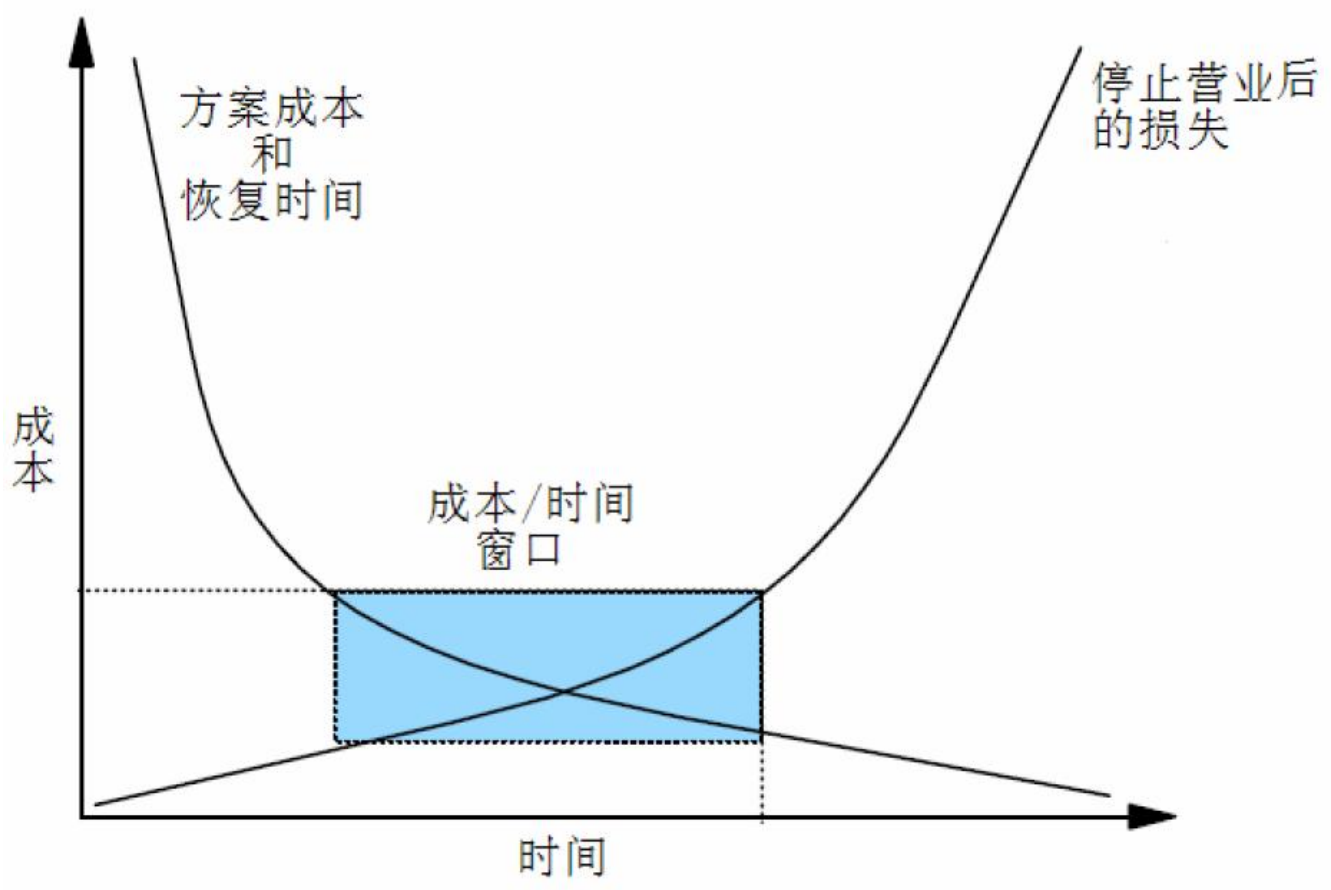
业务连续性的重要方面—4P



- Ø 人员是技术和流程的制定者和执行者
- Ø 流程是指导、约束人员、操控技术、开展业务的保障
- Ø 技术是实现手段和工具
- Ø 供应商是为客户提供服务的机构

阶段四：业务连续性策略制订

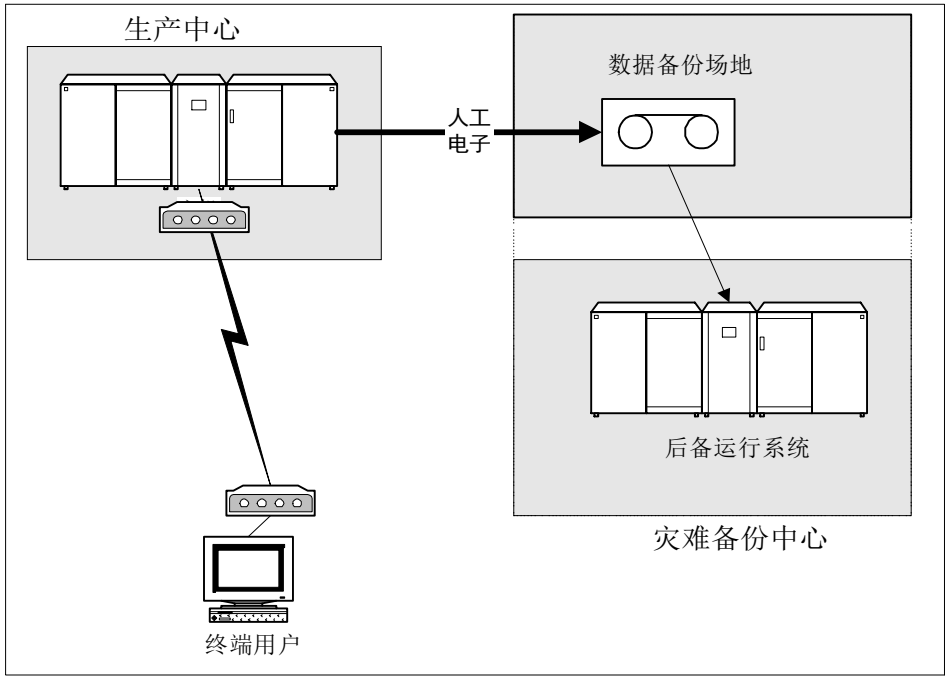




阶段五、容灾方案设计

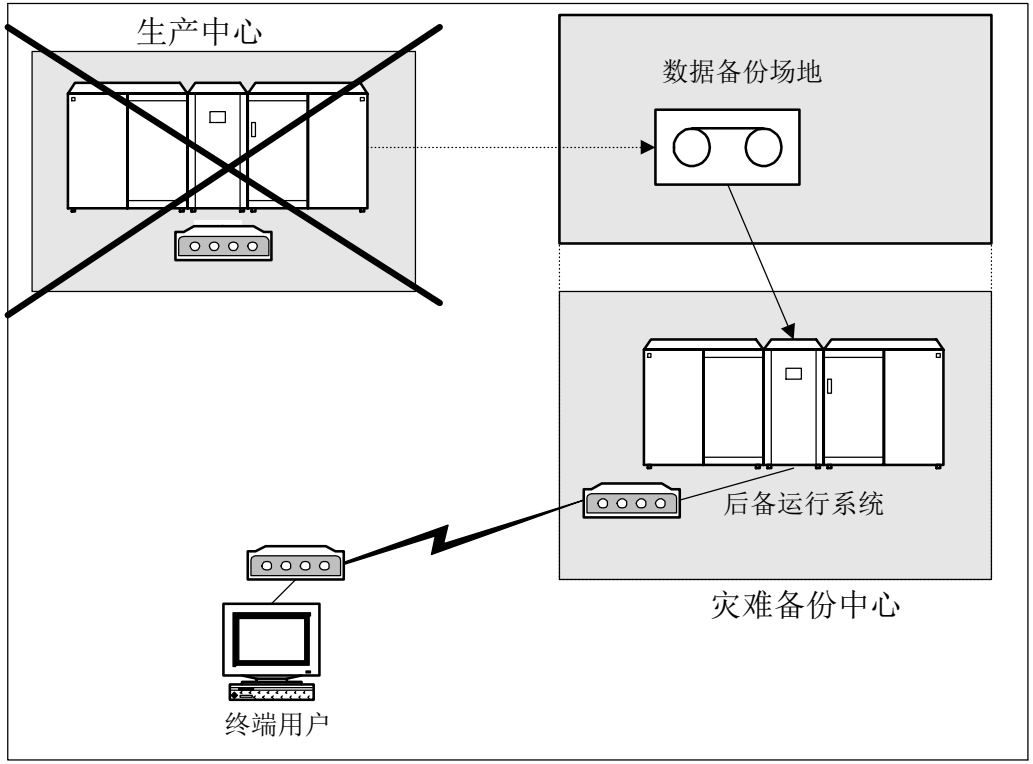
灾难备份系统的组成

- 灾难备份系统一般由可接替生产系统运行的后备运行系统、数据备份系统、终端用户切换到备份系统的备用通讯线路等部分组成。
- 在正常生产和数据备份状态下，生产系统通过人工或网络传输方法向备份系统传送需备份的各种数据。备份中心与生产中心及终端用户的关系如图所示。



灾难备份系统的组成

- 灾难发生后，备份系统将接替生产系统继续运行，备份中心、生产中心及终端用户三者之间的关系如图所示。此时重要营业终端用户将从生产主机切换到备份中心主机，继续对外营业。



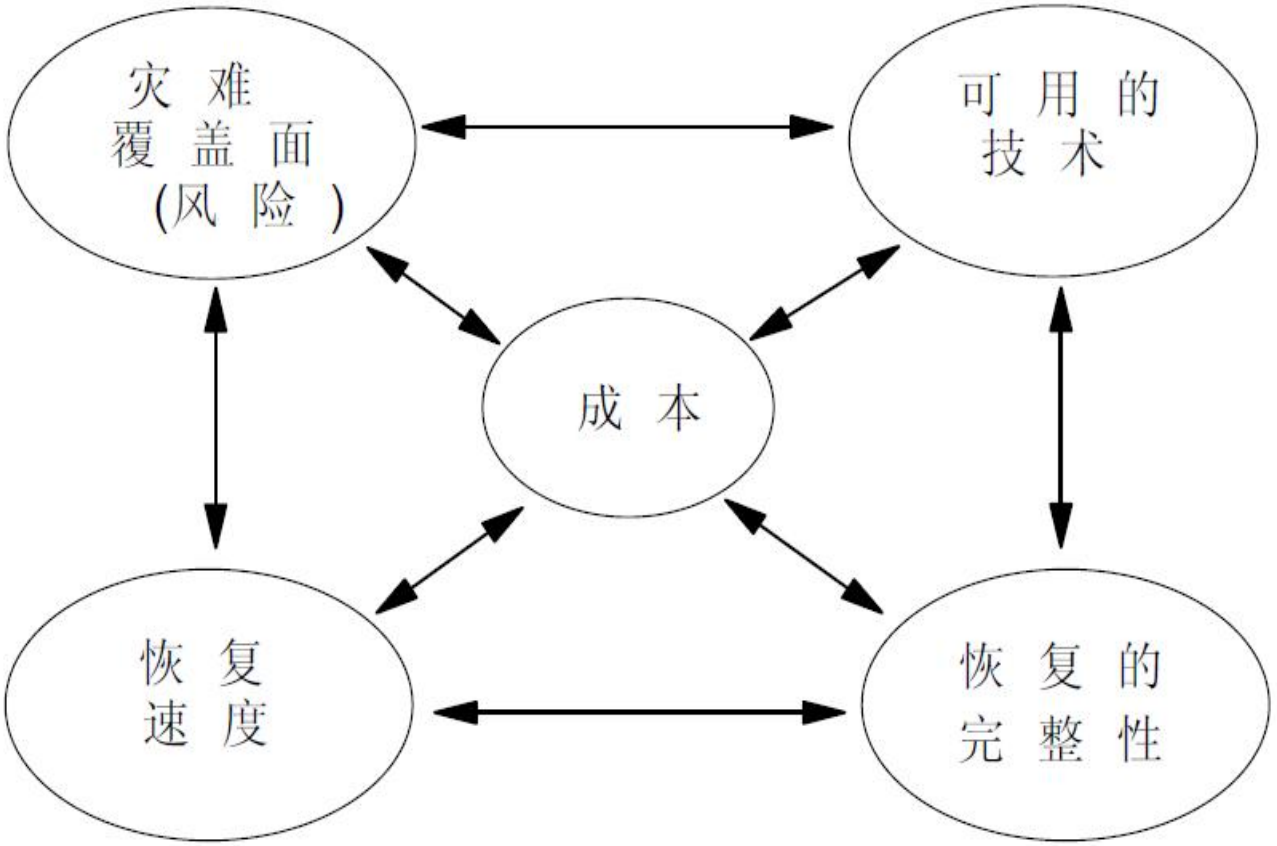
容灾数据复制主要技术方案比较

容灾分类	复制方法	主机影响	使用环境	描述	复制模式和数据一致性	维护难度	RTO/RPO要求
主机软件复制	操作系统的磁盘镜像	10-30%	同构主机	只支持同步方式，所以建议在10公里范围内使用，比较消耗系统CPU资源	同步，可以保证一致性	操作简单，但如果容灾中心的存储故障或中间链路故障，将影响到生产系统	RTO比较小；RPO接近于0
	基于逻辑卷的远程复制	10-30%	异构存储	通过IP网络将逻辑卷Log复制到异构主机，在异地主机重演逻辑卷操作I/O过程	同步和异步，可以保证一致性	一般	RTO较短；同步RPO接近0；异步RPO在分钟级
存储硬件级复制	高端磁盘阵列本身的远程数据拷贝	<8%	同构主机 同构存储	同构存储通过光纤直连方式可以支持到10公里，是采用较广的容灾方式	同步和异步，基本所有存储产品可以保证同步模式的数据一致性	维护容易；主备中心之间比较容易切换	RTO较短；同步RPO接近0；异步RPO在秒级到分钟级

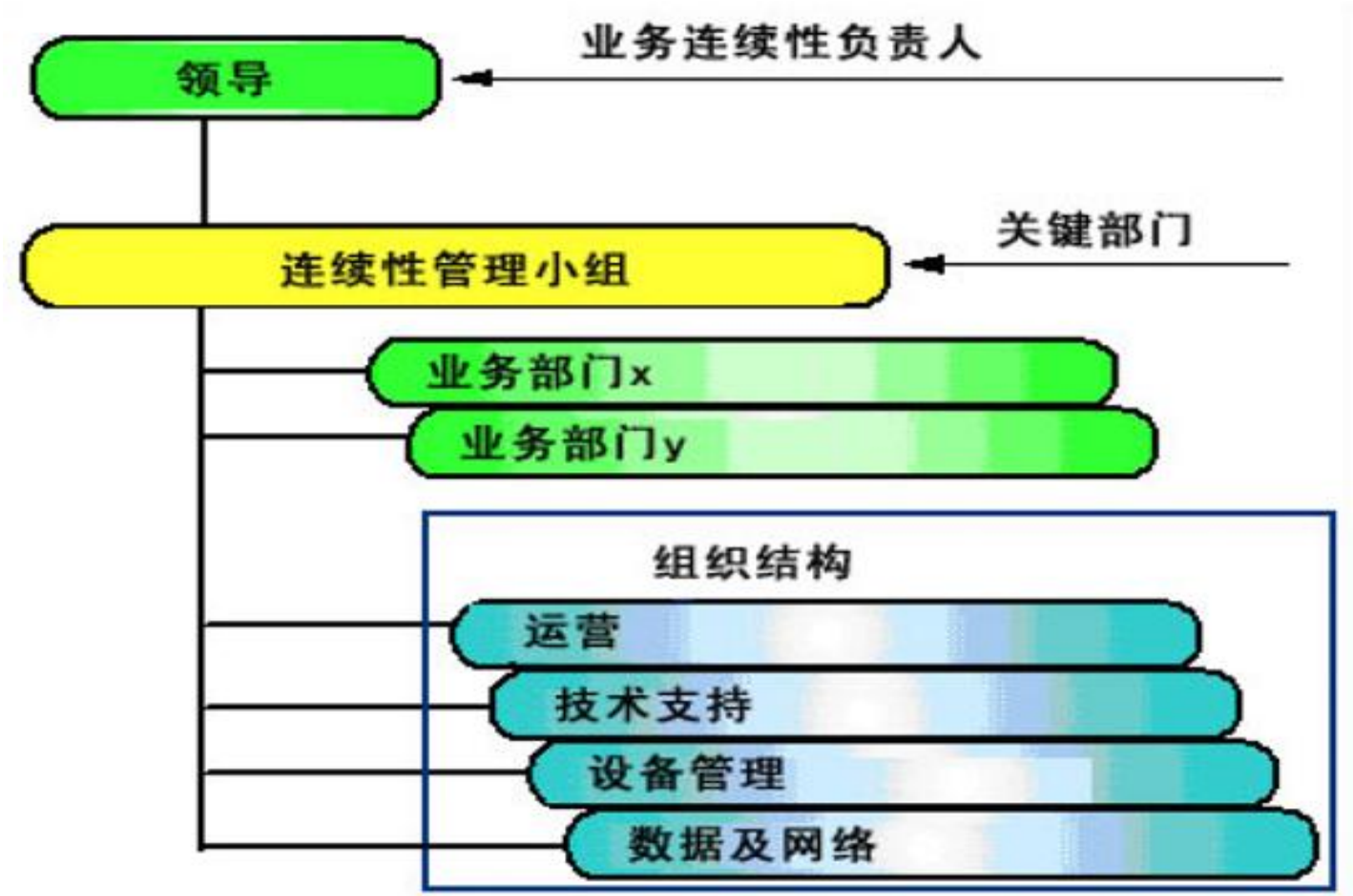
容灾数据复制主要技术方案比较

容灾分类	复制方法	主机影响	使用环境	描述	复制模式和数据一致性	维护难度	RTO/RPO要求
应用层数据复制	应用实现或通过中间件实现	<10%	异构主机 异构存储	设备投资最节省，但需要调整应用	同步或异步，可以保证数据一致性	高。应用修改需要按照容灾规范，维护成本高	交易级
数据库数据复制	数据库本身的复制功能	<10%	同构主机 异构存储 相同数据库	异步Log传输，灾难发生时会丢失少量数据，只能保护数据库里的数据，远程数据中心必须配置主机参数与数据拷贝过程	异步，可以保证数据一致性	维护成本高，主备数据库的结构、参数等需要同步变更，日常维护工作量大	丢失Log文件；RTO可以比较短，但从容灾中心回切生产中心工作量大

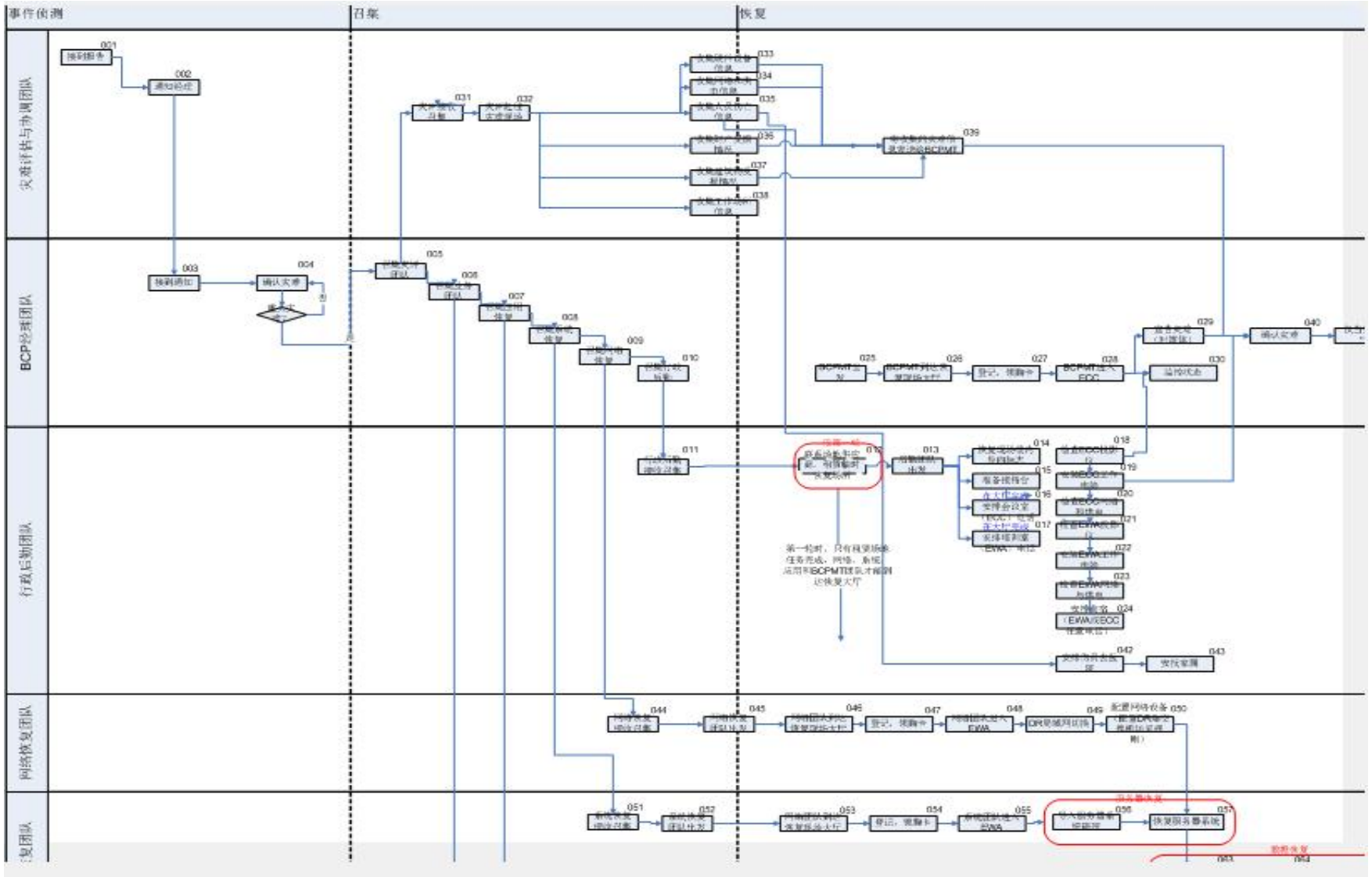
选择容灾方案的五大因素



阶段六、业务连续性流程设计



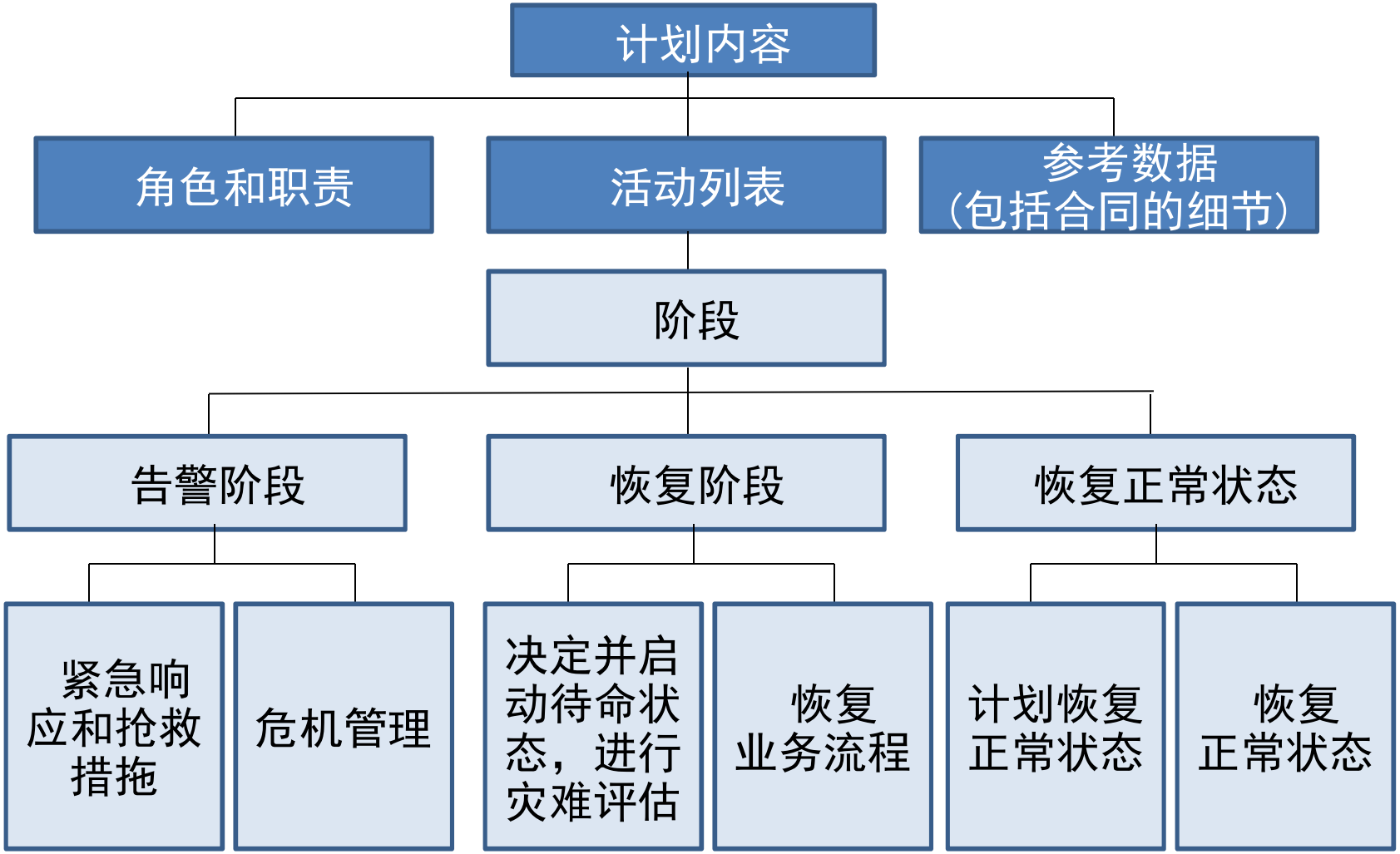
业务连续性演练流程



业务连续性计划（BCP）内容

- 目标和范围
- 角色和职责
- 任务和行动列表
- 资源需求清单
- 详细的联系人清单
- 表格和清单

典型的BCP架构和内容



阶段七、业务连续性流程及方案管理和测试

- ØBCM 演练
- ØBCM 维护
- ØBCM 评审

测试和演练的收益

Ø验证：

- 计划的适用性？
- 计划的完整性？
- 预期的时间内（RTO）能够完成恢复任务
- 员工充分了解
- 资源充分并安排合理
- 外部供应商有能力履行合同

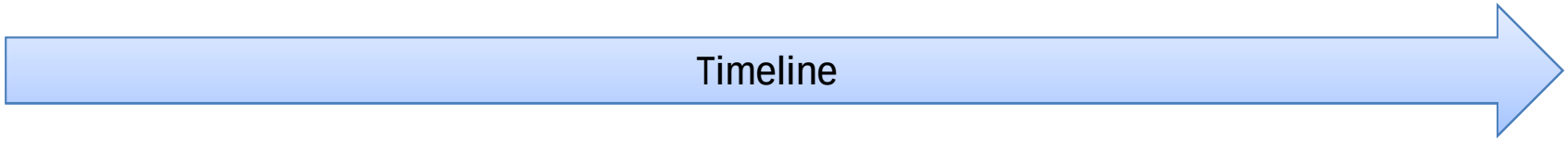
Ø熟练：

- 有效决策
- 减少混乱
- 缩短恢复时间
- 降低恢复成本

BCM的演练过程

遵循流程记录　　是否可达到预期

演练　　评价BCP



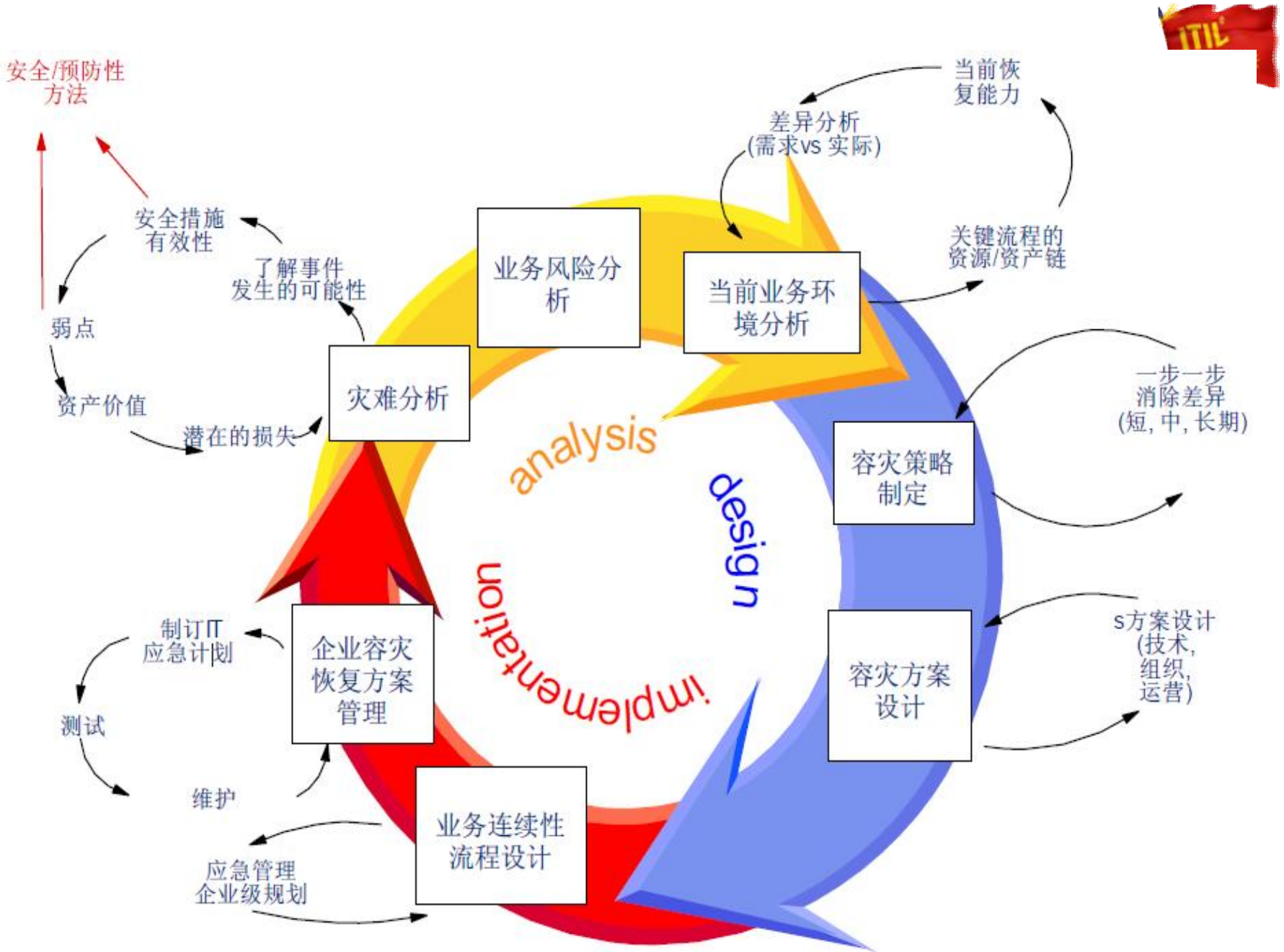
设计演练	协调演练	评价演练	持续改进
演练范围 后勤安排 状态检查	协调人员活动 协调各个部门 处理意外和变更	是否达到目标 研究各个部门的情况	简洁 成功与不足 BCP效果

BCM维护的内容

- 审查和更新BCM的范围，角色和职责
- 分配和更新合适人或团队负责BCM
- 通过演练确保BCM的有效性
- 在组织范围内强化BCM的意识
- 管理BCM演练过程
- 定期审查和更新业务持续性能力，包括风险分析和业务影响风险
- 维护和更新相关文档
- 监控组织的业务持续性能力并确定变更机制
- 维护与业务持续性相关的成本投入

BCM评审的内容

- BCM是否包含了所有确认的重要业务和活动
- BCM是否准确反映了组织目标（优先级和需求）
- BCM是否能有效的应对风险
- BCM是否被更新
- BCM的演练和维护程序是否被有效的执行
- 在演练中发现的问题是否被更新
- 组织是否有对BCM有持续的培训和奖励计划
- BCM程序是否给有效的告知员工
- 变更管理流程是否有效的被执行

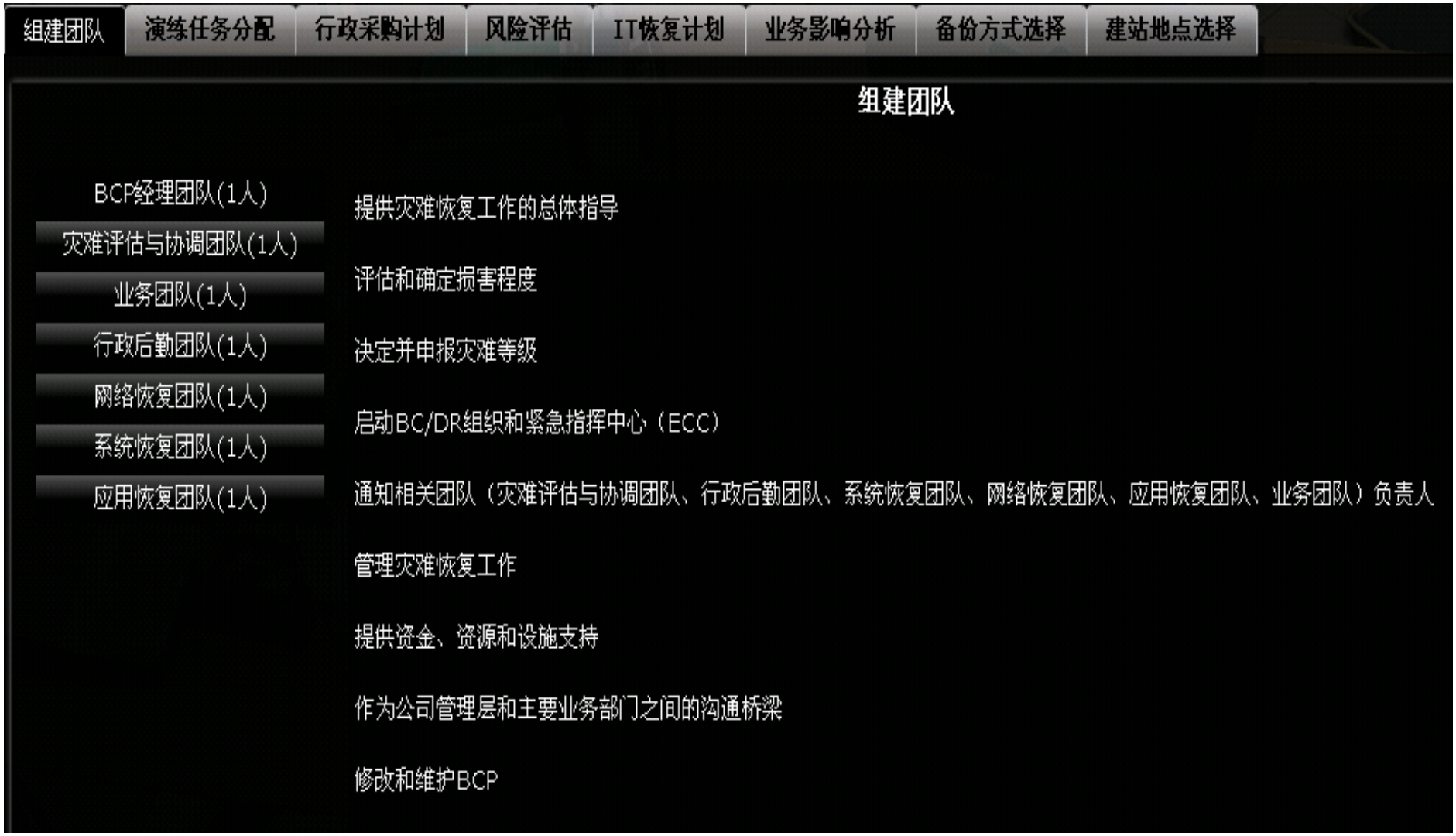

安全/预防性
方法
安全措施
有效性
了解事件
发生的可能性
弱点
资产价值
潜在的损失
业务风险分析
灾难分析
analysis
当前恢复能力
差异分析
(需求vs 实际)
当前业务环境分析
关键流程的
资源/资产链
一步一步
消除差异
(短, 中, 长期)
容灾策略
制定
design
S方案设计
(技术,
组织,
运营)
容灾方案
设计
implementation
制订IT
应急计划
企业容灾
恢复方案
管理
测试
维护
业务连续性
流程设计
应急管理
企业级规划

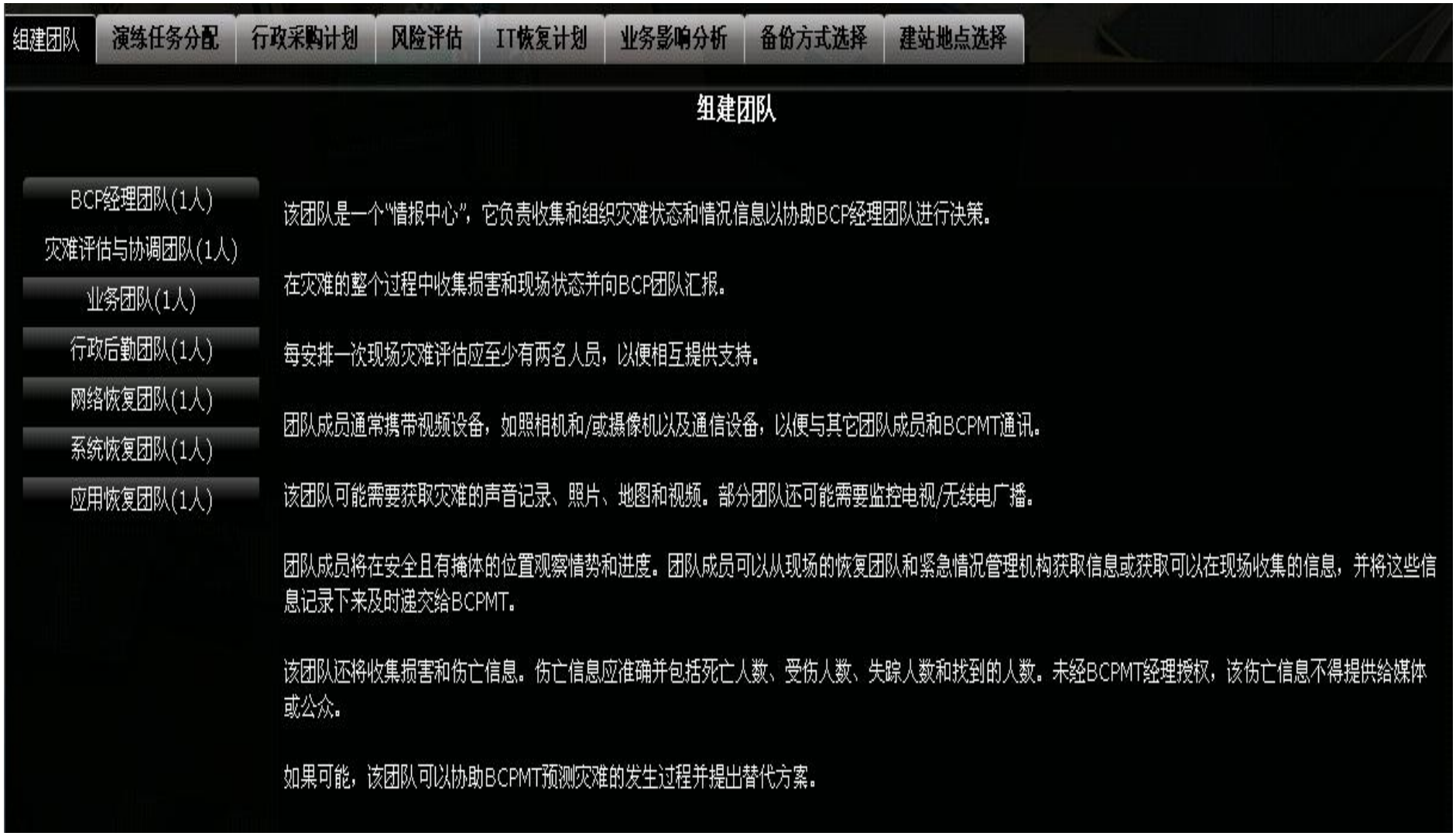
上海地铁追尾事故的反思

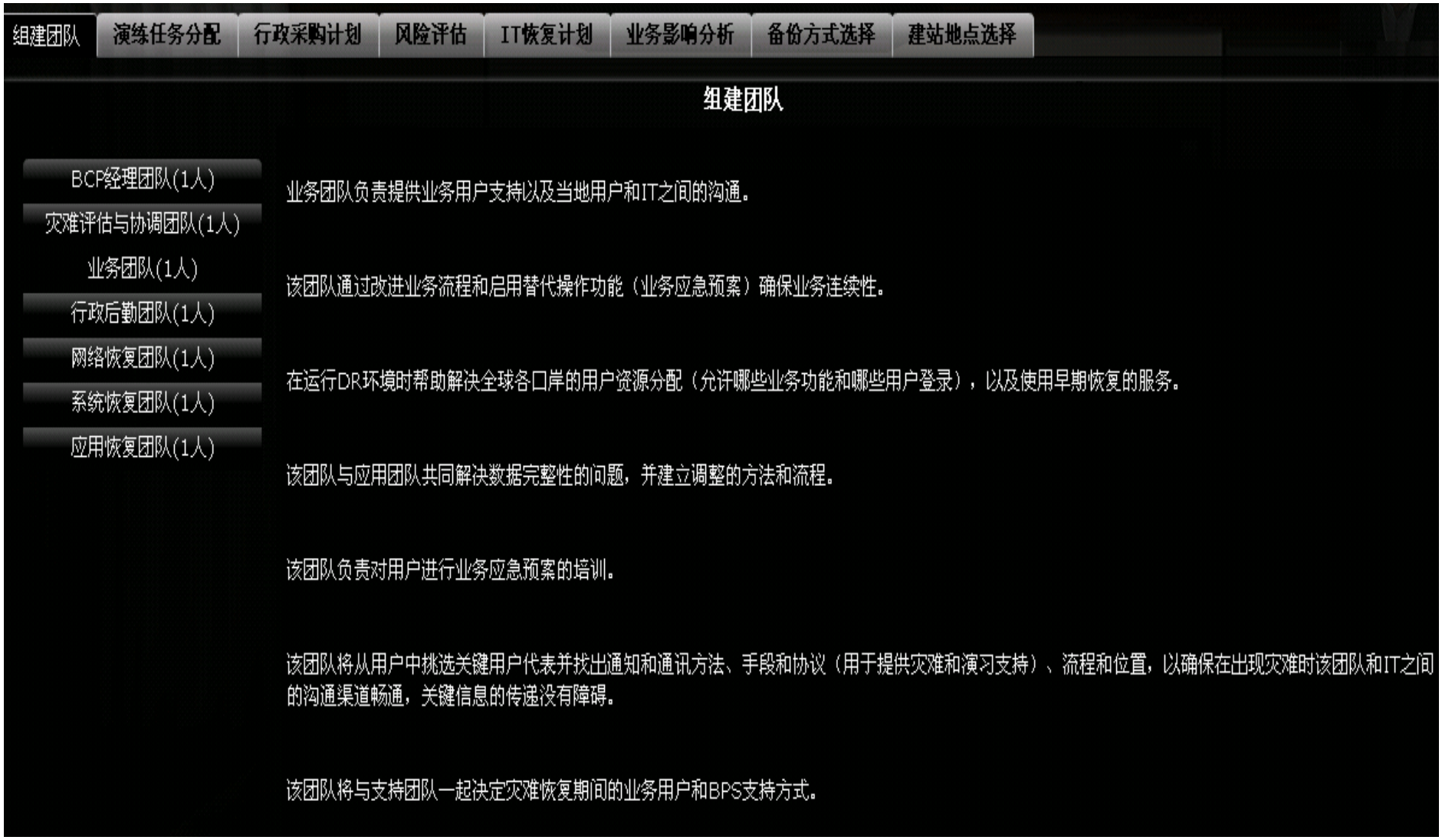
- 上海地铁10号线“9-27”追尾事故查明，当天设备突然失电，致使运营信号中断，地铁10号线行车作业人员即采取人工调度行车方式。
- 事故发生在信号系统故障后采用电话闭塞方法运行约40分钟后。
- 电话闭塞后两站间会分成多个闭塞分区，一般是一公里多一点；而闭塞分区中前后车之间将有红灯、黄灯、黄绿灯三个“不能驶入”的区间，等于是三保险。正常操作下行车应该是可以保证安全的。电话闭塞时两站间可能只允许一辆列车进入。

Agenda

- 业务连续性管理理论回顾
- 业务连续性管理的具体步骤
- 业务连续性演练方法介绍
- Q&A







组建团队 | 演练任务分配 | 行政采购计划 | 风险评估 | IT恢复计划 | 业务影响分析 | 备份方式选择 | 建站地点选择

组建团队

- BCP经理团队(1人)
- 灾难评估与协调团队(1人)
- 业务团队(1人)
- 行政后勤团队(1人)
- 网络恢复团队(1人)
- 系统恢复团队(1人)
- 应用恢复团队(1人)

后勤保障团队主要作为资源提供者向BCP团队和恢复团队提供支持。其工作包括供给、库存维护、后勤支持、设施建立、运输和存储安排、提交采购单。还包括对DR中心所需的文档和供应品预先储备，以确保在发生灾难时能够快速作出响应。

该团队还负责联系医疗救助，维护ECC、EWA，以及安排食宿等。

该团队还负责制定和执行非IT紧急情况（如火灾和断电，环境卫生）的响应方案并与当地相关机构联络。

需要时该团队可以利用各部门的资源为某一区域（如IT、财务和HR）提供支持。

在接到团队经理的通知后，该团队将开始建立ECC，为BCP团队成员的到来作好准备。

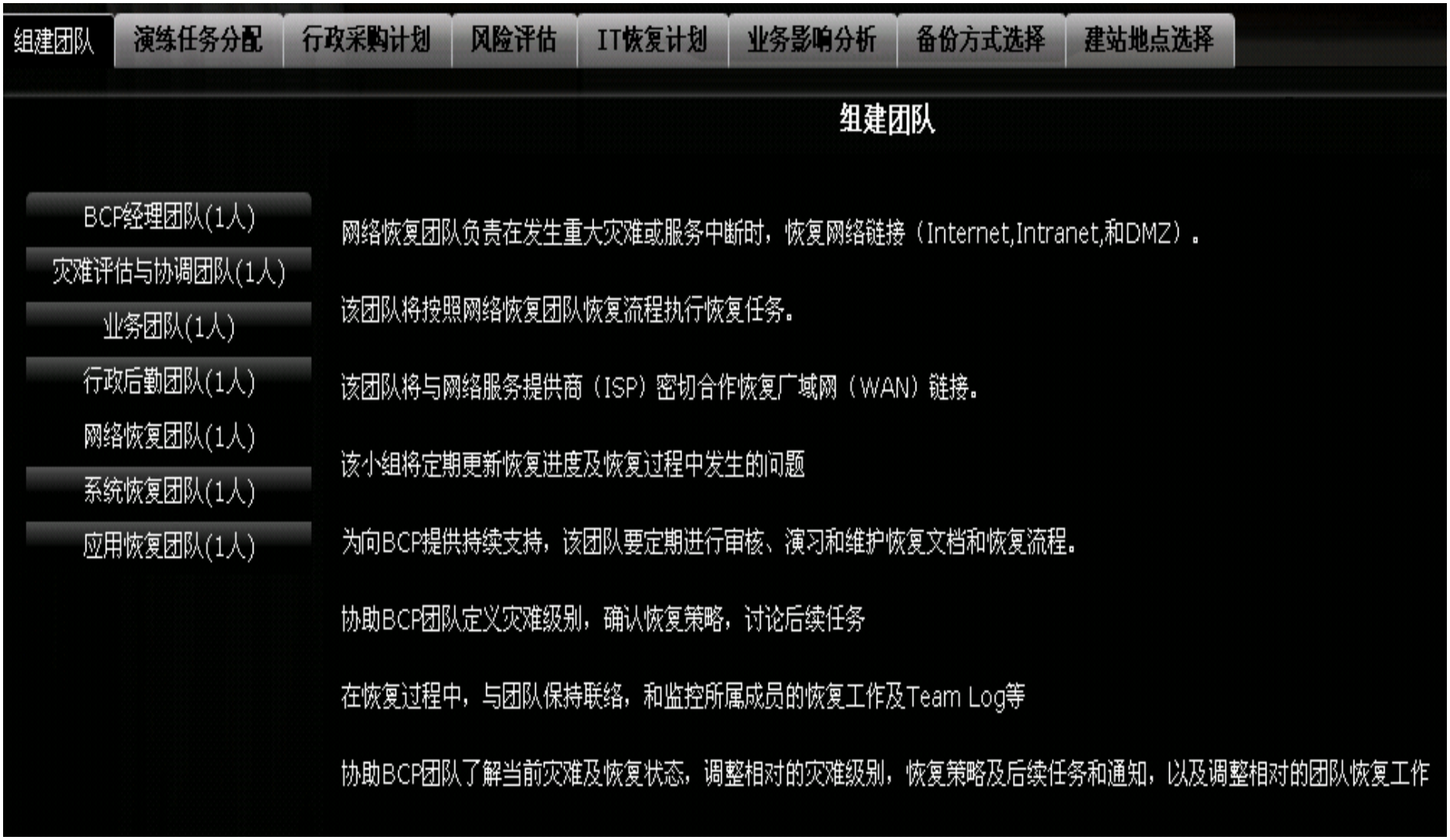
该团队将制定签到流程并设定标牌，以确保抵达的人员能够方便地找到签到位置。

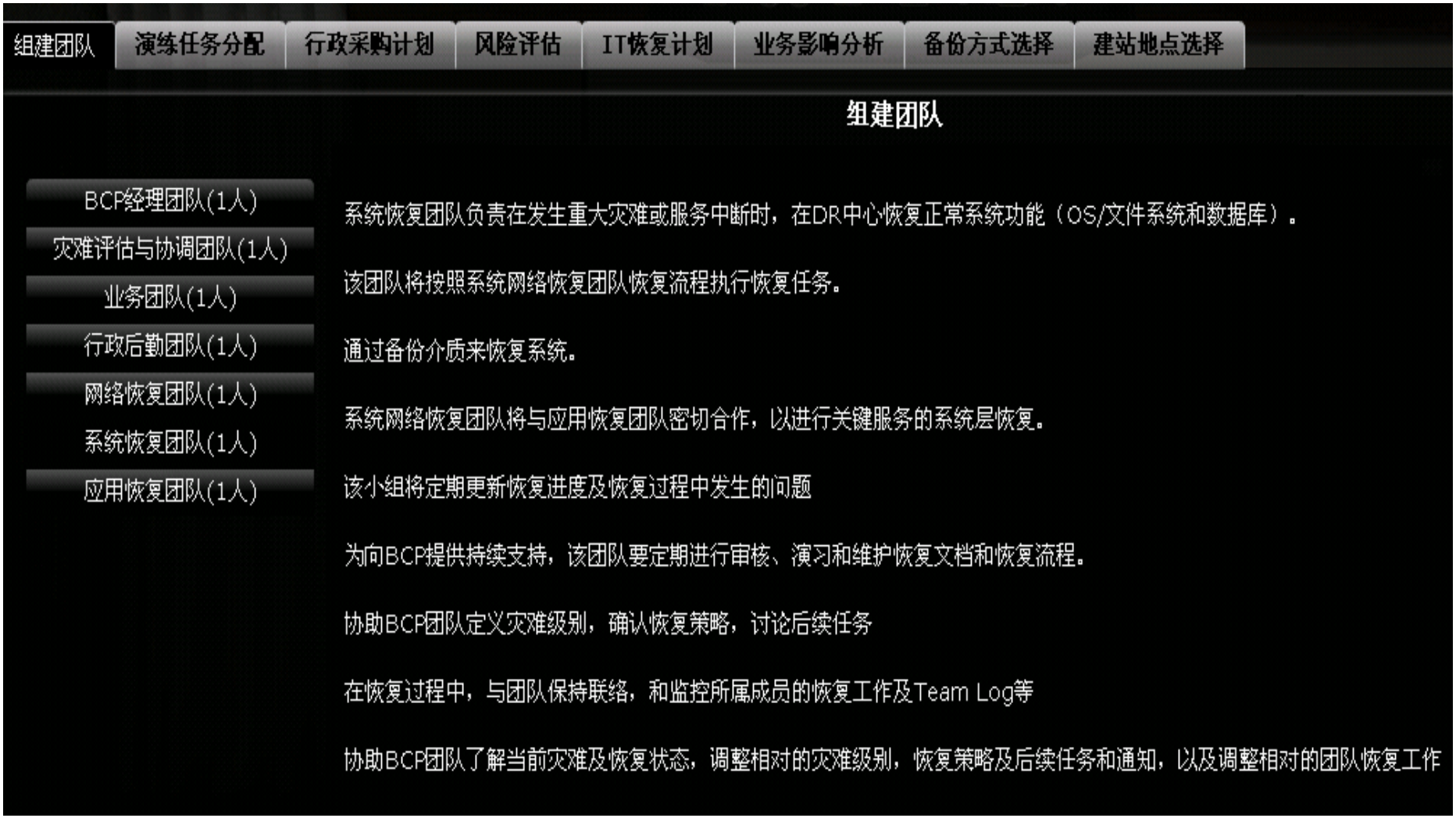
团队成员将在ECC中待命，以为BCP团队提供助理。

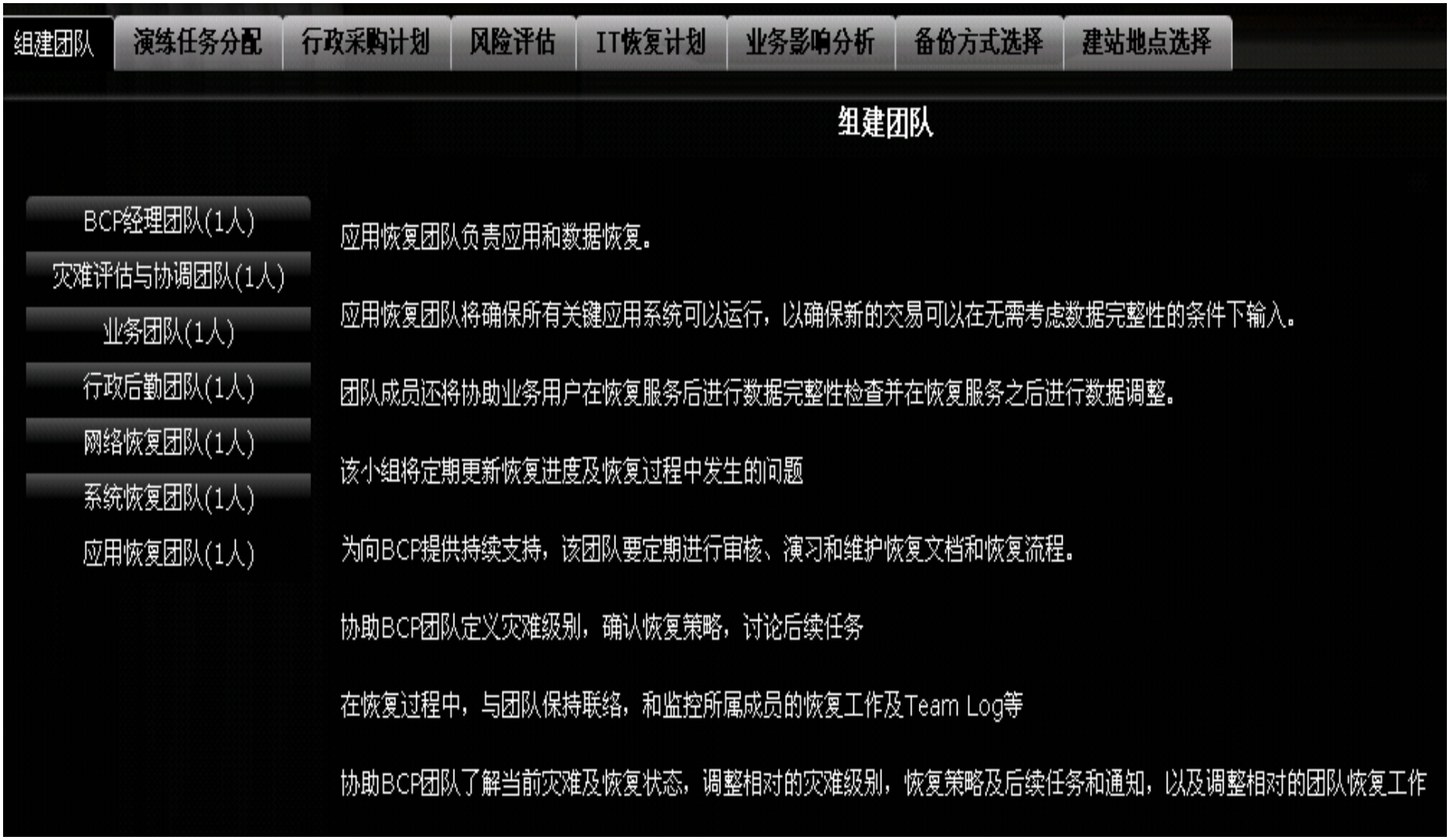
该团队与通讯部门联系，提供通讯设备并保证通讯畅通。

该团队负责从各种形式的灾难信息中摘录有关时间、消息和ECC启动期间所采取措施的信息。

该团队可以协调并处理额外资源（如急救服务，公用事业公司等）申请。







总结与回顾

- 中国每年有将近1亿人参加各种各样的培训，其中近80%的人参加的是工作技能等方面中、低层次的培训全球每年用于组织机构人员培训的费用高达上千亿美元，并且每年还以17%的速度递增，随着知识和技术的不断更新和发展，人们的接受新信息的方式也在发生着潜移默化的变化。
- HPE Simulation模拟系统将MMORPG的理念融入培训的课程中，我们能够让培训变成玩耍，通过丰富多彩的游戏体验让学员获得知识和技能，并留下更深刻的印象，真正达到融会贯通，学以至用

谢谢观赏

三人行，必有我师

ITIL先锋论坛，汇聚IT服务管理大师们的力量