BC/DR Strategy & Implementation:

These units addressed the design and evaluation of BC/DR strategies, comparing frameworks like ISO 22301:2019 and ENISA guidance, and analysing multi-cloud structures (ISO/IEC, 2018; ENISA, 2022; Gartner, 2023).

Key Concepts:

- RTO, RPO and BIA
- ISO 22301:2019
- Single Cloud, Multi-Cloud, Hybrid
- Technologies: Synchronous Replication, Containerisation (Kubernetes, Docker)
- Vendor Lock-in Mitigation: Opara-Martins et al. (2016)
- Architectures: Multi-cloud, Active-Active (Wanclouds, 2025)

Design Requirements:

Requirement	Justification
24/7/365 service	Uninterrupted business
RTO/RPO < 1 min	Prevents downtime/data loss
GDPR compliance	Regulatory fit
Portability	Supports mobility
Resilience & failover	Achieved via multi-cloud

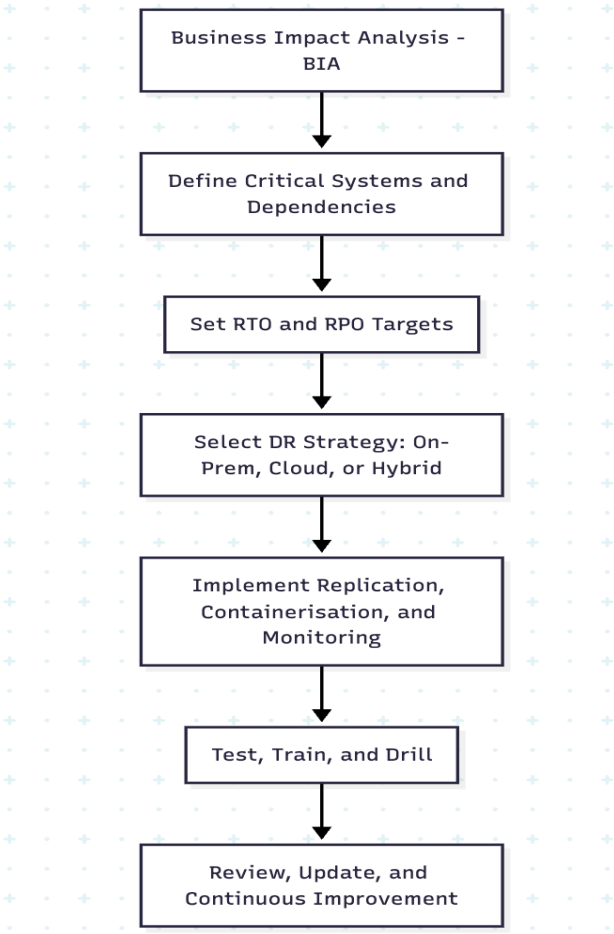
Recommended Architecture:

- Multi-cloud active-active (AWS/Azure)
- Synchronous replication for zero data loss (Alshammari & Alwan, 2017)
- Containerisation for portability (Opara-Martins et al., 2016)
- Automated testing & monitoring (Wanclouds, 2025)

DR Strategy Comparison:

DR Strategy	RTO/RPO	Cost	Lock-in	Suitability
Single-Cloud Active-Passive	5–15 min	Medium	High	Too risky
On-Prem DR	10–30 min	High	Low	Too slow
Multi-Cloud Active-Passive	1–3 min	High	Medium	Acceptable
Multi-Cloud Active-Active	<1 min	High	Low	Best option

DR Planning Lifecycle diagram:



Learning Outcome:

I learnt that there is no universal BC/DR that is in line with the organisation's risk and operational priorities. Through comparing single-cloud, hybrid, and multi-cloud models, I realised that hybrid and active-active architectures deliver stronger resilience. I also recognised that true disaster recovery success depends on compliance, data consistency, regular testing, documentation, and cross-functional drills.

Reference:

Alshammari, R. and Alwan, Z. (2017) 'Disaster Recovery in Single-Cloud and Multi-Cloud Environments', *International Journal of Computer Applications*, 168(3), pp. 21–28.

ENISA (2022) 'ENISA Threat Landscape 2022'. European Union Agency for Cybersecurity. Available at: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022 (Accessed: 20 October 2025).

Gartner (2023) 'Market Guide for Disaster Recovery as a Service (DRaaS)'. Available at: https://recoverypoint.com/press-release/recovery-point-systems-recognized-in-gartners-2023-draas-market-guide (Accessed: 20 October 2025).

ISO/IEC (2018) *ISO 22301: 2019 Business Continuity Management Systems.* Geneva: International Organization for Standardization.

Opara-Martins, J., Sahandi, R. and Tian, F. (2016) 'Critical analysis of vendor lock-in and its impact on cloud computing migration: a business perspective', *Journal of Cloud Computing*, 5(1), pp. 1–18. Available at: https://doi.org/10.1186/s13677-016-0054-z (Accessed: 20 October 2025).

- **Rinaldi, M., Bottani, E. and Regattieri, A. (2022)** 'A literature review on quantitative models for supply chain risk', *Computers & Industrial Engineering*, 170, 108329.

- **Wanclouds (2025)** ‘Best Practices for Building a Cloud-Native Disaster Recovery Strategy’. Available at: https://www.wanclouds.net/blog/kubernetes/best-practices-for-your-cloud-native-disaster-recovery-strategy (Accessed: 20 October 2025).