BUSINESS CONTINUITY/ DISASTER RECOVERY (DR) SOLUTION

With the decision to migrate the Pampered Pets business to a digitised model, it is necessary that the online shop is available 24/7/365. In addition to the shop being moved online, there will be several automated Warehouses as well as new alliances with International Supply Chain partners. Communication between these entities is vital.

The current business model is not reliant on complex IT services, and therefore, the current staff are not qualified or experienced enough to provide the required level of services. To that end, partnering with a Cloud Service Provider (CSP) (TechTarget, ND) is recommended. Compared to the existing setup, this is a major increase in business costs.

The Cloud deployment should be implemented in a Software as a Service (SaaS) model, where the CSP is responsible for all hardware, software, security, applications, and website hosting.

We would suggest that Pampered Pets stays with one of the market leading CSPs (Gartner, 2021), as they cater for small/medium businesses, and all have a flexible payment policy.

Recommended CSP platforms – Amazon (AWS), Google (GCP) or Microsoft Azure.

This reliance on online connectivity, makes it essential that a business continuity (BC) / Disaster Recovery (DR) strategy is developed and implemented.

Whilst designing a strategy for a BC/DR plan, there are 2 factors that are typically considered – Recovery Time Objective (RTO) and Recovery Point Objective (RPO) (Acronis, 2020).

RPO is the amount of data that can afford to be lost during an incident, before causing significant harm to the business. This is measured in time. In Contrast, RTO is the amount of time that an application or system can be unavailable, before causing significant harm to the business – also measured in time.

The requirements from the business are extremely strict, both RTO and RPO are less than a minute, so we must implement a high-availability Active/Active solution. All 3 recommended CSPs can also provide DRAAS (Disaster Recovery as a Service). To ensure business continuity during an incident, the CSPs should be asked to implement a multi-site redundant deployment in separate Cloud Data Centres (DC), A Zone-to-Zone DR that replicates across short distances and will have low latency and yield a low RPO.

Based on the failover requirements, this level of service requires that any applications/databases hosted, are continuously replicating data between the DCs to remain in sync. During an incident, automatic failover between the locations will occur almost immediately with minimal loss of data.

There is a risk that with the DCs being so close together, that a single geographical event could affect the availability. It is possible to implement geographically separate DCs in the Cloud, but replication, latency, and failover timings would be affected. Figure 4.1 below illustrates a high-level diagram of the architecture.

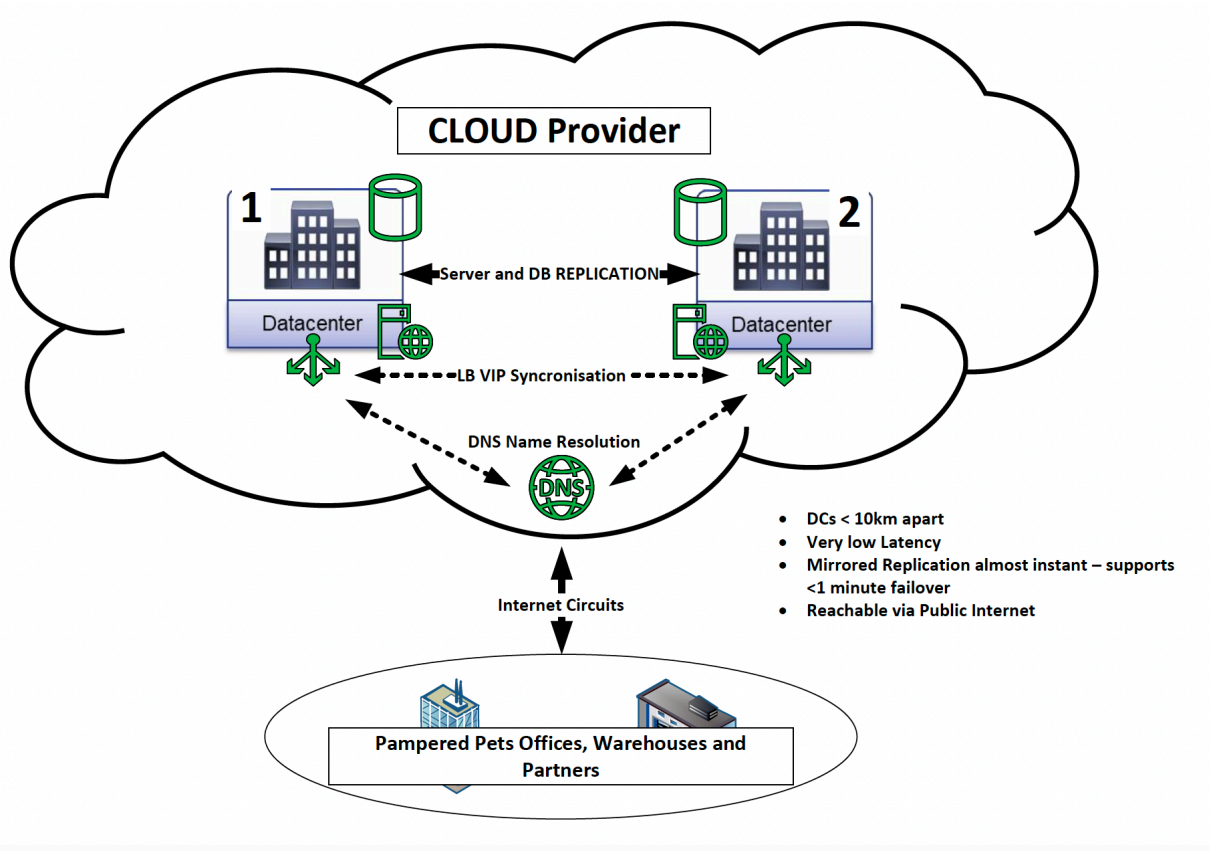

Figure 4.1 High level CLOUD Deployment Design.

As with all Cloud deployments, there is a risk of vendor lock-in (Cloudflare, ND), (Shinwari et al, 2018). If the data is stored in a particular CSP in a vendor-specific format, or a bespoke vendor application, it can be difficult to move away in the future without considerable rework and cost. To avoid this situation, it is recommended to use only open-standard and commonly available applications, APIs, Protocols, and data formats that would allow for the customer to change CSP more easily in the future.

A multi-cloud solution at this stage with different CSPs, would add unnecessary complexity. Regardless which CSP is chosen, they must ensure that they follow the

relevant data protection rules and standards of all the countries where Pampered Pets are operating.

Finally, with the proposed IT operation being Cloud based, it is recommended that redundant internet circuits be implemented for resilience.

REFERENCES

Guevara, P. (2022) *A Guide to Understanding 5x5 Risk Matrix.* Secure Culture. Available from: https://safetyculture.com/topics/risk-assessment/5x5-risk-matrix [Accessed 15 October 2022].

Raghavan, K., Desai, M., Rajkumar, P. (2017) *Managing Cybersecurity and e-Commerce Risks in Small Businesses*. Available from: http://ibii-us.org/Journals/JMSBI/V2N1/Publish/V2N1_2.pdf [Accessed 18 October 2022].

TechTarget, (ND). *Cloud Service Provider*. Available from: https://www.techtarget.com/searchitchannel/definition/cloud-service-provider-cloud-provider [Accessed 12 October 2022].

Gartner, (2021) *Magic Quadrant for Cloud Infrastructure and Platform Services*. Available from: https://www.gartner.com/doc/reprints?id=1-271OE4VR&ct=210802&st=sb [Accessed 12 October 2022].

Shinwari, N., Nasrullah, S., Sharma, N. (2018) *Vendor Lock-In Situation in Cloud Computing.* Available from: https://www.researchgate.net/profile/Neeta-Sharma-7/publication/329586396_VENDOR_LOCK-IN_SITUATION_IN_CLOUD_COMPUTING/links/5c10e329a6fdcc494fede43c/VENDOR-LOCK-IN-SITUATION-IN-CLOUD-COMPUTING.pdf [Accessed 12 October 2022].

Acronis, (2020) *RPO and RTO – definition and understanding the difference*. Available from: https://www.acronis.com/en-us/blog/posts/rto-rpo/ [Accessed 12 October 2022].

Cloudflare, (ND) *What is vendor lock-in? Vendor lock-in and cloud computing*. Available from: https://www.cloudflare.com/en-gb/learning/cloud/what-is-vendor-lock-in/ [Accessed 12 October 2022].