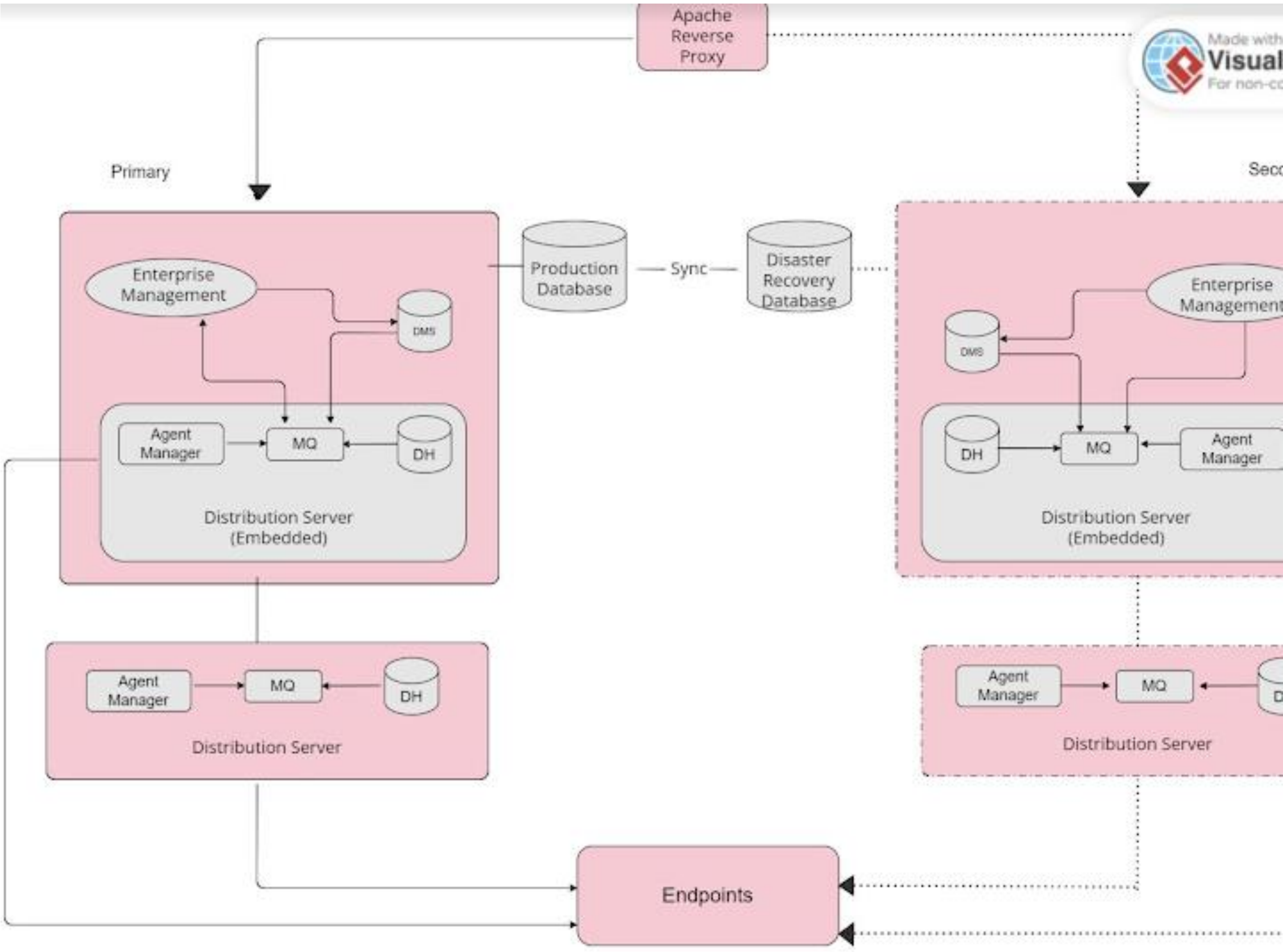
Disaster Recovery (DR) Strategy

Ms O'dour quest for DR strategy is in line with Group C 's recommendation for the proposed digitalized business model for PP. The Implementation of appropriate DR plan is crucial in minimizing the real threat of economic loss, disruption to business operations and diminishing of brand credibility as result of unforeseen operational Disasters. Disasters examples are disruption of IT infrastructure functionality, security breaches, natural disaster, power outages, equipment failures etc. The ISO 22301 recommends that a business should undergo risk assessment, Business impact analysis (BIA), create BC strategy, risk recovery plans, a continuous testing and monitoring of the set strategy to have a functionable BC plans for a going-concern enterprise.

The DR objective for PP is the availability of IT infrastructure to support online shopping 24/7/365 in the event of any disaster affecting the shop premises. The expected Recovery Time Objective (RTO) should be less than 1 minute, meaning the maximum time before the system is completely changeover in the event of disaster while, the threshold for Recover Point Objective (RPO) is less than or equal to 1 minute data loss meaning the point that system must be recovered to avoid further data loss.

The DR solution is an active-active DR failover configuration that will spans between two sites and its means the online platform is critical to the business. The two sites will be identical and active with multiple data centre, storage, server clustering and synchronous to provides high availability in the two sites. If the primary site is unavailable, the PP will continue to operate in the secondary site to achieve the set DR objective. There will be a replicated virtual machine that will automatically failback to the secondary site when the primary site becomes unavailable which makes recoverability easier (Eliot.S,2023)
r.



ACTIVE-ACTIVE SITE For DR Solution.

Recommended Cloud Platform and Vendor Lock-in:

The multi-Cloud Service Provider (CSP) is the ideal for an Active-Active DR solution to avoid cases of data corruption and vendor errors however, we recommend single CSP that is on different operating zone. This is because Multi CSP is costly and PP’s available capital and market-share in the new digital business model is low. The cluster can be hosted in Oracle as it provides hybrid infrastructure services.

The following factors are important in selecting a vendor:

- Data portability: PP need to ensure the vendor allows easy portability of data in readable format in the event of switch-over when their database grows and the current CSP's capabilities is not suitable.
- Interoperability: It is critical to ensure the vendor's infrastructure has the interoperability to link with other vendors. Interoperability between cloud layers needs standardized APIs to allow higher cloud layer exchange and interact.
- Standardization: supports applications among cloud service providers to interoperate with one another, exchange and cooperatively interact with data as well as protocol for joint coordination and control. It is critical for PP to evaluate vendor's compliance with standardization before utilization of its application.
- Service Level Agreement (SLA): PP needs to pay attention to all the terms and conditions in the SLA especially on service availability of 24/7/365, smooth exit in the event of dissatisfaction and exclusivity service clauses to avoid vendor lock-in challenges.
- Open-Source Technologies: PP can also consider option of open-source technology. This is where they are free to use, modify and are not dependent on a single provider. It increases the degree of control an organisation has over its technological stack and reduces the challenge of relying on one source.

Conclusion

The Monte Carlo assessment provides quantitative insights into the potential financial impacts of identified risks, guiding the company in risk management and resource allocation. Also, the simulation assists in better understanding of PP operational systems and probability of the uncertainty events. An adequate DR strategy which is a subset of Business continuity plan and CSP with all the key success factors of vendor lock-in considered, will position PP new business model in a trajectory and competitive edge.

References

1. Oracle WMS Cloud Product Team (2023). Oracle Warehouse Management Cloud. Available from: https://docs.oracle.com/en/cloud/saas/warehouse-management/23b/owsec/security-guide.pdf [Accessed October 20 2023].

2. University Essex Lecture Cast unit 9. Business Continuity and Disaster Recovery**,** Available from: https://www.my-course.co.uk/mod/scorm/player.php?scoid=23630&cm=853366&currentorg=articulate_rise&display=popup[Accessed 6 October 2023]
3. Kanikicheria ,P.(2020). Disaster Recovery strategies in Cloud or in general. Available from: https://prashix.medium.com/disaster-recovery-strategies-in-cloud-or-in-general-c1a01f192a3[Accessed 07 October 2023 .
4. Microsoft Ignite Article 04/14/2023**.**Azure Virtual Desktop disaster recovery concepts .Available from: https://learn.microsoft.com/en-us/azure/virtual-desktop/disaster-recovery-concepts[access [Accessed 10 October 2023].
5. EC-Council Cybersecurity Exchange (2022)What Are the Top 5 Cloud Computing Security Challenges?. Available from :https://www.eccouncil.org/cybersecurity-exchange/cloud-security/what-are-the-security-challenges-in-cloud-computing/#:~:text=Common%20Cloud%20Computing%20Security%20Risks&text=Security%20system%20misconfiguration,Unsecure%20access%20control%20points [Accessed 08 October 2023].

6. Geeks (Jan 27, 2023). Vendor Lock-in in Cloud Computing. Available from:https://www.geeksforgeeks.org/vendor-lock-in-in-cloud-computing/ [Accessed 05 October 2023].

7. Morrow. el at (2021), Carnegie Mellon University Software Engineering Institute, Cloud Security Best Practices Derived from Mission Thread Analysis. Available from: https://apps.dtic.mil/sti/pdfs/AD1139951.pdf[Accessed 08 October 2023].

8. Opera-Martins et al (2014). International Conference on Information Society (i-Society 2014) Critical Review of Vendor Lock-in and Its Impact on Adoption of Cloud Computing. Available from:https://eprints.bournemouth.ac.uk/22467/1/Critical%20Review%20of%20Vendor%20Lock-in%20and%20Its%20Impact%20on%20Adoption%20of%20Cloud%20Computing.pdf [Accessed 04 October 2023]