身为挨踢达人

ITIL ITSM IT服务管理 IT运维 Prince2 ISO20000 IT规划 BCM ISO27001 CISA PMP ITSS

唯自我增值与免费，不能辜负

- YY频道89519382
- 每周四晚上八点半
- ITIL先锋论坛网络讲堂
- 与专家们高峰对话！

扫一扫，从此不再错过

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

如何获取每周专家讲堂信息？告诉你！

关注微信ITILXF_（注意有下划线哦)或者登录www.itilxf.com找社区服务

错过了讲堂怎么办？来这里听录音吧！

http://www.itilxf.com/thread-32695-1-1.html

想学习哪些IT管理知识？告诉我们吧！

http://www.itilxf.com/thread-33143-1-1.html

如何才能上专家讲堂？如何进行合作？

http://www.itilxf.com/thread-33143-1-1.html

专家讲堂由谁主办，来自哪里，看这里！

ITIL先锋论坛是国内最大的IT服务管理专业社区，自2010年底成立以来始终致力于以ITIL为代表的信息技术科学方法论在国内的推广与落地，目前已发展论坛会员已跃20000人，16000多微博粉丝，8000多名QQ群友，60000多条帖子，10000多分可供下载的管理及实践资料。ITIL先锋论坛在各位版主及广大网友的共同努力下，将继续为IT服务管理初学者提供入门的引领，为IT服务管理实践者提供落地的支撑，为IT服务管理业界提供沟通交流的平台。

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

《灾备项目落地》

录音下载地址：http://www.itilxf.com/thread-35921-1-1.html

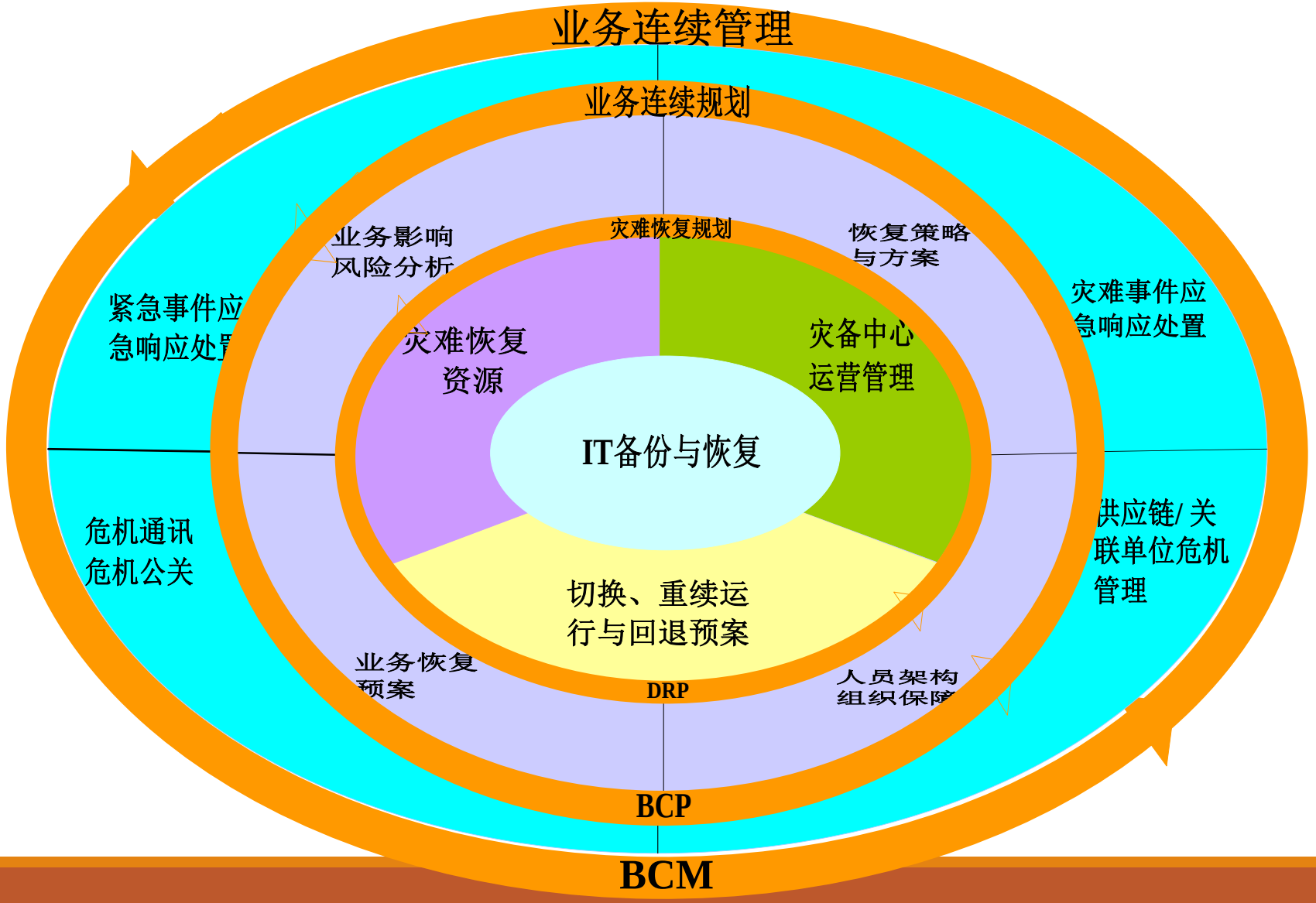
灾备项目DRP落地

唐龙

总体安排

10	业务连续性管理体系
20	灾难恢复预案设计
15	灾难恢复预案主要内容
15	案例共享

业务连续性管理体系


业务连续管理
业务连续规划
灾难恢复规划
业务影响
风险分析
恢复策略
与方案
紧急事件应
急响应处置
灾难恢复
资源
灾备中心
运营管理
灾难事件应
急响应处置
IT备份与恢复
危机通讯
危机公关
供应链/ 关
联单位危机
管理
切换、重续运
行与回退预案
业务恢复
预案
DRP
人员架构
组织保障
BCP
BCM

灾备体系建设

灾难备份
系统持续
运营管理

- 灾难恢复策略建议
- 制订灾难恢复预案
- 灾难恢复演练
- 专业培训

灾备场
地和基
础设施

灾难备份中心技术实现

术语定义

灾难 Disaster

- 由于人为或自然的原因，造成信息系统严重故障、瘫痪或其数据严重受损，使信息系统支持的业务功能停顿或服务水平达到不可接受的程度，并持续**特定时间**的突发性事件。通常导致信息系统需要**切换到灾难备份中心**运行。

灾难恢复 Disaster Recovery

- 为了将信息系统从灾难造成的不可运行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**。

灾难恢复规划（DRP） Disaster Recovery Planning

- 为了规避灾难带来的损失和保证**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所做的**事前计划和安排**。

术语定义

灾难备份中心；备用场所 Alternate Site

■ 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、备用的基础设施和专业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。

灾难备份 backup for disaster recovery

■ 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。

灾难恢复预案 Disaster Recovery Plan

■ 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。

总体安排

10	业务连续性管理体系
20	灾难恢复预案设计
15	灾难恢复预案主要内容
15	案例共享

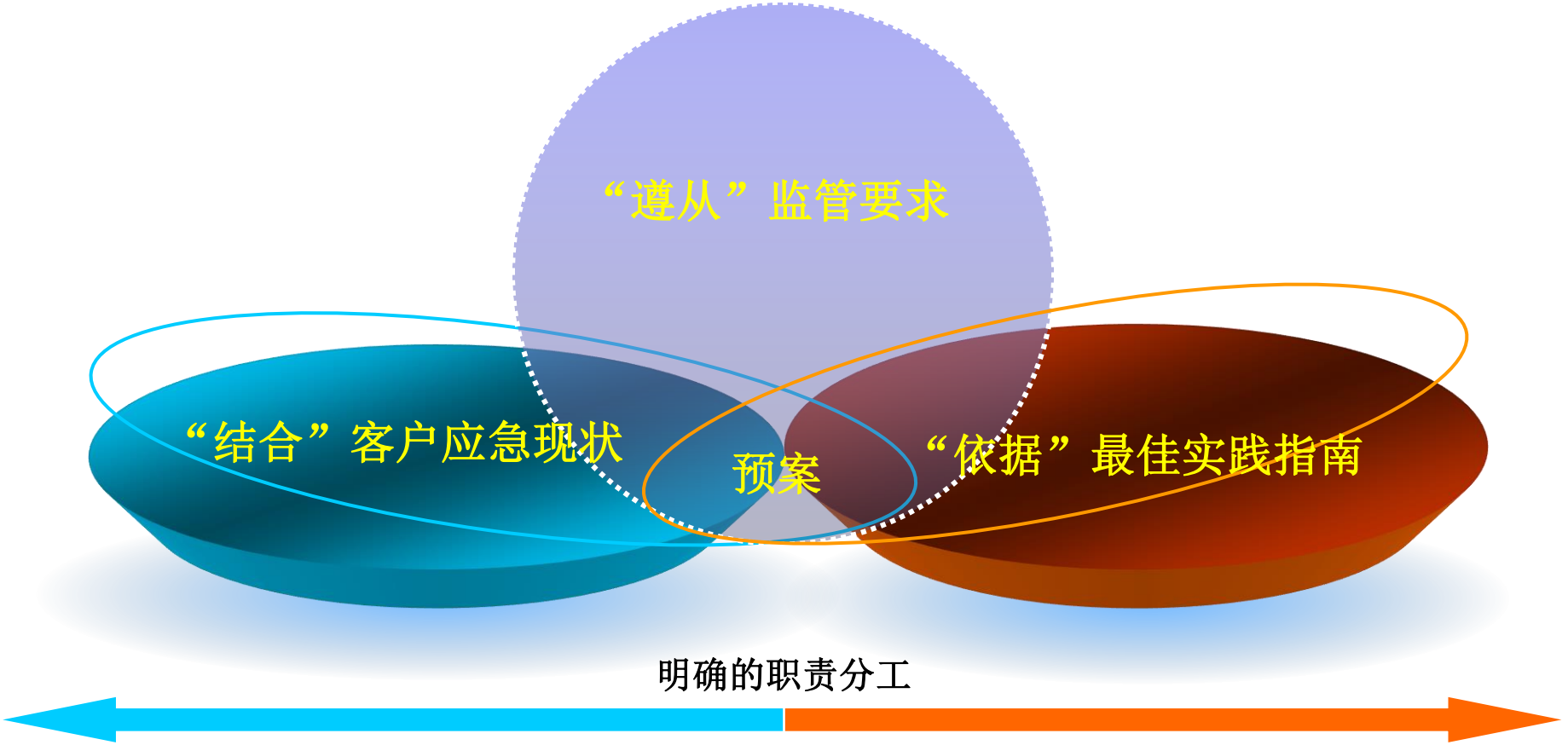
预案类别

计划名称	目标	范围
业务连续性预案	提供重大中断恢复期间维持重要业务运行的规程。	涉及到业务处理，和IT相关的仅限于其对业务处理的支持。
灾难恢复预案	提供在灾备中心促进恢复能力的详尽规程。	通常聚焦于IT问题。
业务恢复预案	提供灾难后立即恢复业务运行的规程。	涉及到业务处理；不聚焦于IT问题；和IT相关的仅限于其对业务处理的支持。
紧急/灾难事件应急响应流程	提供为应对物理威胁、减少生命损失或伤害以及保护财产免遭损失的协调性规程。	聚焦于特定设施中的人员和财产；不基于业务处理或IT系统功能。
危机通信和公关计划	提供向个人和公众散发状态报告的规程。	涉及到与个人和公众的通信；不聚焦于IT问题。

预案制定的原则

一致性	• 各层应急响应预案之间应协调一致，相互兼容
有效性	• 预案应尽可能满足应急实际需要，并保持定期测试和更新
易用性	• 预案应运用易于理解语言和图表，并适合在紧急情况下使用
完整性	• 预案应包含应急响应和恢复全过程，以及全部所需数据和资料
明确性	• 预案应采用清晰结构，所需资源、工作内容和步骤应具体明确

灾难恢复预案的依据



信息系统灾难恢复规范

附录B 灾难恢复预案框架

信息系统
灾难恢复规范

要点提炼

B.1 目标和范围

B.2 组织和职责

B.3 联络与通讯

B.4 突发事件响应流程

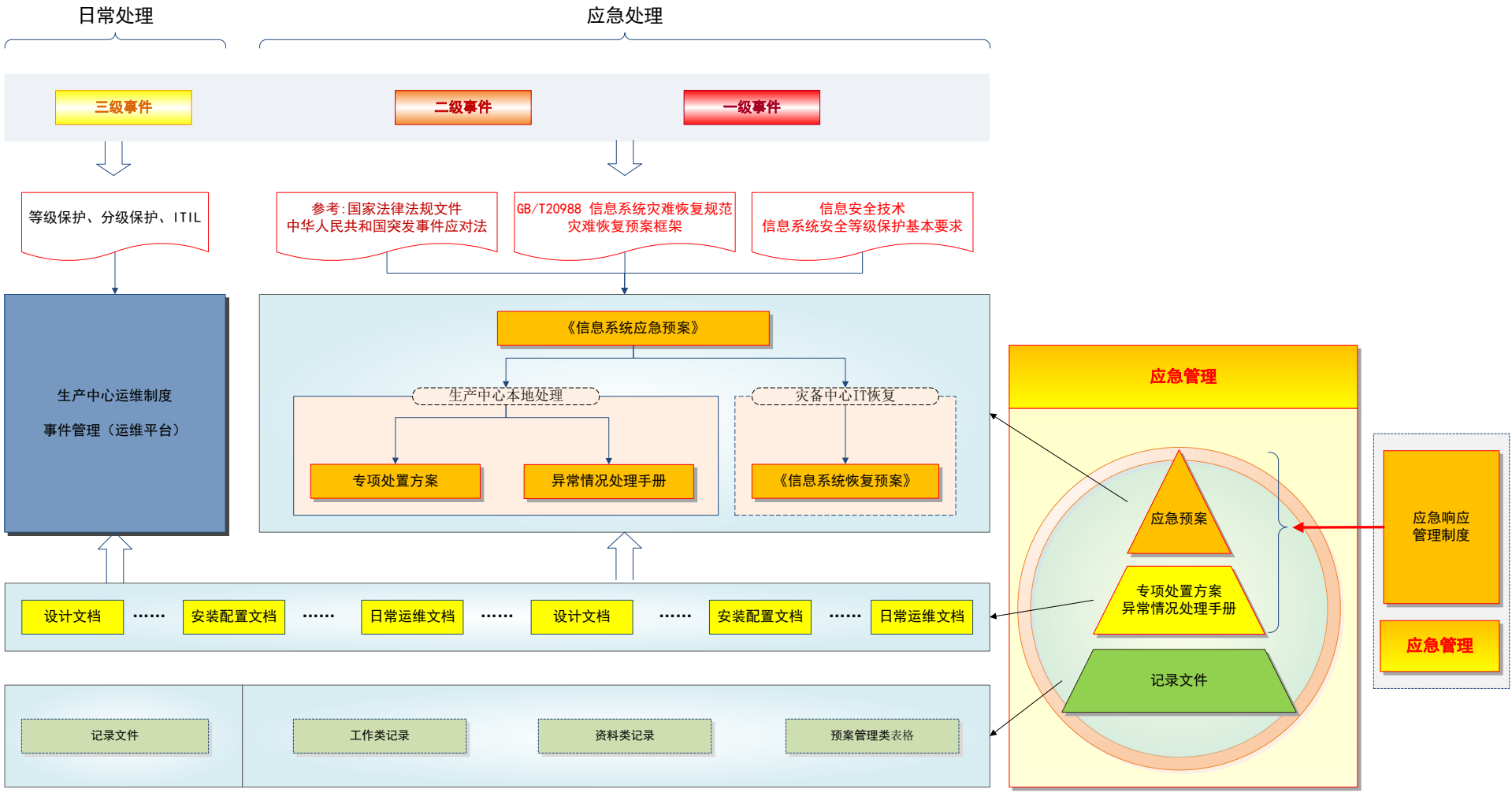
B.5 恢复及重续运行流程

B.6 灾后重建和回退

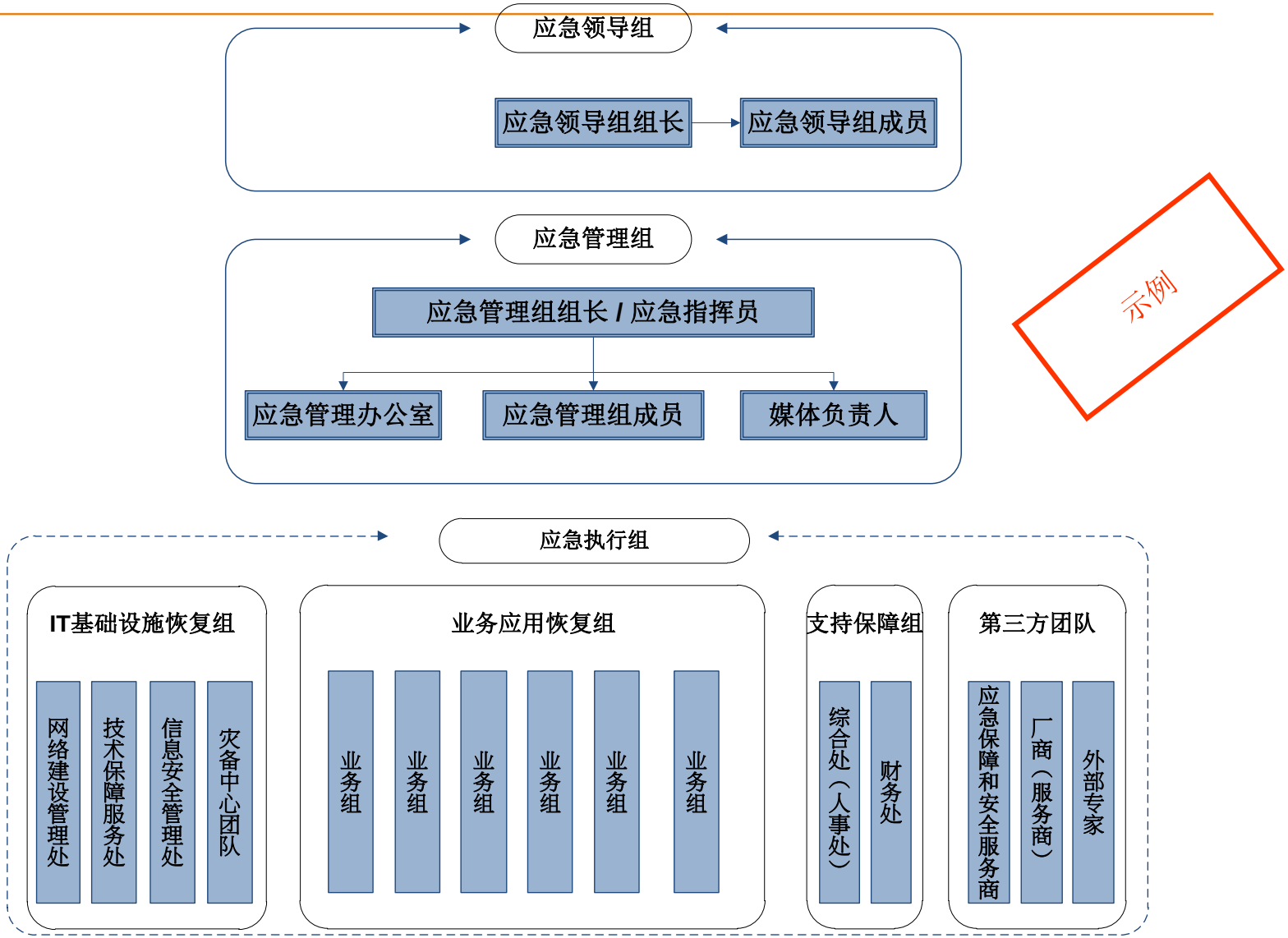
B.7 预案的保障条件

B.8 预案附录

预案整体架构设计

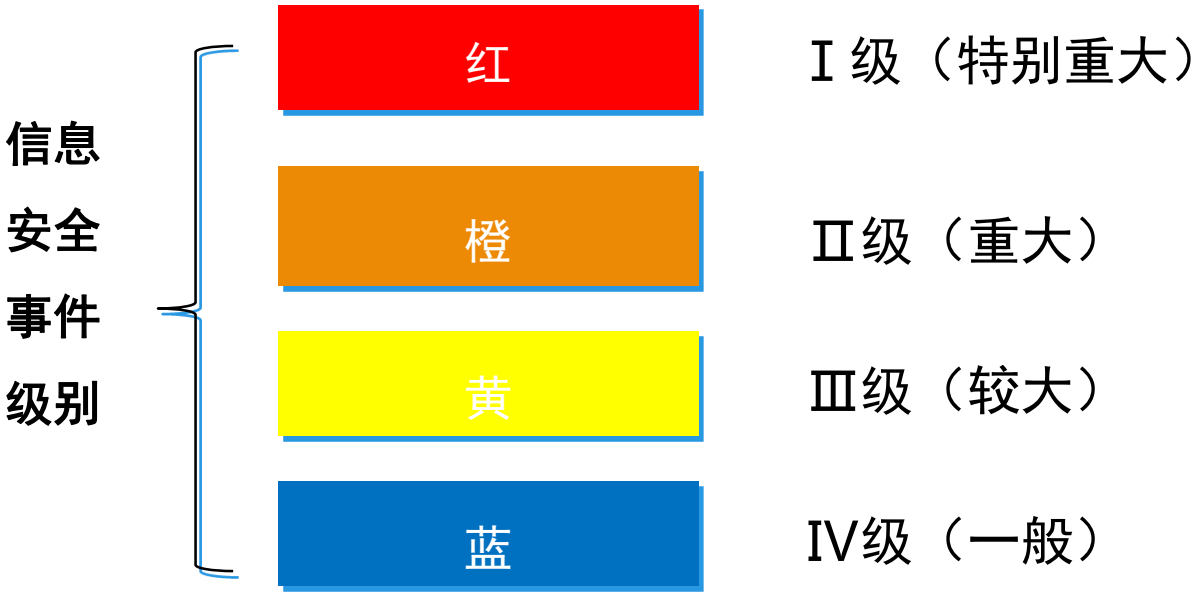

日常处理
应急处理
三级事件
二级事件
一级事件
等级保护、分级保护、ITIL
参考:国家法律法规文件
中华人民共和国突发事件应对法
GB/T20988 信息系统灾难恢复规范
灾难恢复预案框架
信息安全技术
信息系统安全等级保护基本要求
生产中心运维制度
事件管理（运维平台）
《信息系统应急预案》
生产中心本地处理
灾备中心IT恢复
专项处置方案
异常情况处理手册
《信息系统恢复预案》
应急管理
应急预案
专项处置方案
异常情况处理手册
记录文件
应急响应
管理制度
应急管理
设计文档
安装配置文档
日常运维文档
设计文档
安装配置文档
日常运维文档
记录文件
工作类记录
资料类记录
预案管理类表格

应急组织架构设计

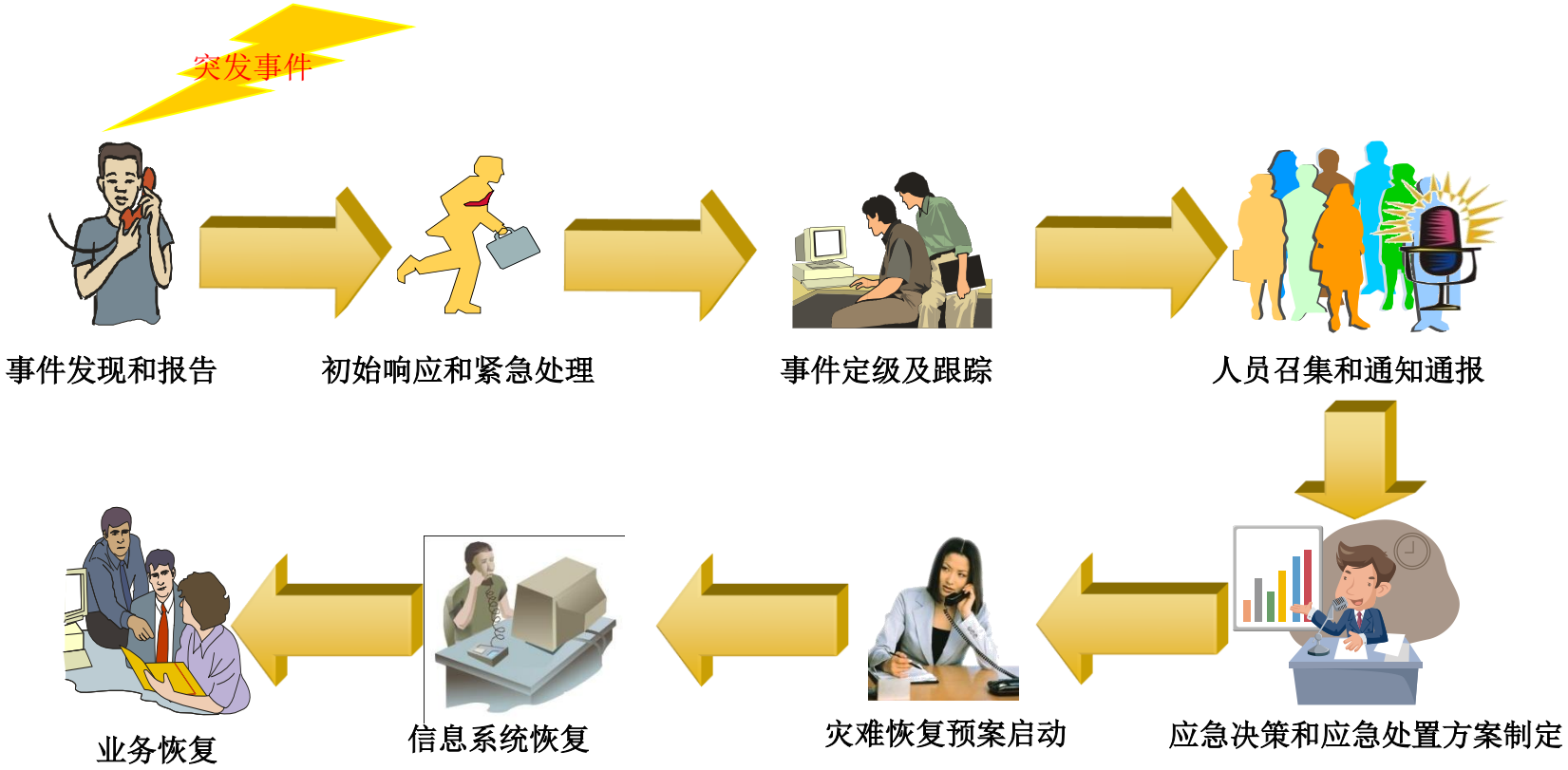

应急领导组
应急领导组组长
应急领导组成员
应急管理组
应急管理组组长 / 应急指挥员
应急管理办公室
应急管理组成员
媒体负责人
示例
应急执行组
IT基础设施恢复组
网络建设管理处
技术保障服务处
信息安全管理处
灾备中心团队
业务应用恢复组
业务组
业务组
业务组
业务组
业务组
业务组
支持保障组
综合处（人事处）
财务处
第三方团队
应急保障和安全服务商
厂商（服务商）
外部专家

突发事件分级

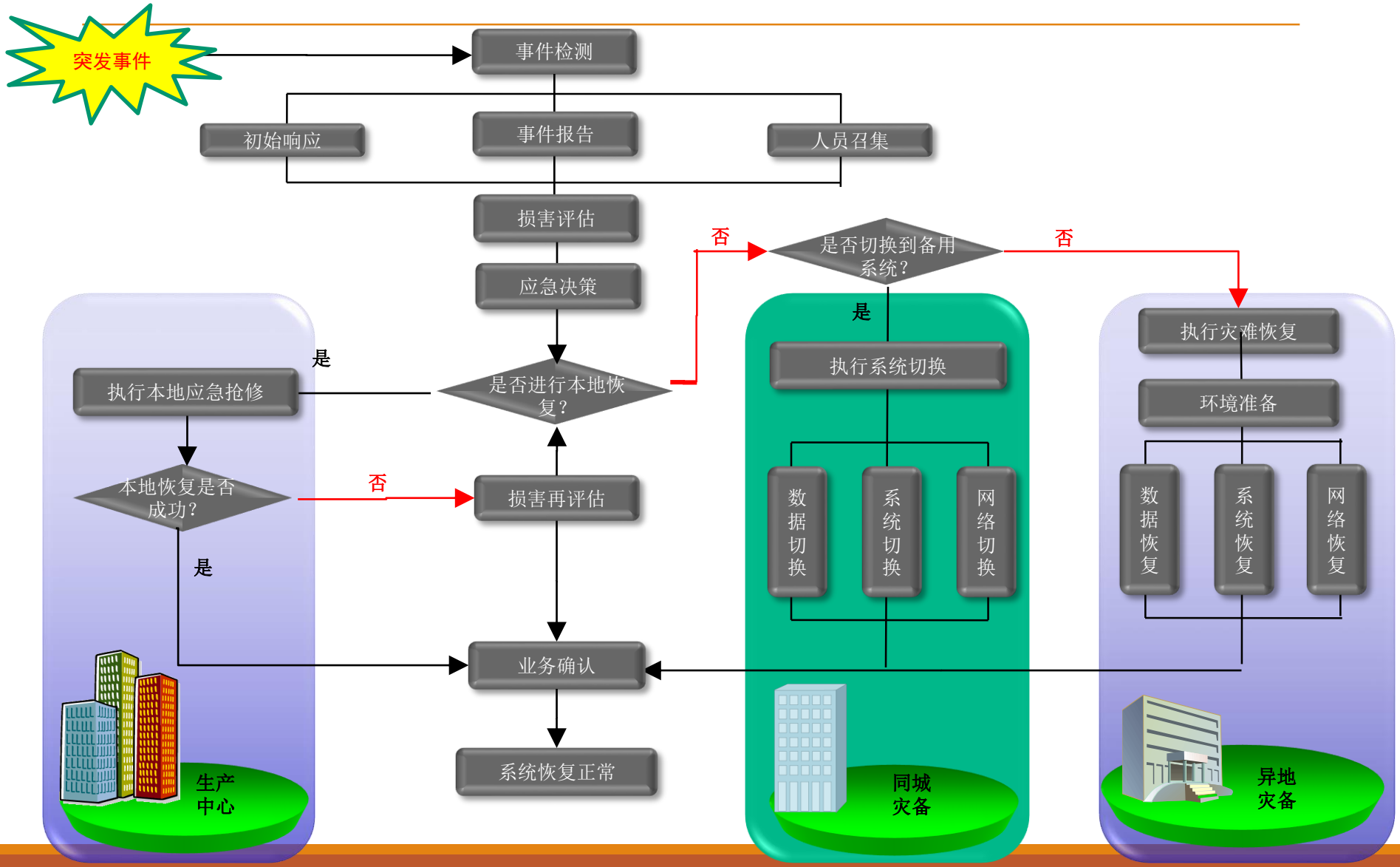
按照事件性质、严重程度、可控性和影响范围等因素，可将事件分为不同的级别，根据事件级别进行分级响应



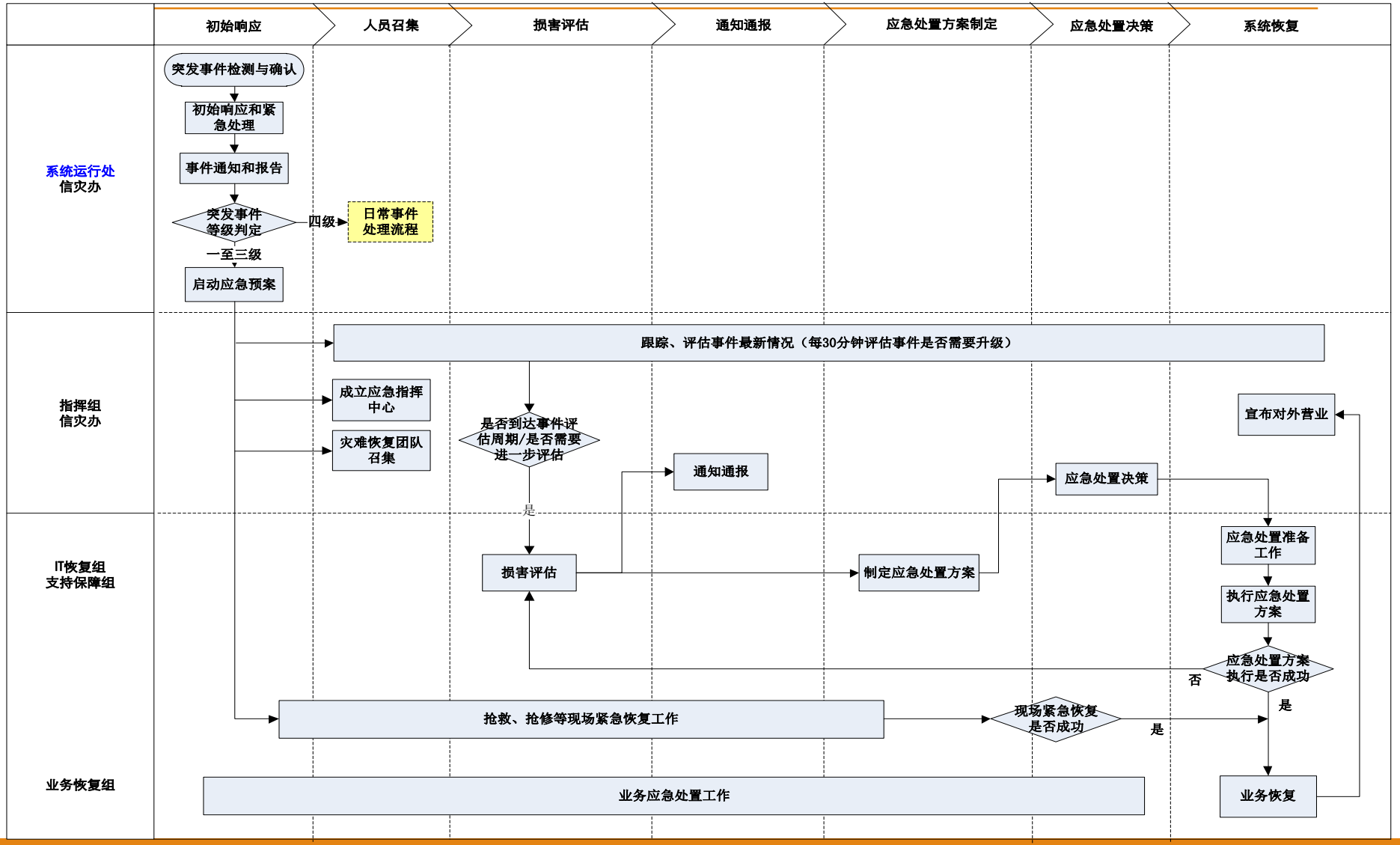
应急响应和灾难恢复流程设计



应急响应和灾难恢复流程设计



应急响应和灾难恢复流程设计



灾难恢复系统技术方案设计

总体安排

10	业务连续性管理体系
20	灾难恢复预案设计
15	灾难恢复预案主要内容
15	案例共享

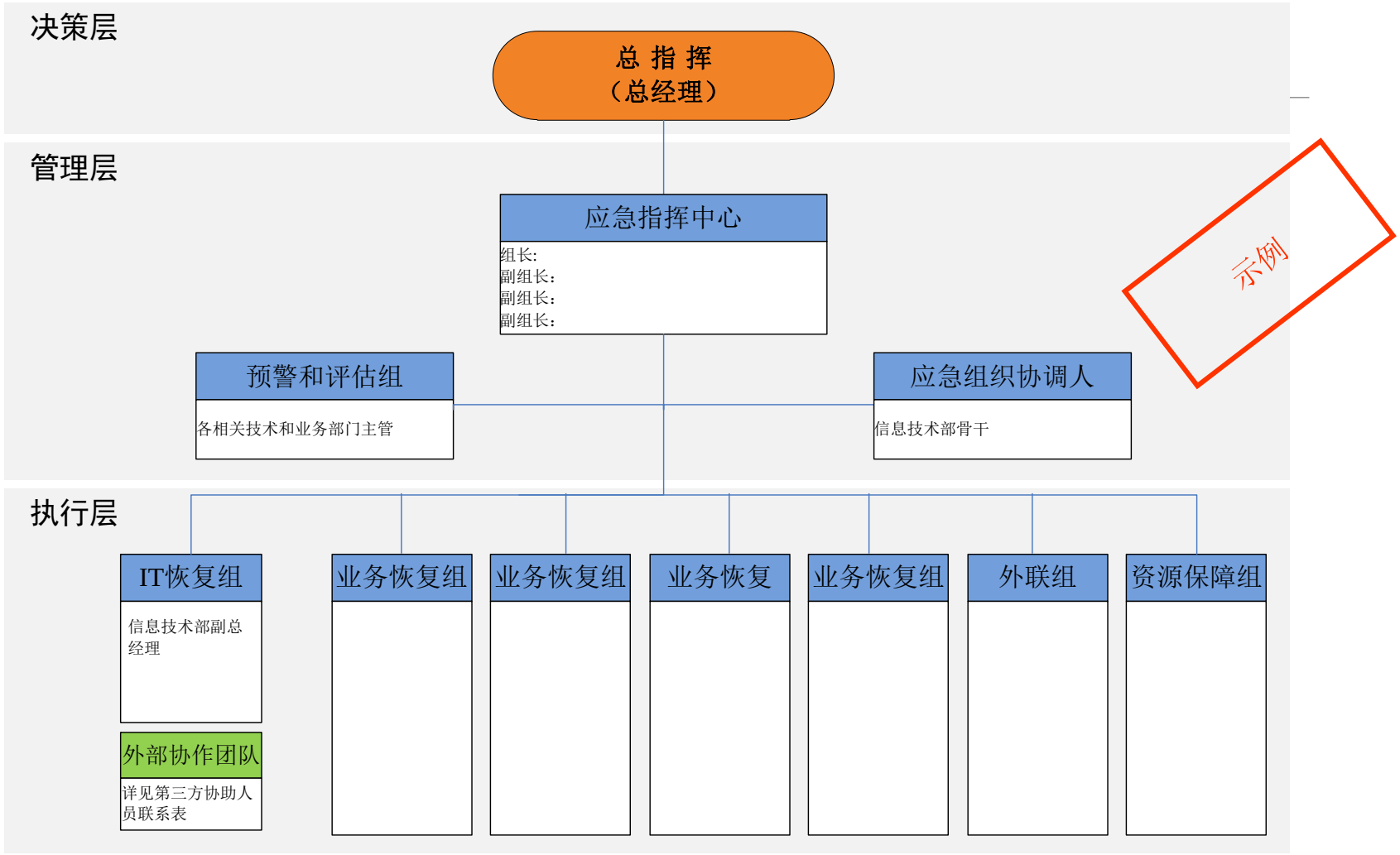
灾难恢复预案内容提要

应急管理组织	• 如何建立激活式组织，详细描述角色和职责 • 灾难应急管理组织体系包括：决策层，管理层和执行层
应急管理通讯	• 关注跨部门的合作，建立统一的应急联动机制。定义通知的方式、规则
灾难恢复策略	• 确定恢复范围和目标，制定恢复等级和执行方式
应急响应和灾难恢复流程	• 以应急管理组织为视角，工作阶段为导向描述流程
技术切换和回切规程	• 描述信息系统生产中心切换至灾备中心的操作步骤及在灾备中心回切的操作步骤
灾备中心重续运行	• 描述资源保障和人员保障计划等
重建和回退	• 说明重建及回退的目标、组织方式、工作流程

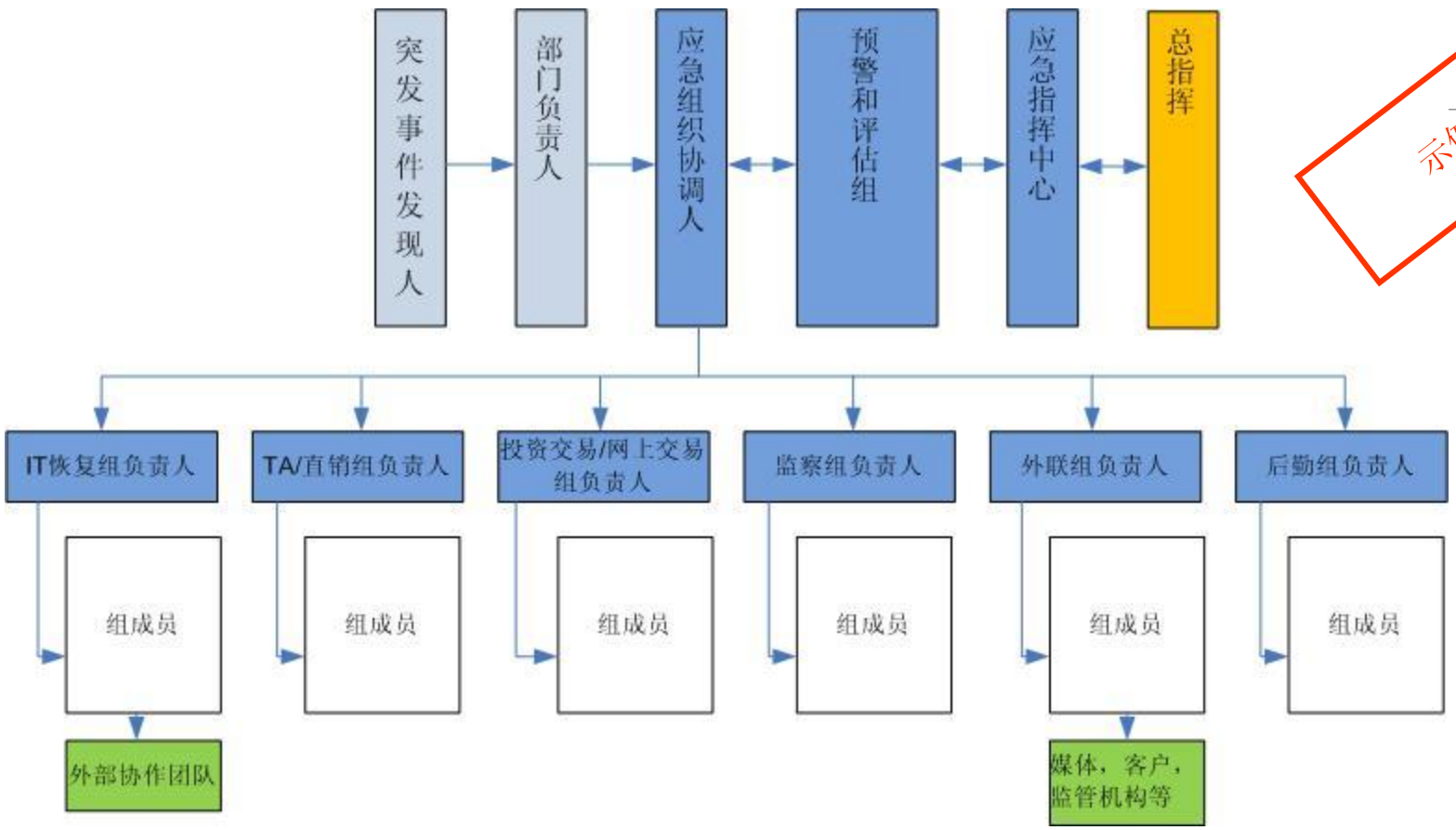
灾难恢复场景定义

灾备中心可恢复	局部电力故障、局部通讯故障
	设备故障、数据库系统故障、操作系统故障
	人为操作失误、人为蓄意破坏、黑客、病毒、生产中心机房场所倒塌、盗抢、鼠害、爆炸、恐怖袭击
不宜启用灾备中心恢复	对数据中心主机房场地不造成破坏，只造成生产系统短时间不能运行或系统资源不能被访问
	在短时间内可以由本地恢复的灾难，如计算机主机设备、网络通讯设备、供电设备的某一部件损坏。
	由应用软件错误造成的系统中断。
同城灾备中心无法恢复	本地区或数据中心和容灾备份系统同时遭受的全局性灾难

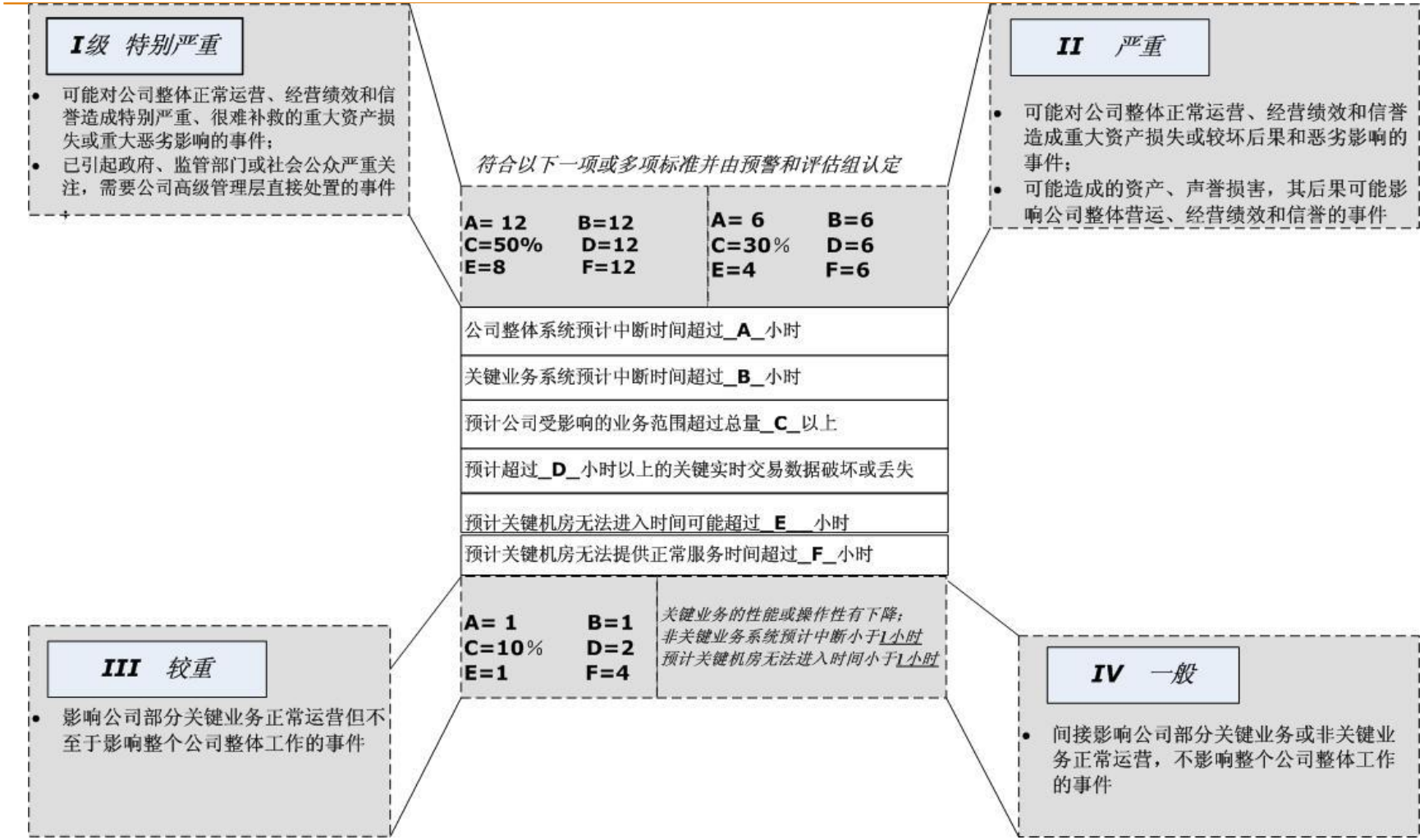
灾难恢复组织架构


决策层
总 指 挥
（总经理）
管理层
应急指挥中心
组长:
副组长：
副组长：
副组长：
预警和评估组
各相关技术和业务部门主管
应急组织协调人
信息技术部骨干
示例
执行层
IT恢复组
信息技术部副总经理
外部协作团队
详见第三方协助人员联系表
业务恢复组
业务恢复组
业务恢复
业务恢复组
外联组
资源保障组

应急管理通讯


突发事件发现人
部门负责人
应急组织协调人
预警和评估组
应急指挥中心
总指挥
示例
IT恢复组负责人
TA/直销组负责人
投资交易/网上交易组负责人
监察组负责人
外联组负责人
后勤组负责人
组成员
组成员
组成员
组成员
组成员
组成员
外部协作团队
媒体，客户，监管机构等

灾难恢复策略-突发事件等级



灾难恢复策略-执行方式

立即恢复

- 如果现场情况显示明显无法在短期内完成本地恢复，直接进行灾难宣告，启动灾难备份中心。

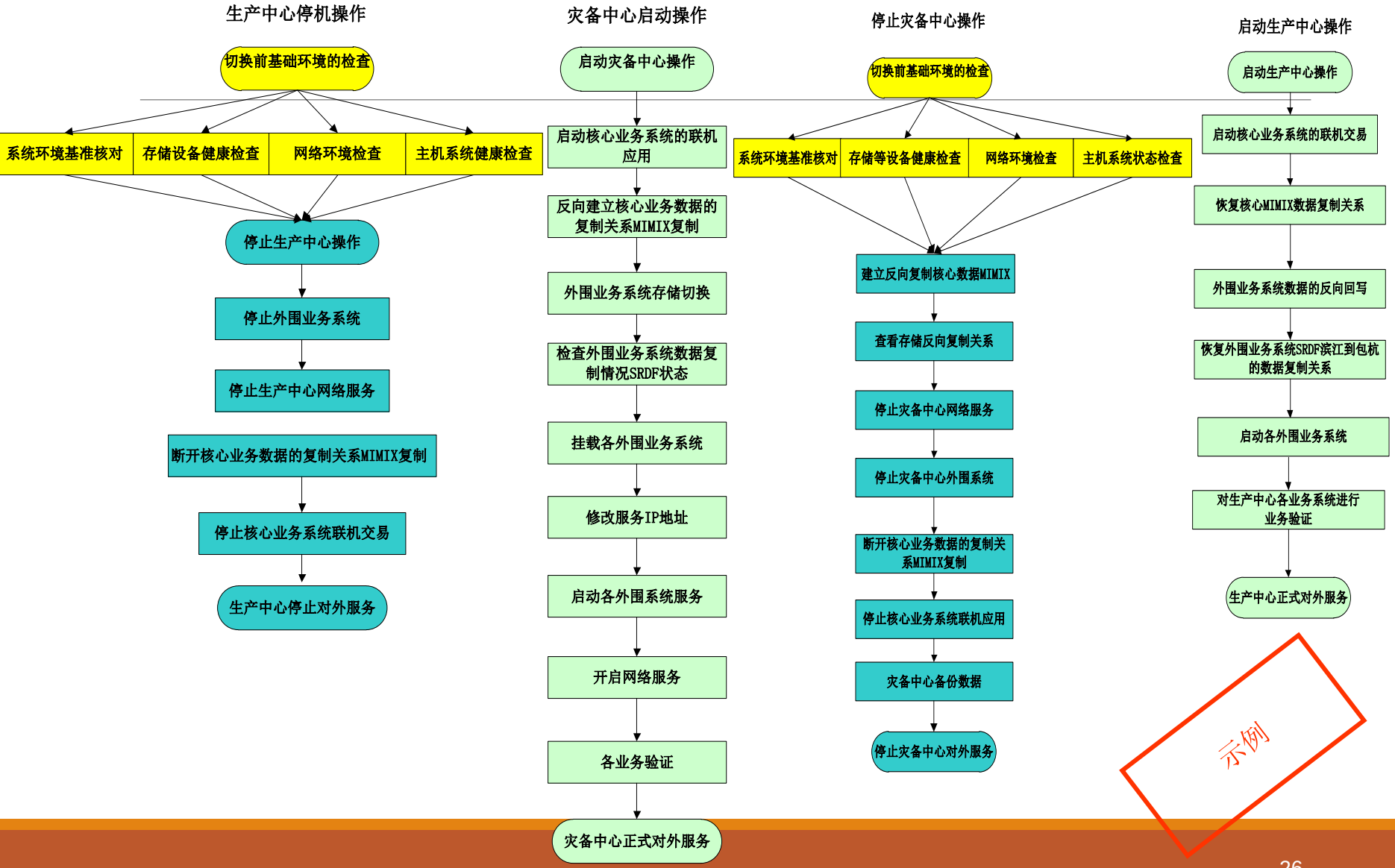
评估后恢复

- 如果现场情况不够明朗，无法马上判断是否能够及时完成本地恢复，则等待评估结论和现场抢修的结果，直到状况明确后，根据具体情况判断是否进行灾难宣告。

强制恢复

- 如果在灾难预警后一定时间内，在到达强制决策时间点后仍然无法给出明确的评估结论，可以强制启用灾备中心恢复。

技术切换和回切流程


生产中心停机操作
切换前基础环境的检查
系统环境基准核对
存储设备健康检查
网络环境检查
主机系统健康检查
停止生产中心操作
停止外围业务系统
停止生产中心网络服务
断开核心业务数据的复制关系MIMIX复制
停止核心业务系统联机交易
生产中心停止对外服务
灾备中心启动操作
启动灾备中心操作
启动核心业务系统的联机应用
反向建立核心业务数据的复制关系MIMIX复制
外围业务系统存储切换
检查外围业务系统数据复制情况SRDF状态
挂载各外围业务系统
修改服务IP地址
启动各外围系统服务
开启网络服务
各业务验证
灾备中心正式对外服务
停止灾备中心操作
切换前基础环境的检查
系统环境基准核对
存储等设备健康检查
网络环境检查
主机系统状态检查
建立反向复制核心数据MIMIX
查看存储反向复制关系
停止灾备中心网络服务
停止灾备中心外围系统
断开核心业务数据的复制关系MIMIX复制
停止核心业务系统联机应用
灾备中心备份数据
停止灾备中心对外服务
启动生产中心操作
启动生产中心操作
启动核心业务系统的联机交易
恢复核心MIMIX数据复制关系
外围业务系统数据的反向回写
恢复外围业务系统SRDF滨江到包杭的数据复制关系
启动各外围业务系统
对生产中心各业务系统进行业务验证
生产中心正式对外服务
示例

灾备中心重续运行

在系统对外宣告正式提供服务后，还应制定持续运行计划，包括人员保证计划、物资保证计划等，保证在规定的时间内灾备中心持续的提供信息系统服务。

为了确保系统正常运行，至少包括但不限于以下方面的考虑：

- **办公场地变更**

  例如原业务办公场地可能没有和灾备中心的网络连接，有些业务操作员有可能需要临时调配到灾备中心进行办公，应当考虑在灾备中心提供一定的办公场地

- **人员保障制度**

  灾备中心接管运行后，需要配备必须的生产中心的技术和运维人员。

- **日常运维制度变更**

  例如备份磁带的传递，原来是定时从生产中心运输到灾备中心，现在需要从灾备中心运输到另外的保存地点。

- **降低服务水平**

  如果灾备中心需要长时间运行，但由于灾备中心并不能提供和生产中心同等的服务水平（例如主机处理能力、存储的性能和大小、网络带宽等等），需要有策略地降低部分业务的服务水平、选择性地关闭某些相对不重要的外围服务

重建和回退

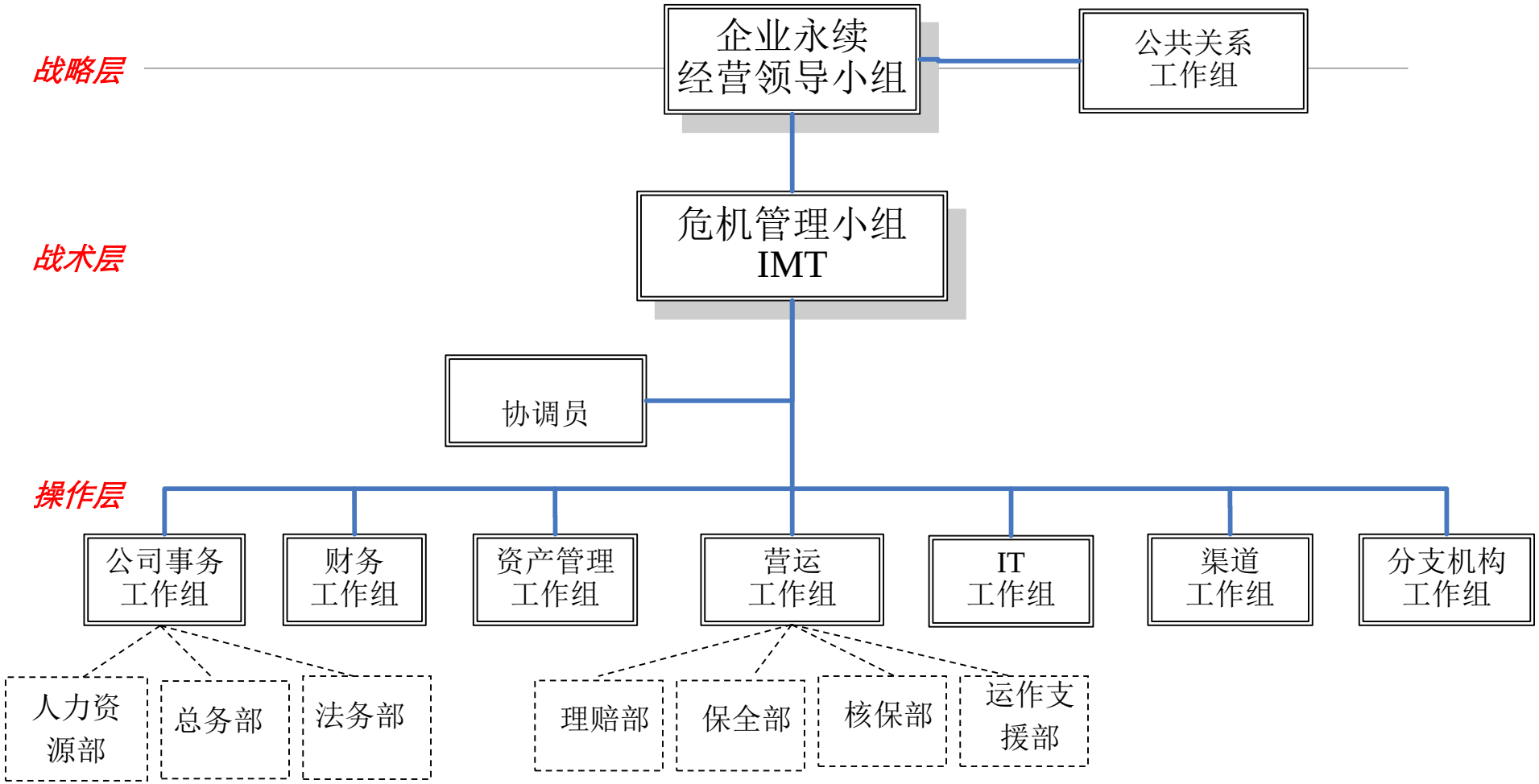
生产系统的回退是指将灾备份系统的功能转移到新建或恢复的生产系统，各项业务恢复到正常运行状态的过程，内容包括：

- 重建系统的测试；
- 系统的回退切换；
- 数据的回退切换，检查系统中的备份数据；
- 网络的回退切换；
- 业务功能的切换；
- 相关数据安全处理，防止重要信息的泄漏；
- 灾难备份系统恢复为备用状态；
- 人员和重要设备撤离。

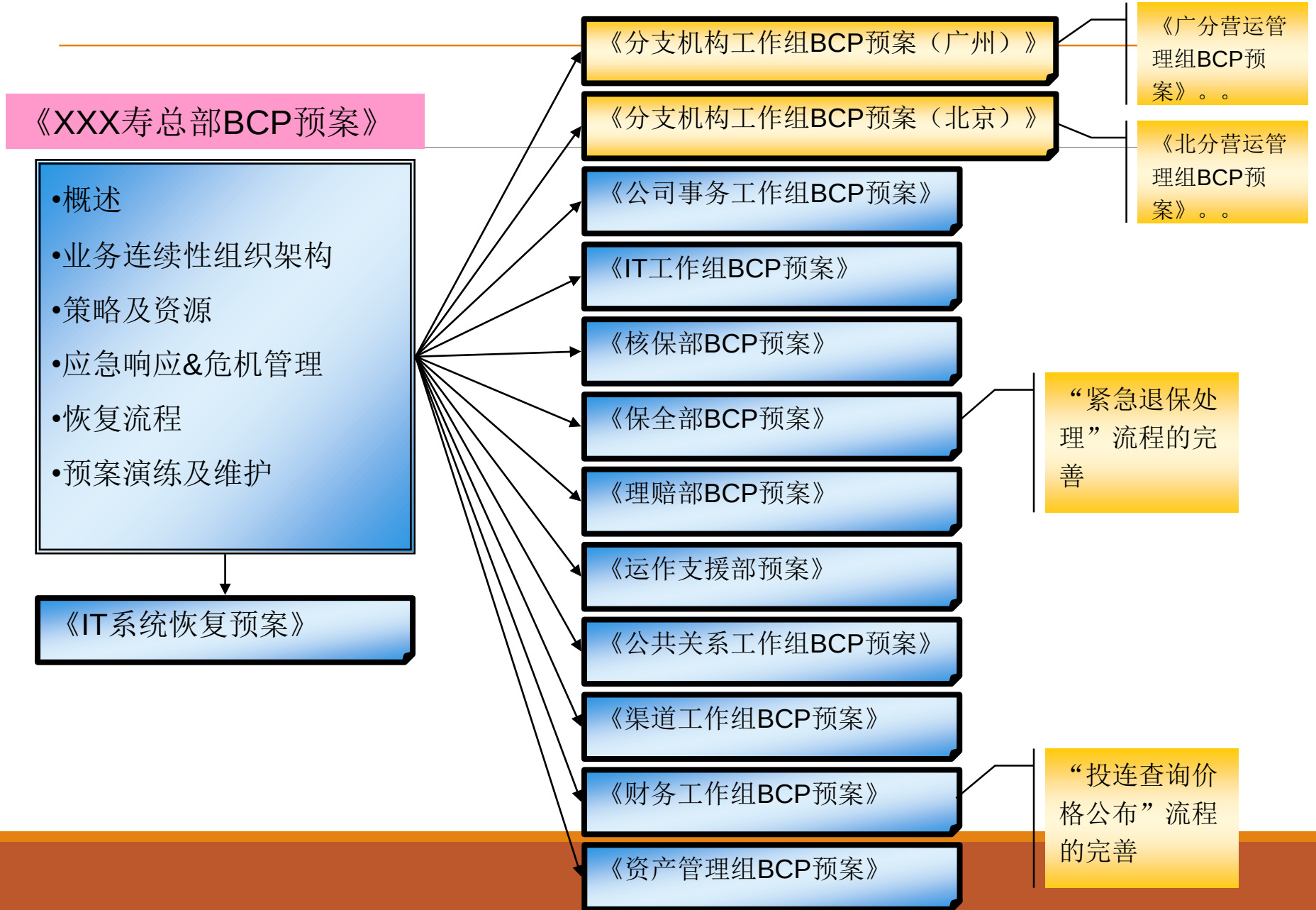
总体安排

10	业务连续性管理体系
20	灾难恢复预案设计
15	灾难恢复预案主要内容
15	案例共享

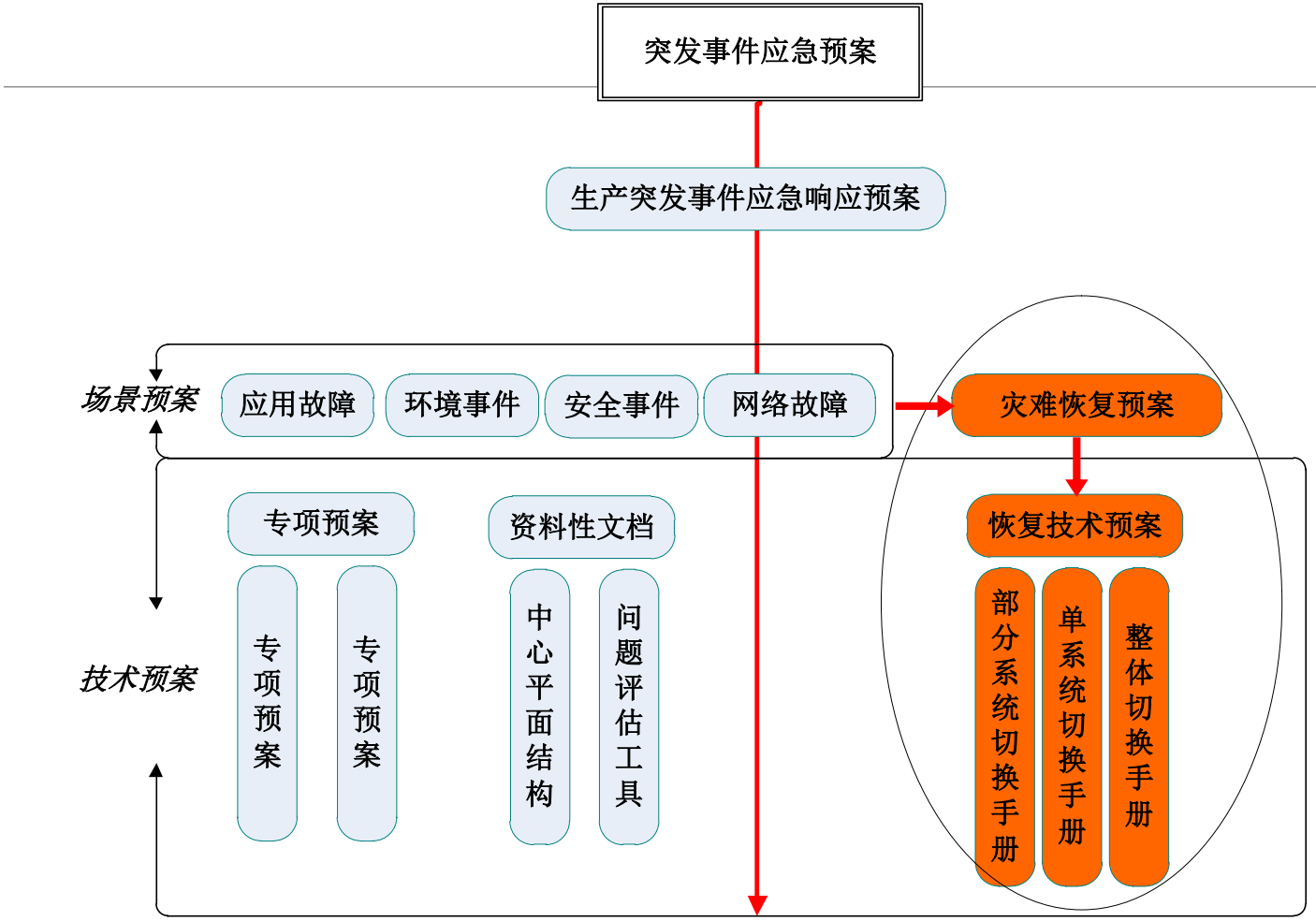
某保险公司BCP组织


战略层
企业永续
经营领导小组
公共关系
工作组
战术层
危机管理小组
IMT
协调员
操作层
公司事务
工作组
财务
工作组
资产管理
工作组
营运
工作组
IT
工作组
渠道
工作组
分支机构
工作组
人力资
源部
总务部
法务部
理赔部
保全部
核保部
运作支
援部

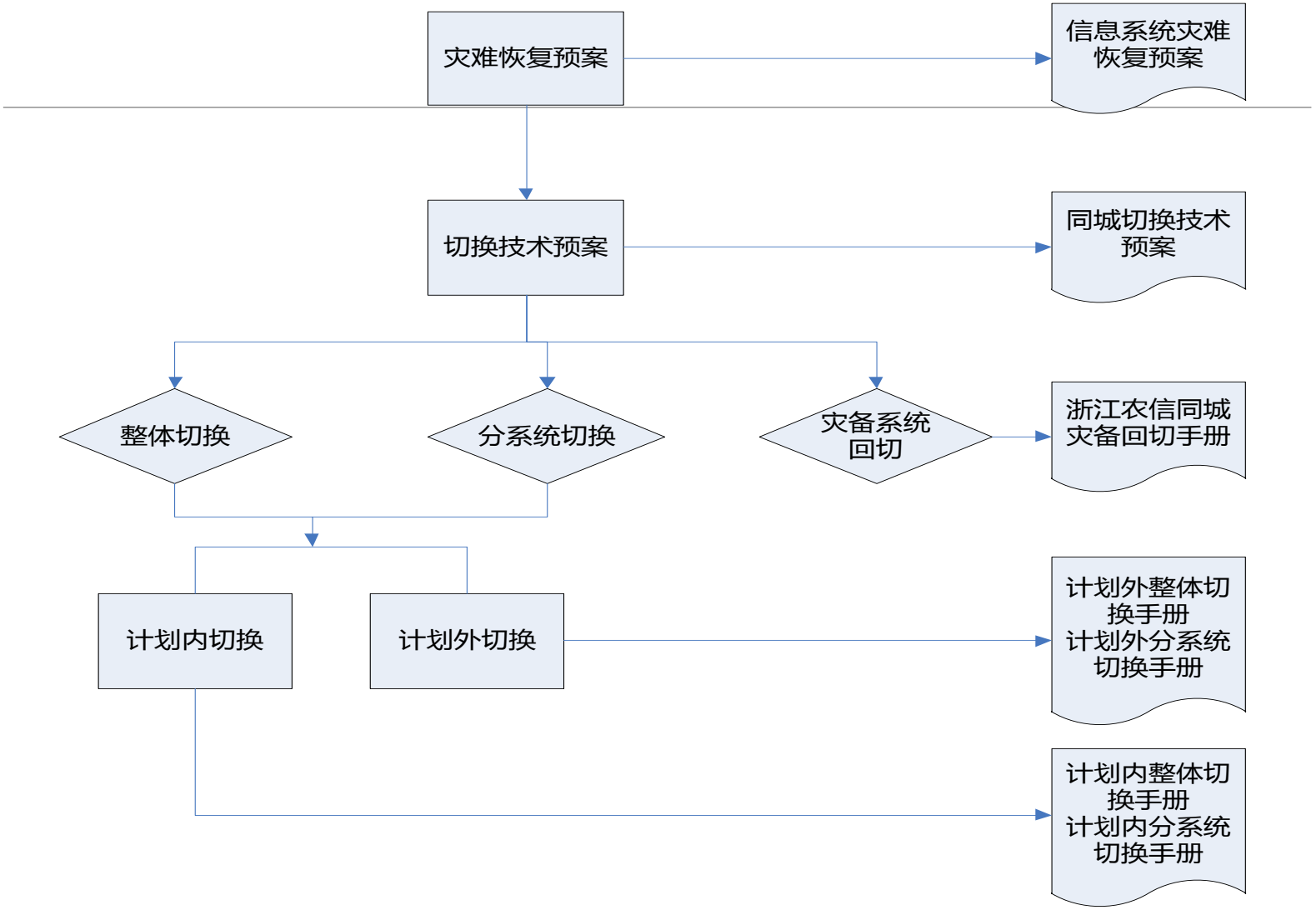
某保险公司分部门BCP预案



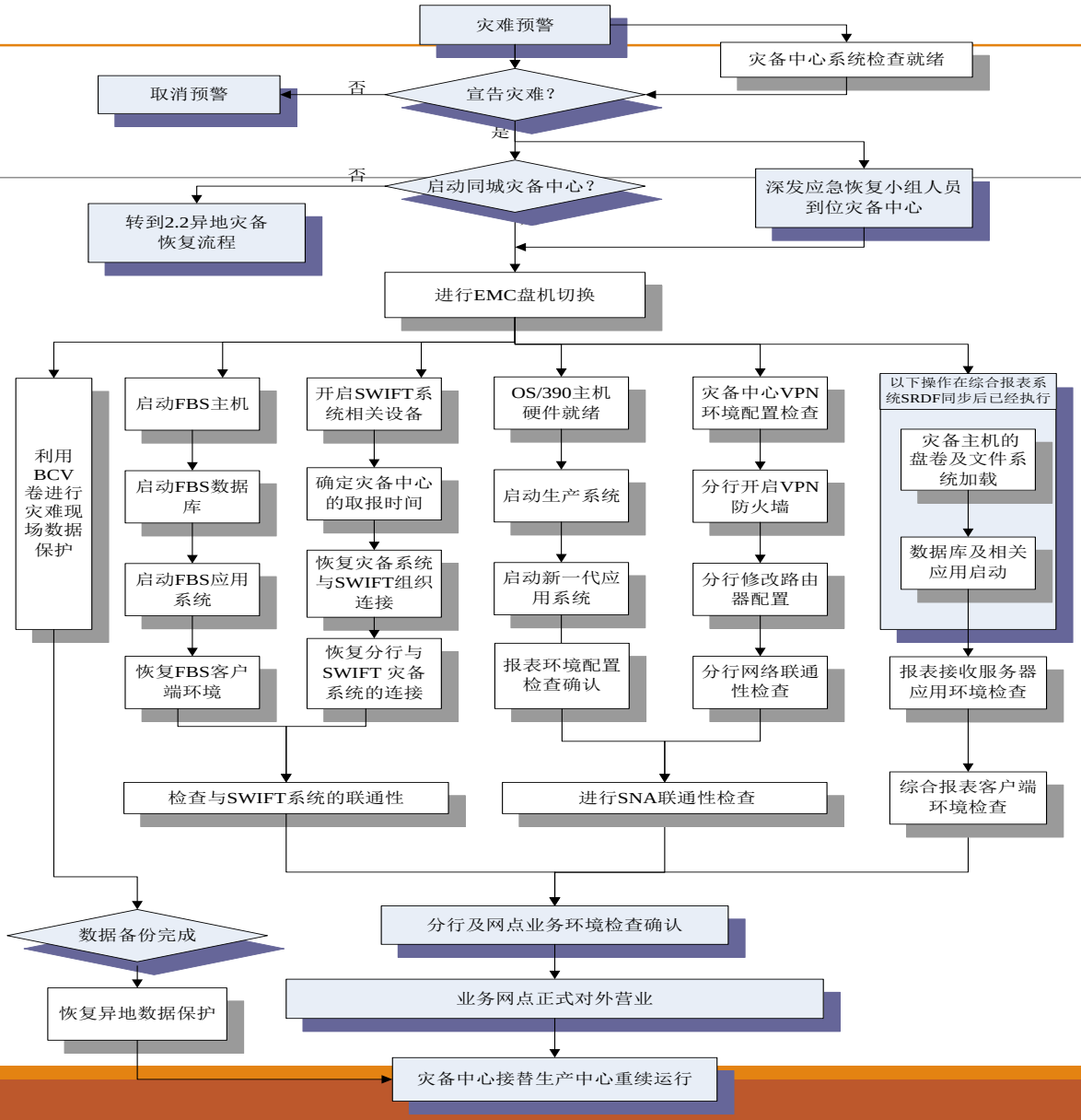
某银行预案体系


突发事件应急预案
生产突发事件应急响应预案
场景预案
应用故障
环境事件
安全事件
网络故障
灾难恢复预案
专项预案
资料性文档
恢复技术预案
技术预案
专项预案
专项预案
中心平面结构
问题评估工具
部分系统切换手册
单系统切换手册
整体切换手册

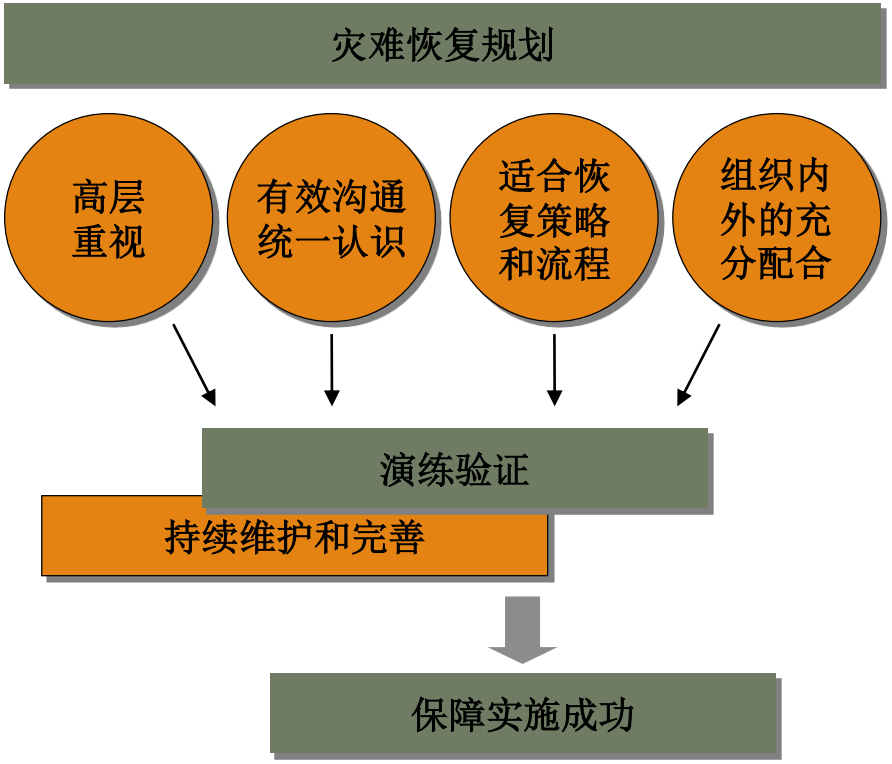
预案调用关系


灾难恢复预案
信息系统灾难恢复预案
切换技术预案
同城切换技术预案
整体切换
分系统切换
灾备系统回切
浙江农信同城灾备回切手册
计划内切换
计划外切换
计划外整体切换手册
计划外分系统切换手册
计划内整体切换手册
计划内分系统切换手册

某银行切换流程图


灾难预警
灾备中心系统检查就绪
取消预警
否
宣告灾难？
是
否
启动同城灾备中心？
深发应急恢复小组人员到位灾备中心
转到2.2异地灾备恢复流程
进行EMC盘机切换
利用BCV卷进行灾难现场数据保护
启动FBS主机
启动FBS数据库
启动FBS应用系统
恢复FBS客户端环境
开启SWIFT系统相关设备
确定灾备中心的取报时间
恢复灾备系统与SWIFT组织连接
恢复分行与SWIFT 灾备系统的连接
OS/390主机硬件就绪
启动生产系统
启动新一代应用系统
报表环境配置检查确认
灾备中心VPN环境配置检查
分行开启VPN防火墙
分行修改路由器配置
分行网络联通性检查
以下操作在综合报表系统SRDF同步后已经执行
灾备主机的盘卷及文件系统加载
数据库及相关应用启动
报表接收服务器应用环境检查
综合报表客户端环境检查
检查与SWIFT系统的联通性
进行SNA联通性检查
数据备份完成
恢复异地数据保护
分行及网点业务环境检查确认
业务网点正式对外营业
灾备中心接替生产中心重续运行

小结


灾难恢复规划
高层重视
有效沟通统一认识
适合恢复策略和流程
组织内外的充分配合
演练验证
持续维护和完善
保障实施成功

谢 谢