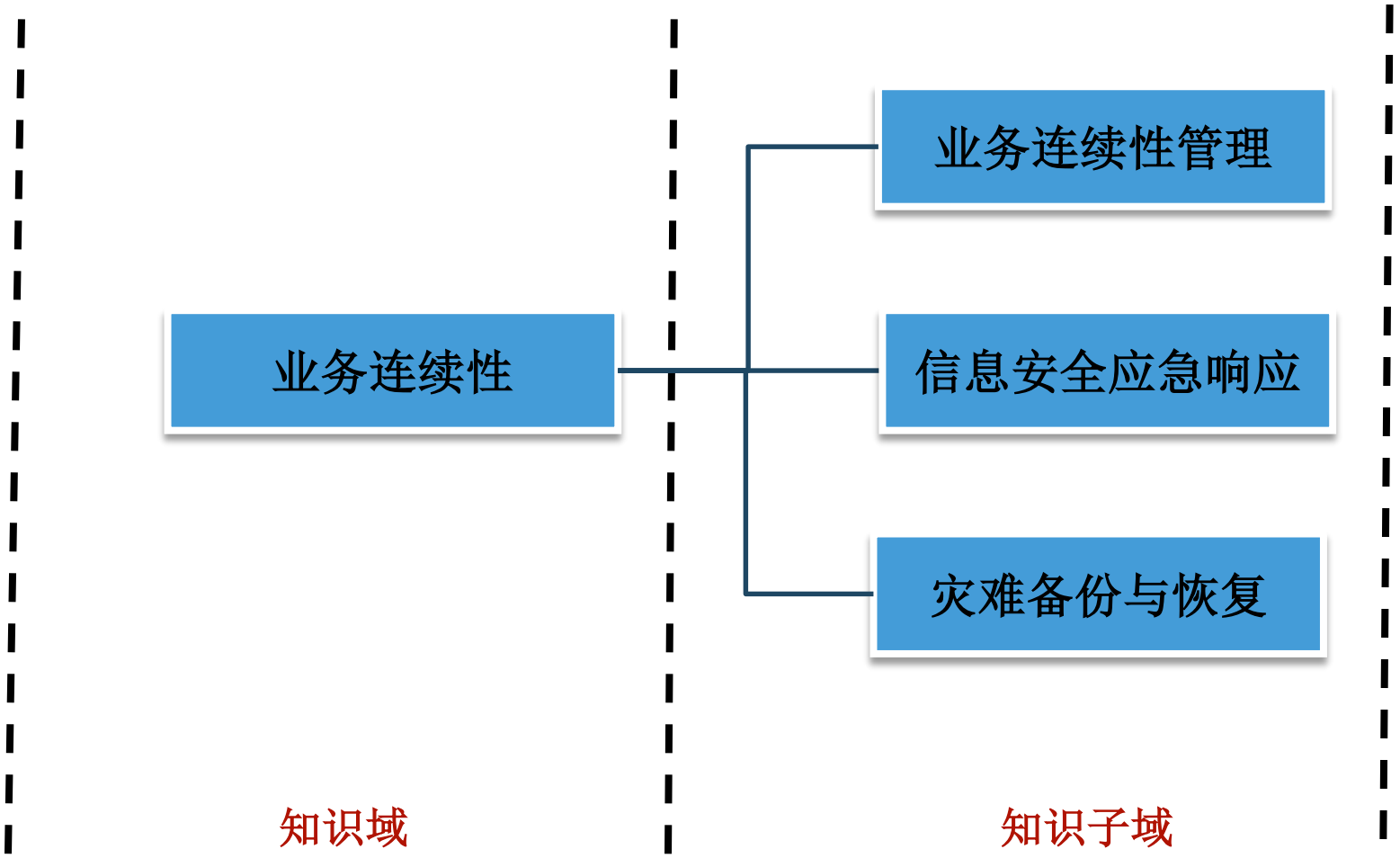
业务连续性

版本：4.2

东方瑞通

课程内容



知识子域：业务连续性管理

- 业务连续性管理基础
  - 了解业务连续性、业务连续性管理的概念；
  - 理解业务连续性管理对组织机构的重要性；
  - 了解业务连续性管理生命周期六个阶段的工作内容。

业务连续性管理基础

- 业务连续性(BC)
  - 业务连续性（Business Continuity, BC）是组织对事故和业务中断的规划和响应，使业务可能在预先定义的级别上持续运行的组织策略和战术上的能力
- 业务连续性管理(BCM)
  - BCM是找出组织有潜在影响的威胁及其对组织业务运行的影响，通过有效响应措施保护组织的利益、信誉、品牌和创造价值的活动，并为组织提供建设恢复能力框架的整体管理过程
- 一项综合管理流程，由业务驱动，集合了技术、管理的一体化动态管理流程

业务连续性管理基础

- BCM与组织机构
  - BCM应为业务战略服务
  - BCM是风险管理框架的补充，主要考虑业务中断的影响
- BCM的生命周期
  - 需求、组织和管理程序的确定
  - 业务分析，确定关键业务流程和关键因素
  - 制定业务策略
  - 开发并执行业务持续计划
  - 意识培养和建立
  - 计划演练

知识子域：业务连续性管理

- 业务连续性计划
  - 了解业务连续性计划的概念及制定业务连续性计划的四个步骤；
  - 理解组织管理在业务连续性计划过程中的重要性及四个要素；
  - 理解业务影响分析在业务连续性计划过程中的作用及各项工作内容；
  - 了解业务连续性计划制定和批准实施工作的内容并理解风险降低、风险转移、风险规避和风险接受四种风险处置方式；
  - 了解业务连续性计划文档化的作用、文档应包括的内容及批准、实施、评估及维护等相关概念。

业务连续性计划

- 什么是业务连续性计划
  - 一套基于业务运行规律的管理要求和规章流程，能够使一个组织在突发事件面前迅速做出反应，以确保关键业务功能可以持续，而不造成业务中断或业务流程本质的改变
- 建立在对组织机构各种过程的风险评估之上
- 关注基础设施功能和资源减少或受限的情况下维持业务操作
- BCP应成为组织管理文化的一部分，企业业务模式或业务过程变化情况下，应重新设计

组织管理

- 理解业务组织
  - 充分了解组织的体系结构及其组成部分
  - 清晰每个业务流程及相互依赖关系
- 建立BCP团队
  - 负责人 、团队成员
- 评估BCP资源
  - 购买和部署冗余设备、办公用品等
  - BCP开发过程，BCP测试、培训、和维护过程中的人力资源
- BCP的合规性要求
  - 法律法规合规性、合同的合规性

业务影响分析

- 确定组织持续运行的关键资产、针对这些资产的威胁、评估每种资产出现的威胁及对业务的影响
- 提供量化度量以确定投入资源的优先顺序
- 工作内容
  - 确定业务优先级
  - 风险分析
  - 资产优先级划分

业务影响分析完成后，文档化所有的流程！

确定业务优先级

- 业务流程综合列表，按重要性排序
- 业务功能实际运作需要资源（计算机系统、人员、通信、物理设备）和服务
- 确定业务优先级的关键点
  - 业务所需资源的相互关系
  - 对外部组织或其他方的依赖

确定业务优先级

- 确定业务优先级需要做的工作
  - 评估如果业务中断，随时间推移对组织所造成的影响
  - 为每项业务建立最大允许中断时间
  - 识别任何相互依赖的活动、资产、用于支持的基础设施和资源
- 度量标准
  - 恢复时间目标（ RTO）

风险分析

- 识别并分析组织所面临的重大风险
- 风险要素识别
  - 威胁分析
  - 可能性分析
  - 影响分析

参考安全评估中相关内容！

资产优先级划分

- 针对各种不同风险所分配的业务连续性资源的优先级
- 确定资源水平时，应考虑相关利益方的需求
- 优先级列表可结合定量和定性两种方法确定

制定及批准实施

- BCP的制定
  - 确定业务连续性计划要处理的风险及采取的措施
- 四种风险处置方式
  - 风险降低
  - 风险转移
  - 风险规避
  - 风险接受

风险降低

- 预防性策略和反应性策略
  - 采用适当地、低成本的预防性措施应当优于反应性策略
- 重点保护对象：人力资源
  - 人是BCP的关键组成部分
  - 措施：人员冗余（AB角、轮岗、多技能培训等）、负责同一重要业务人员不能同时面临某个特定风险，例如不能同乘一架飞机

风险降低

- 重点保护对象：IT基础设施
  - 信息系统设施主要部分（硬件、软件、支撑环境等）
  - 措施：保护性措施（发电机、火灾探测和灭火社保等）、冗余措施等
- 重点保护对象：辅助性设施
  - 为完成业务所需要的其他设施（非IT）
  - 措施：强化机制和过程、备用场所

风险转移

- 降低财务风险或资产的风险的有效方式，但有些风险不能转移
- 转移方式
  - 购买保险
  - 合同（向第三方支付费用）
    - 外包合同中承诺的赔付
    - 采购第三方服务

风险规避

- 风险规避
  - 变更、延缓或停止某种服务或业务功能
  - 该措施只能在与组织目标、法律法规符合性以及利益相关方的期望不发生冲突时考虑
- 风险接受
  - 采取措施的潜在收益与成本不成比例
  - 对某些风险能够采取措施的能力有限

文档化

- 文档化是BCP过程中的关键步骤
- 文档需要包含的内容
  - BCP的目标:必须细化
  - 职责声明：确保相关人员都了解他们的职责
  - 优先级声明
  - 风险评估
  - BCP策略
  - 关键业务记录计划
  - 应急响应的知道原则
  - 测试与演练

批准与实施

- 向高层汇报并获得计划的批准
- 培训和教育，计划中涉及的所有人都需要接受与职责相关的培训

评估及维护

- 业务的动态性决定了业务连续性要求也会随时改变
- 定期讨论、复审、测试结果，必要时进行版本更新

知识子域：信息安全应急响应

- 信息安全事件与应急响应
  - 了解信息安全事件的概念及应急响应在信息安全保障工作中的重要性；
  - 了解我国信息安全事件的分类分级标准；
  - 了解国际及我国信息安全应急响应组织；
  - 了解应急响应组织架构。

应急响应的概念

- 信息安全事件
  - 由于自然或人为以及软、硬件本身缺陷或故障的原因，对信息系统造成危害，或者在信息系统内发生对社会造成负面影响的事件
  - 对信息安全事件进行有效管理和响应，是组织机构安全战略的一部分
- 应急响应
  - 组织为了应对突发/重大信息安全事件的发生所做的准备，以及在事件发生后所采取的措施。

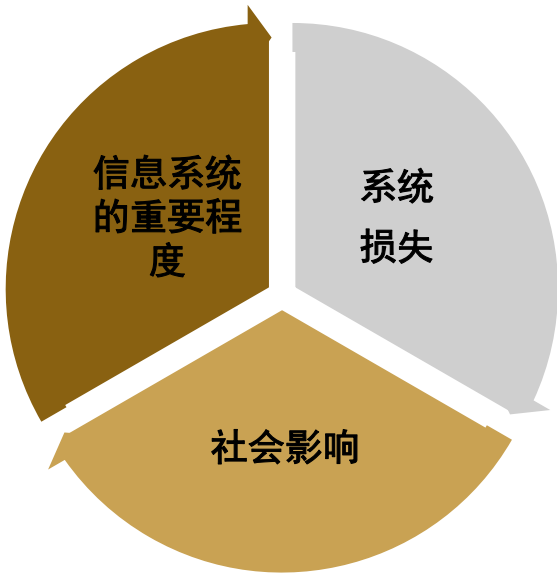
应急响应工作列为我国信息安全保障工作的重点之一！

信息安全事件分类分级

- 分类分级是有效防范和响应信息安全事件的基础，能够使事前准备、事中应对和事后处理的各项相关工作更具针对性和有效性
- 分类
  - GB/Z 20986-2007 中，分有害程序事件、网络攻击事件、信息破坏事件、信息内容安全事件、设备设施故障、灾害性事件和其他信息安全事件7个基本类别，每个类别下有若干子类

信息安全事件分类分级

- 分级
  - 参考要素：信息系统的重要程度、系统损失和社会影响
  - 四级（GB/Z 20986—2007）
    - 特别重大事件（I级）
    - 重大事件（II级）
    - 较大事件（III级）
    - 一般事件（IV级）



信息安全应急响应组织

- 国际应急响应组织
  - 计算机应急响应协调中心（CERT /CC）
- 国家应急响应组织
  - 国家计算机网络应急技术处理协调中心（CNCERT /CC ）
- 组织机构应急响应组织架构
  - 应急响应领导组
  - 应急响应技术保障组
  - 应急响应专家组
  - 应急响应实施组
  - 应急响应日常运行组

知识子域：网络安全应急响应

- 网络安全应急响应预案
  - 了解网络安全应急响应预案的概念及作用；
  - 理解应急响应演练的作用、分类、方式及流程。
- 计算机取证及保全
  - 了解计算机取证的概念及取证的过程；
  - 理解计算机取证过程中准备、保护、提取、分析和提交五个步骤的工作内容。
- 信息安全应急响应管理过程
  - 了解应急响应管理中准备、检测、遏制、根除、恢复和跟踪总结六个阶段工作的内容和目标

应急响应预案

- 什么是应急预案
  - 在分析网络与信息系统突发事件后果和应急能力的基础上，针对可能发生的重大网络与信息系统突发事件，预先制定的行动计划或应急对策。
- 应急预案编制
  - 建立在综合防灾规划之上
  - 描述支持应急操作的技术能力，并适应组织要求
  - 在详细程度和灵活程度之间取得平衡
  - 为信息安全事件中不熟悉计划的人员提供快捷明确的指导

应急响应预案的格式

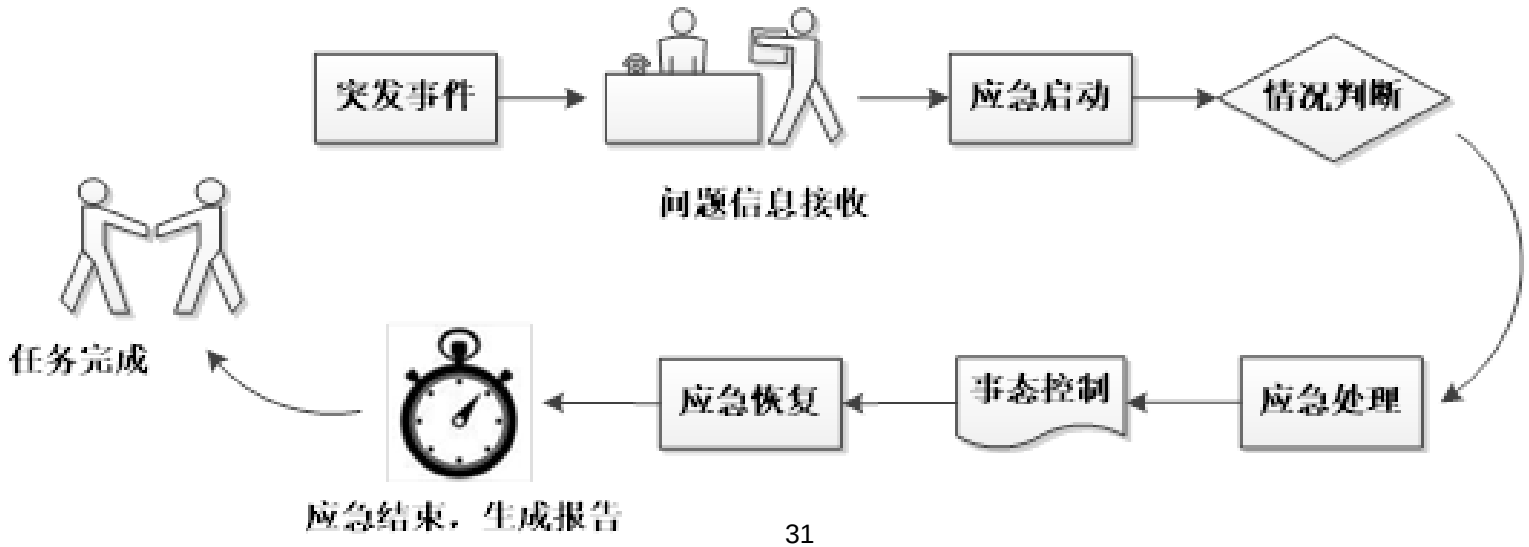
- 没有标准格式
  - 可参考《国家网络安全事件应急预案》
  - 应包括总则、角色及职责、预防和预警机制、应急响应流程、应急响应保障措施和附件

应急演练与演习

- 检验应急响应预案的有效性、应急准备的完善性、应急响应能力的适应性和应急人员的协同性
- 演练方式
  - 桌面演练、模拟演练、实战演练
- 演练深度
  - 数据级演练、应用级演练、业务级演练

信息安全应急演练的操作流程

- 应急事件通报
- 确定应急事件优先级
- 应急响应启动实施
- 应急响应时间后期运维
- 更新现有应急预案



计算机取证的概念

- 什么是计算机取证
  - 使用先进的技术和工具，按照标准规程全面地检查计算机系统，以提取和保护有关计算机犯罪的相关证据的活动
- 原则
  - 合法原则、充分授权原则、优先保护证据原则、全程监督原则
- 取证流程

计算机取证-准备

- 获取授权
  - 取证工作获得明确的授权（授权书）
- 目标明确
  - 对取证的目的有清晰的认识
- 工具准备
  - 对取证环境的了解及需要准备的工具
- 软件准备
  - 对取证的软件进行过有效的验证
- 介质准备
  - 确保有符合要求的干净的介质可用于取证

计算机取证–保护

- 保证数据安全性
  - 制作磁盘映像——不在原始磁盘上操作
- 保证数据完整性
  - 取证中不使用可能破坏完整性的操作
- 第三方监督
  - 所有操作都有第三方在场监督

计算机取证–提取

- 优先提取易消失的证据
  - 内存信息、系统进程、网络连接信息、路由信息、临时文件、缓存
- 文件系统
  - 数据恢复、隐藏文件、加密文件、系统日志
- 应用系统
  - 系统日志

计算机取证-分析及提交

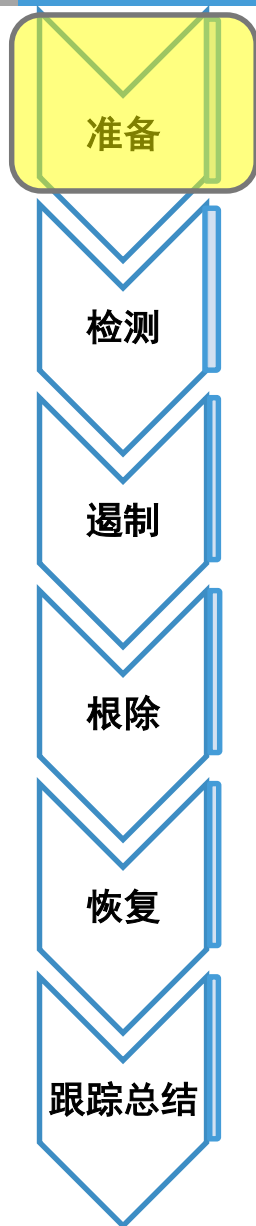
- 证据在什么地方？
  - 日志、删除的文件、临时文件、缓存
- 从证据中能发现什么？
- 如何关联证据？
- 电子取证提交
  - 必须与现实取证结合，文档化很重要

应急响应六阶段

- 第一阶段：准备——让我们严阵以待
- 第二阶段：检测——对情况综合判断
- 第三阶段：遏制——制止事态的扩大
- 第四阶段：根除——彻底的补救措施
- 第五阶段：恢复——系统恢复常态
- 第六阶段：跟踪总结——还会有第二次吗

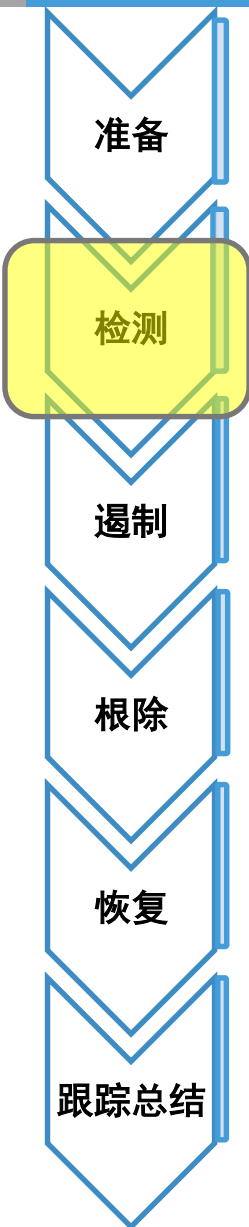
第一阶段 — 准备

- 工作目标
  - 确定重要资产和风险，实施针对风险的防护措施；
  - 编制和管理应急响应计划
    - 应急响应计划的编制准备
    - 编制应急响应计划
    - 应急响应计划的测试、培训演练和维护
- 为响应组织和准备相关资源
  - 人力资源(应急响应组织)
  - 财力资源、物质资源、技术资源和社会关系资源等



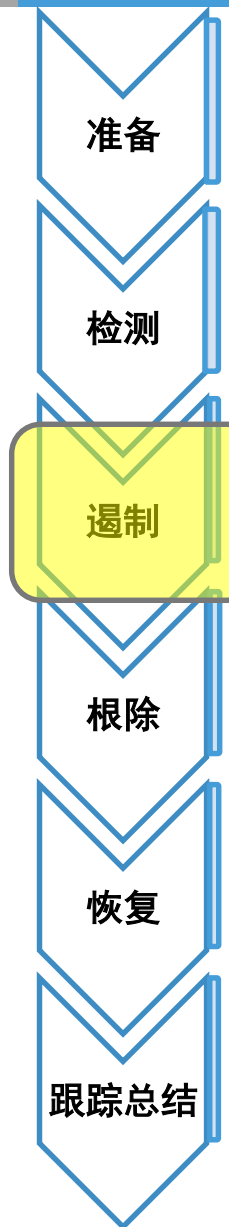
第二阶段 — 检测

- 工作目标
  - 检测并确认事件的发生
  - 确定事件性质和影响
- 工作内容
  - 进行监测、报告及信息收集
  - 确定事件类别和级别
  - 指定事件处理人，进行初步响应
  - 评估事件的影响范围
  - 事件通告（信息通报、信息上报、信息披露）



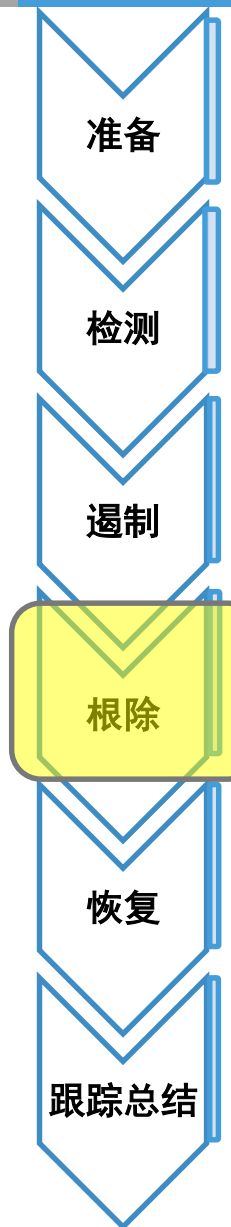
第三阶段 — 遏制

- 工作目标
  - 限制事件影响的范围、损失
- 工作内容
  - 启动应急响应计划
  - 确定适当的响应方式
  - 实施遏制行动
  - 要求用户按应急行为规范要求配合遏制工作



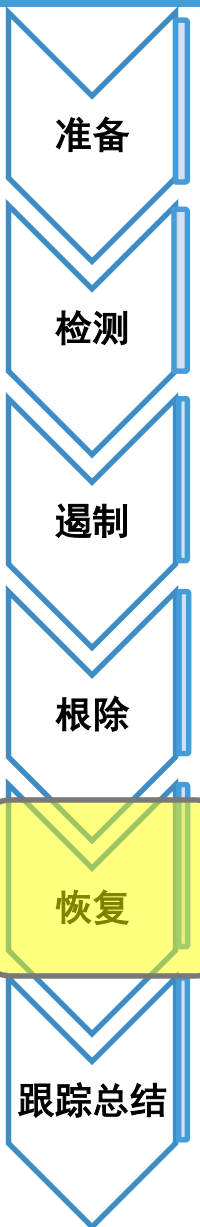
第四阶段 — 根除

- 工作目标
  - 避免问题再次发生的长期的补救措施
- 工作内容
  - 详细分析，确定原因
  - 实施根除措施，消除原因



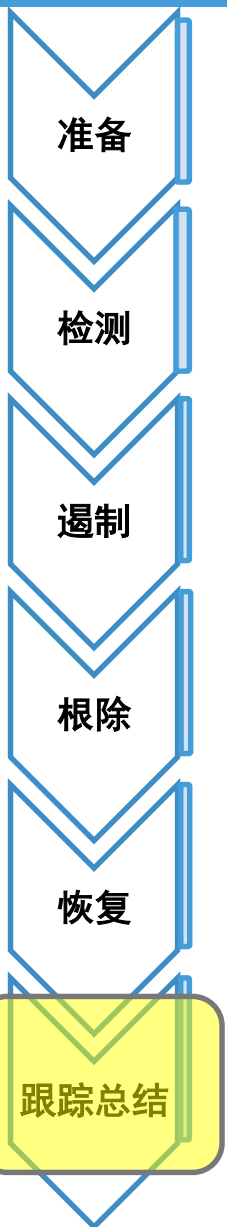
第五阶段 — 恢复

- 工作目标
  - 恢复系统至正常状态
- 工作内容
  - 根据破坏程度决定是在原系统还是备份系统中恢复
  - 按恢复优先顺序恢复系统和业务运行



第六阶段 — 跟踪总结

- 工作目标
  - 回顾并汇总所发生事件的相关信息
- 工作内容
  - 关注系统恢复以后的安全状况，记录跟踪结果
  - 评估损失、响应措施效果
  - 分析和总结经验、教训
  - 重新评估和修改安全策略、措施和应急响应计划
  - 对进入司法程序的事件，进行进一步调查，打击违法犯罪活动
  - 编制并提交应急响应报告



知识子域：灾难备份与恢复

- 灾难备份与恢复基础
  - 了解灾难备份、灾难恢复计划的概念及作用；
  - 理解RTO、RPO等灾备的关键指标；
  - 了解国家灾备相关政策与标准；
  - 了解灾难恢复组织结构。

灾难备份与恢复基础

- 灾备概念
  - 为了保证关键业务和应用在经历各种灾难后，仍然能够最大限度的提供正常服务所进行的一系列系统计划及建设行为，其目的就是确保关键业务持续运行以及减少非计划宕机时间
  - 灾难备份是灾难恢复的基础，灾难恢复不能只考虑信息系统的恢复，更应关注业务的恢复
- 灾难恢复计划
  - 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

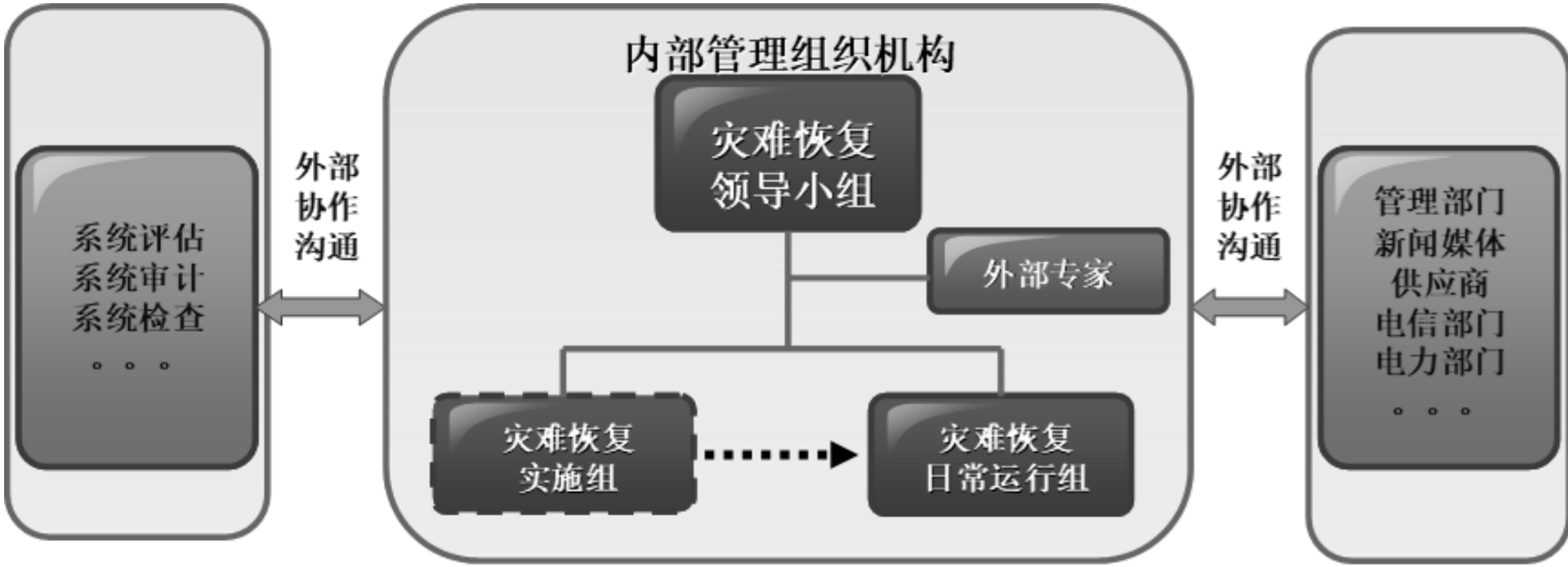
灾备指标

- 恢复点目标（RPO）
  - 定义：灾难发生后，系统和数据必须恢复到的时间点要求
  - 代表了当灾难发生时允许丢失的数据量
- 恢复时间目标（RTO）
  - 定义：灾难发生后，信息系统和业务功能从停顿到必须恢复的时间要求
  - 代表了企业能容忍的信息系统和业务功能恢复的时间

灾备组织

组织构成

- 领导组、规划实施组、日常运行组
- 规划工作可聘请外部专家，实施和运行也可委托外包机构承担



国家灾备政策及相关标准

- 27号文首次提出灾备概念
- 重要信息系统灾难恢复指南：指明了灾难恢复的工作流程、等级划分和预案的制定框架
- GB/T 20988-2007，规定了灾难恢复工作流程、灾难恢复等及方案设计、预案、演练
- 《灾难恢复中心建设与运维管理规范》，指出了灾备中心建设的全生命周期、灾备中心的运维工作

知识子域：灾难备份与恢复

- 灾难恢复相关技术
  - 了解DAS、SAN、NAS存储技术的概念及应用区别；
  - 了解全备份、增量备份、差分备份等备份方式的区别；
  - 了解常用的备份介质；
  - 理解磁盘冗余阵列RAID-0、RAID-1、RAID-5等配置的差别；
  - 了解冷站、温站、热站等概念。

存储技术

- 直接附加存储（DAS）
  - 直接连接在各种服务器或客户端扩展接口下的数据存储设备， 依赖计算机，是硬件堆叠，不带操作系统
  - 优点：适用物理位置分散情况、容易实现打容量存储，性能较高、实施简单
  - 缺点：对服务器依赖性强，占用服务器资源、扩展性较差、资源利用率低、可管理性差
- 存储区域网络（SAN）
  - 专用网络、效率高、扩展方便
  - 成本高、实施复杂、难度大

存储技术

- 网络附加存储（NAS）
  - 直接通过网络接口将存储设备与网络相连实现数据存储的机制
  - 有独立IP地址，操作系统等
  - 优点：易于安装不是和管理、不占用服务器资源、跨平台
  - 不足：性能相对较差，因为数据传输使用网络，可能影响网络流量、甚至可能产生数据泄漏等安全问题

备份技术

- 备份方式
  - 完全备份
  - 增量备份
  - 差量备份
- 备份介质
  - 磁带
  - 硬盘

冗余磁盘阵列（ RAID）

- 实现方式
  - RAID-0（条带）：提高了磁盘子系统的性能，但不提供容错能力
  - RAID-1 （镜像）：磁盘一对一镜像，确保数据不丢失
  - RAID-5（奇偶校验）：三块以上磁盘，其中一块作为校验信息，允许第一磁盘损坏
- 可基于硬件，也可基于软件

备用场所

- 冷站
- 温站
- 热站
- 移动站
- 镜像站

知识子域：灾难备份与恢复

- 灾难恢复策略
  - 了解国际标准SHARE78对灾难备份的能力划分的0~6级的区别；
  - 理解我国《重要信息系统灾难恢复指南》中划分的6个灾难恢复等级要求；
  - 了解企业常用的容灾策略中数据容灾、系统容灾、应用容灾的概念；
  - 了解确定灾难恢复能力级别的方法。

国际标准SHARE78

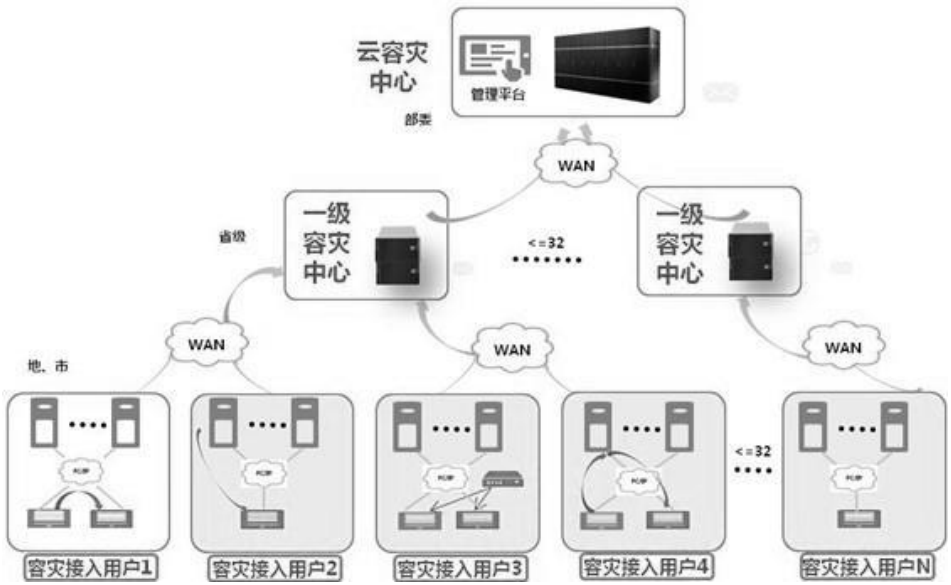
- 划分依据：八个方面
- 灾难备份能力0~6级
  - 0级：无异地备份
  - 1级：简单异地备份
  - 2级：热备中心备份
  - 3级：电子传输备份
  - 4级：自动定时备份
  - 5级：实时数据备份
  - 6级：数据零丢失

重要信息系统灾难恢复指南

- 划分依据：七个要素
- 6个灾难恢复等级
  - 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 电子传输及完整设备支持
  - 第5级 实时数据传输及完整设备支持
  - 第6级 数据零丢失和远程集群支持

组织容灾策略构建

- 根据对灾难的抵抗程度，容灾技术可分为以下三种：
  - 数据容灾（首要前提）
  - 系统容灾（基本基础）
  - 应用容灾（主要关键）



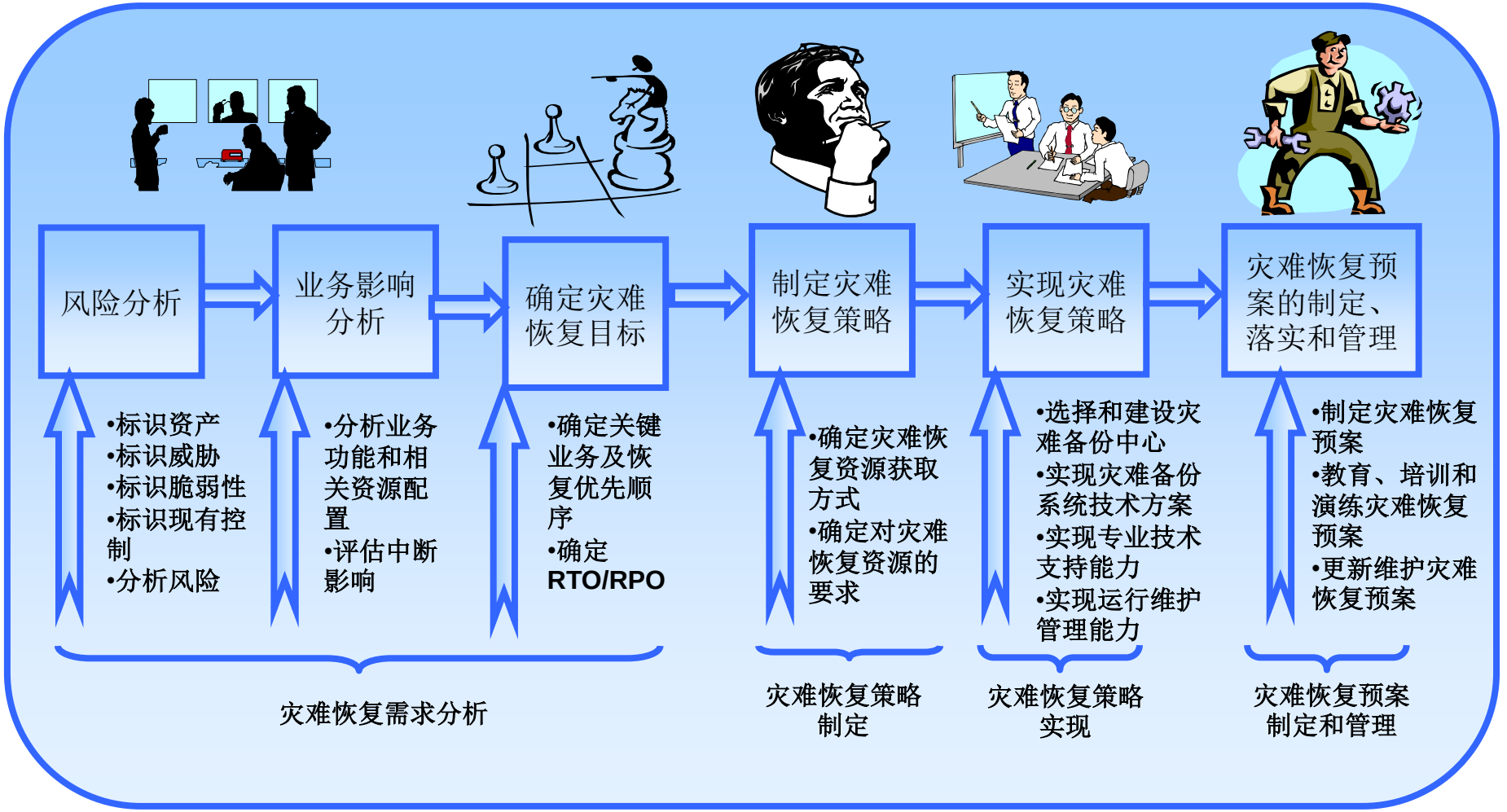
知识子域：灾难备份与恢复

- 灾难恢复管理过程
  - 了解灾难恢复管理规划的作用及工作过程；
  - 理解灾难恢复需求分析风险分析、业务影响分析和确定灾难恢复目标三个子步骤的工作内容和目标；
  - 理解灾难恢复策略制定的原则和工作方法；
  - 了解灾难恢复策略实现的工作步骤和要求；
  - 了解灾难恢复预案的制定与管理工作内容及要求。

灾难恢复规划的工作内容

- 灾难恢复规划：是一个周而复始的、持续改进的过程，包含以下四个阶段
  - 灾难恢复需求分析
  - 灾难恢复策略制定
  - 灾难恢复策略实现
  - 灾难恢复预案的制定和管理

灾难恢复规划的管理过程



灾难恢复需求分析

- 风险分析
  - 资产、威胁、脆弱性、可能性、影响
- 业务影响分析
  - 分析业务功能和相关资源配置
  - 评估中断影响
- 确定灾难恢复目标
  - 关键业务功能及恢复的优先顺序
  - RTO 和RPO 的范围

灾难恢复策略制定及策略实现

- 策略制定
  - 明确需要哪些灾难恢复资源、各项灾难恢复资源的获取方式，以及对各项灾难恢复资源的具体要求
- 策略实现
  - 选择和建设灾难备份中心
  - 实现灾难备份系统技术方案
  - 实现专业技术支持能力
  - 实现运行维护管理能力

灾难恢复预案制定和管理

- 制定灾难恢复预案
- 灾难恢复计划的教育与培训
- 灾难恢复计划演习
- 灾难恢复预案的保存与分发

总结

- 业务连续性管理
  - 业务连续性的概念
  - 业务连续性计划建设过程
- 网络安全应急响应
  - 安全事件、分类分级
  - 应急响应预案
  - 应急响应管理过程
- 灾难备份与恢复
  - 灾难备份与恢复基本概念，灾备技术
  - 灾难恢复策略与灾难恢复规划管理过程

谢谢观看！