《业务连续性管理》考前知识点串讲

一、安全事件和应急响应

1. 应急响应概念：**事件前**的**充分准备**和**事件后的应急处置**。
2. 安全事件分类：**有害程序事件、网络攻击事件、信息破坏事件、信息内容事件、设备设施故障事件、自然灾害事件**，其他事件。
3. 事件分级的要素：**系统重要程度、系统损失、社会影响**。
4. 事件分级：（**4**）一般事件、（**3**）较大事件、（**2**）重大事件、（**1**）特大事件。
5. 事件处理的过程：1-**准备**、2-**检测**、3-**遏制**、4-**根除**、5-**恢复**、6-**跟踪总结**。
6. 事件应急预案：制定、评估和批准、演练和演习、预案的修订和升级。
7. 计算机取证

1）原则：**合法**、**充分授权**、**优先保护**、**全程监督**。

2）过程：1-**准备**、2-**证据保护**、3-**证据提取**、4-**证据分析**、5-**证据报告提交**。

二、业务连续管理基础

1. 概念：BCM（业务连续性管理）
2. 业务连续性管理基础：1）业务部门主导、it 参与。2）业务连续性管理是针对造成业务中断的安全事件的准备工作及处置恢复工作。
3. 业务连续性管理过程：1-**业务优先级,2-风险分析,3-业务连续性优先级,4-制定业务连续性预案,5-根据预案进行应急处置。**
4. RTO 和 RPO 的对比。RTO 代表可用性，RPO 代表完整性。

理想情况下 RTO=RPO=0，RPO 理论可以为 0，RTO 从用户角度可以为 0，从技术原理的角度只能无限接近于 0.

1）RTO:恢复的时间多少、恢复的效率、中断的时间。

2）RPO:损失的数据、数据的完整性有关。

三、灾备恢复

1. 灾备恢复的概念：应对灾难事件备份工作及灾难性事件后的恢复工作。
2. 灾备恢复的过程：

1）**需求分析**：风险评估、BIA（业务影响分析）、需求指标（**RTO/RPO**）。

2）**灾备恢复策略：7 个要素**来制定，**数据**备份系统、备用**数据处理**系统、备用**网络系统**、备用**基础设施**、备份的**技术**支持**能力**、备用的**管理**维护**能力**、灾备恢复的**预案**。

3）**灾备恢复策略实现**：7 个要素来实现。

4）**灾备恢复预案制定和维护**：参考安全事件的预案。

5）灾难性事件的恢复处置过程。

3. 灾备恢复的能力

1）国际标准：0 到 6 级（不考）

2）国家标准：1-6 级。

1 级：基本支持级，数据完全备份 1 周一次，介质场外存放。

2 级：备用场地级，数据完全备份 1 周一次，需要部分系统和网络设备。

3 级：电子传输和部分设备支持：完全备份 1 天一次，网络定时传输，部分设备。

4 级：电子传输和完整设备支持：完全备份 1 天一次，网络定时传输，完整设备，就绪状态。

5 级：实时传输和完整设备支持：完全备份 1 天一次，网络实时传输，就绪状态和自动切换。

6 级：数据的零丢失和远程集群

4. 国标 6 级参考 7 要素：**数据**备份系统、备用**数据处理**系统、备用**网络系统**、备用**基础设施**、备份的**技术**支持**能力**、备用的**管理**维护**能力**、灾备恢复的**预案**。
5. 灾备恢复的技术

1）**DAS**、**NAS** 的区别和对比（参考 SAN、云存储）

- 前者分散存储，浪费资源，可靠性高；后者的集中存储；节约资源；单点故障（需要进行容灾备份）

2）完整备份、差分备份、增量备份的区别及使用的场景

- 完整备份：数据全部备份；备份周期间隔长；场景是系统数据背景；
- 差分备份：和完整数据备份基线对比后更新修改后的数据备份；备份周期间隔中；场景是系统数据、业务数据背景。
- 增量备份：和非完整数据备份基线的版本数据进行备份；备份周期间隔短；场景是业务数据备份。

3）RAID0/1/5 的区别：

RAID-O（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，一块作为校验信息，允许第一磁盘损坏。

4）冷站、温站、热站、移动站、镜像站的不同及使用的场景。

站点	费用	硬件设备	电信	设置时间	位置
冷站	低	无	无	长	固定
温站	中	部分	部分/完全	中	固定
热站	中/高	完全	完全	短	固定
移动站	高	随相关情况而定	随相关情况而定	随相关情况而定	不固定
镜像站	高	完全	完全	无	固定

温馨提示：为了减少学习的负担和聚焦核心，知识点总结写的是关键的精要的要点，并非是知识点的全文，请一定进一步结合官方的教材进行理解和掌握全面，以免产生以偏概全的问题。

（END）