The introduction of digitalization in the pet pampering business brings transformative opportunities, but assessing potential risks to product quality and supply chain security is essential. While we anticipate improved operational efficiency and enhanced customer experiences, conceivable threats exist.

Product Quality:

1. *Quality Degradation (Low Probability):* However, introducing digital systems introduces the risk of technical failures or data breaches. These incidents, though unlikely, could negatively impact product quality by disrupting critical operations or compromising the health and safety of pets.

Supply Chain Security:

1. *Cybersecurity Threats (Moderate Probability):* Adopting digital tools and data storage exposes us to cybersecurity threats. There is a moderate risk of data breaches, which could compromise the integrity of our supply chain, leading to potential disruptions in product availability.

Expected Monetary Value (EMV): (Gunasekaran and Janani, 2021)

Step 1: Define Risks and Probabilities

1. **Risk 1: Quality Improvements**
    - Probability: 0.7 (70% chance of quality improvements)
    - Impact Magnitude: $100,000 (expected annual revenue increase)
1. **Risk 2: Quality Degradation**
    - Probability: 0.1 (10% chance of quality degradation)
    - Impact Magnitude: -$50,000 (potential annual loss)
1. **Risk 3: Enhanced Supply Chain Security**
    - Probability: 0.6 (60% chance of enhanced security)
    - Impact Magnitude: N/A (positive impact)
1. **Risk 4: Cybersecurity Threats**
    - Probability: 0.3 (30% chance of cybersecurity threats)
    - Impact Magnitude: -$200,000 (potential annual loss)

Step 2: Calculate EMV for Each Risk

To calculate the EMV for each risk, multiply the probability by the impact magnitude:

1. **EMV for Quality Improvements:**
2. EMV = 0.7 x $100,000 = $70,000

3. **EMV for Quality Degradation:**
4. EMV = 0.1 x -$50,000 = -$5,000
5. **EMV for Enhanced Supply Chain Security:**
6. Since this risk has a positive impact, the EMV is inherently positive.
7. EMV = 0.6 x (Positive Impact Magnitude) = $X (positive value)
8. **EMV for Cybersecurity Threats:**
9. EMV = 0.3 x -$200,000 = -$60,000

Step 3: Calculate Total EMV

Total EMV = EMV (Quality Improvements) + EMV (Quality Degradation) + EMV(Enhanced Security) + EMV(Cybersecurity Threats)

Total EMV = $70,000 - $5,000 + $X - $60,000 = $5000

Step 4: Decision Making

- Since the Total EMV is positive (indicating a net gain), digitalization is expected to have a positive financial impact.

Choosing Expected Monetary Value (EMV) as a risk analysis technique in the context of digitalization's impact on a pet pampering business offers several advantages:

1. **Quantitative Assessment:** By assigning numerical values to probabilities and impact magnitudes, EMV provides a quantitative assessment of risks. This makes comparing and prioritizing risks more manageable based on their financial implications.
2. **Financial Focus:** EMV focuses on the financial aspect of risks, helping decision-makers understand the potential monetary consequences of different scenarios. This is particularly valuable for businesses that must justify investments and allocate resources effectively.
3. **Scenario Analysis:** EMV allows us to assess multiple scenarios by considering various probabilities and impact magnitudes. This flexibility lets you explore different risk mitigation strategies and their potential outcomes.
4. **Objective Decision-Making:** EMV analysis provides an objective basis for decision-making. It reduces reliance on subjective assessments and biases, helping stakeholders make more rational and data-driven choices.

Summary of EMV-Based Quantitative Modeling Results and Recommendations (Walke, Topkar and Matekar, 2011)

Risk of Loss of Quality:

The Expected Monetary Value (EMV) analysis for potential loss of quality in the pet pampering business due to digitalization yields the following insights:

1. Probability of Quality Improvements (PQI): The probability of quality improvements, ranging from 0.6 to 0.8 (triangular distribution), suggests a moderate likelihood of quality enhancements due to digitalization.
2. Probability of Quality Degradation (PQD): The probability of quality degradation, varying from 0.05 to 0.15 (triangular distribution), indicates a low but non-negligible risk of quality degradation.

Recommendations for Managing Quality Risks:

- Continuous Monitoring: Implement a rigorous monitoring system to track changes in product quality and ensure that digitalization efforts lead to improvements.
- Quality Control Measures: Establish quality control protocols to maintain and enhance the quality of pet pampering services and products.

Risk of Supply Chain Issues:

The EMV-based analysis for potential supply chain issues in the pet pampering business due to digitalization provides the following insights:

1. Probability of Enhanced Supply Chain Security (PSCS): The probability of enhanced supply chain security, ranging from 0.5 to 0.7 (triangular distribution), suggests a moderate likelihood of improved security in the supply chain.
2. Probability of Cybersecurity Threats (PCT): The probability of cybersecurity threats, varying from 0.2 to 0.4 (triangular distribution), indicates a moderate risk of cybersecurity threats affecting the supply chain.

List of Potential Supply Chain Issues:

- Data Breaches: Risk of unauthorized access leading to breaches, potentially compromising customer information and operational data.

- Supply Chain Disruptions: Risk of cyberattacks disrupting supply chain operations, resulting in delays in product delivery or interruptions in the availability of pet care products.
- Counterfeit Products: Risk of counterfeit pet products entering the supply chain, potentially damaging product quality and reputation.

Recommendations for Managing Supply Chain Risks:

- Cybersecurity Measures: Secure your supply chain against data breaches and disruptions.
- Supply Chain Monitoring: Develop and deploy supply chain monitoring systems to detect and mitigate the risk of counterfeit products entering the supply chain.
- Contingency Planning: Establish a comprehensive contingency plan to respond effectively to supply chain disruptions caused by cybersecurity threats.

In summary, the EMV-based quantitative modeling underscores the importance of balancing digitalization's potential benefits and risks in the pet pampering business. While opportunities for quality improvement and enhanced supply chain security are promising, diligent monitoring, quality control, cybersecurity measures, and contingency planning are essential to ensure the success of the digitalization strategy while safeguarding product quality and supply chain integrity.

Moreover, a robust cybersecurity framework and contingency planning must be prioritized to ensure that the digitalization of our pet pampering business maximizes benefits while minimizing risks. The probability of quality improvements and enhanced supply chain security is promising, but vigilance is necessary to safeguard against potential quality degradation and cybersecurity threats. By addressing these challenges proactively, we can confidently move forward, maintaining our world-famous product quality and the security of our supply chain. (Sørensen, 2018)

Client Requirements

- The online shop needs to be available 24/7/365
- with a less than 1-minute changeover window should DR need to be invoked.
- The business can only afford to lose up to 1 minute of data.
- Recommend the platform that should be chosen to host the solution and provide advice on vendor lock-in.

The BC plan deals with plans and procedures to ensure that the business and its staff can continue to operate in as close to the usual way as possible.

Disaster Recovery (DR):

Two factors drive the DR plan and design:

- The Recovery Time Objective (RTO)
- The Recovery Point Objective (RPO)

DR solutions can vary in scope and complexity by a vast amount – anything from an essential backup tape to a complete hot standby system can constitute a DR solution – which is chosen by the RTO, RPO, and the cost requirements. From the client requirement specified above, it can be deduced that the RTO is 1 minute and the RPO is not more than 1 minute.

The ISO 22301 standard for Business Continuity recommends that a business:

- Undergoes a risk assessment.
- Undergoes a business impact analysis.
- Selects a BC strategy.
- Creates and implements policies and procedures.
- Performs regular tests to ensure that the strategy is appropriate.
- Ensures that plans operate as expected.

Adhering to the standard gives customers trust and confidence in a company, knowing that it has plans in place to deal with emergencies and that it will be able to continue to do business even if a disaster should occur.

A Disaster Recovery plan is an integral part of any BC plan and can be analyzed thus:

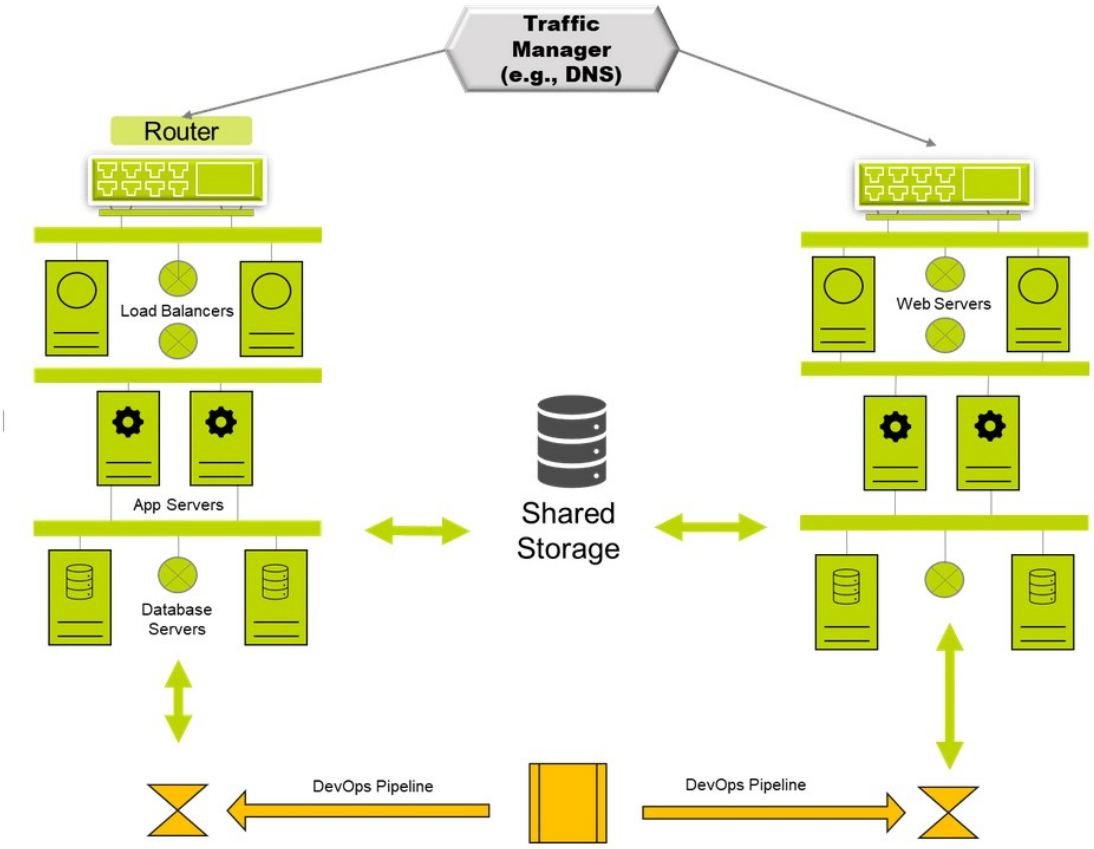

Fig:

DR Strategy

The figure above employs an active-active approach, which suggests that two systems should be running concurrently - ideally in different regions (or one on-premise and one in the cloud). There should be a traffic manager [TM] managing the front-end traffic and monitoring both systems to detect if either fails or automatically switches over to the second without disrupting the user. Code will be deployed to both sites simultaneously. There is an option to use a blue-green deployment strategy where all users are switched over to one site to test the new

code, while the second site is held at the older version in case there are user errors with the new code.

Databases should be configured as AOAG groups or use Cosmos DB in multi-master mode. Any other data should be copied synchronously between sites. Ideally, applications should be deployed in stateless containers, and all user-states should be managed via the database.

The downside of this approach is cost in that the business will be paying for two complete systems and potentially only using one. However, suppose applications are configured to be stateless. In that case, there is no reason why both sites cannot be used simultaneously – the TM can easily allocate users to both systems on a round-robin basis.

The system is highly recoverable since both sites run identical systems, and if one site fails, all users can be switched to the other.

The table below analyzes the efficiency of the active–active approach as a suitable DR strategy for the system under review:

CATEGORY	PROS	CONS	CAVEATS
Availability	Active-active provides immediate, tested always on service.	Cost of additional environments.	Applications must be designed to be active-active ready.
Recoverability	Synchronous copies mean fast, highly recoverable service.	Recoverability by definition in paired regions.	Need additional solution to cope with data corruption - sync copies will just copy corruption.
Resilience	Always on solution means that every component is replicated and always available - may reduce cost by not duplicating within region.	May require switch over to alt region.	Loss of a region will affect resilience; doesn't solve corruption issue.
Data Corruption	Small replication delays may help address corruption risks.	Replication delays mean data loss and higher RPO.	Needs careful tuning to mitigate corruption and avoid data loss.
Regions	Single vendor may make replication and switching easier.	Vendor errors may affect ALL regions - DR will not help.	Consider the multi-vendor solution - more complex, possibly higher cost.

Disaster Recovery (DR) Solution can be summarized as follows:

1. Data Backup and Replication:
    - Based on the client's requirement, the system should implement real-time data backup and replication to ensure that no more than 1 minute of data is lost. This can be achieved by using technologies like continuous data protection (CDP) or synchronous data replication.
    - Cloudification over on-premises data handling; using multiple suppliers to eliminate data lock-in, design lock-in, and faults from having a single supplier. Subscribing to multiple suppliers also ensures reliability.
2. Geographically Redundant Data Centers:
    - All applications and data used will be hosted in geographically redundant data centers to minimize the risk of a disaster affecting both locations simultaneously.
3. Load Balancers and Failover:
    - Utilize load balancers and automatic failover mechanisms to ensure high availability. This will help in achieving the less than 1-minute changeover window if DR needs to be invoked.
4. Regular Testing:
    - Regular testing of the Disaster Recovery plan will be done to ensure it functions as expected. Both planned and unplanned tests will be carried out to assess the readiness of the system.
5. Data Encryption:

The system will also Implement strong data encryption and security measures to protect sensitive information during data replication and storage.

6. Off-Site Backups:
    - To safeguard data in case of a major disaster that affects the primary and secondary data centers, we can take advantage of off-site backups.

Platform Selection:

When choosing a platform to host the DR solution, the following factors should be considered:

1. Cloud Service Providers:

- Cloud service providers such as Amazon Web Services (AWS), Microsoft Azure, or Google Cloud Platform (GCP) should be explored. These providers offer extensive infrastructure and DR services.

2. Hybrid Approach:
    - A hybrid approach can also be considered by utilizing a combination of on-premises infrastructure and cloud services. This provides flexibility and redundancy.
3. Data Center Providers:
    - If cloud services (which are preferred) are not suitable or in line with budgetary plans, data center providers that offer colocation services, which allow you to host your own infrastructure in their facilities can be explored.
4. Service Level Agreements (SLAs):
    - It is also important to evaluate the SLAs provided by potential platform providers, to ensure they meet the 24/7/365 availability and less than 1-minute changeover window requirements.

Addressing Vendor Lock-In:

Vendor lock-in can be a concern when using third-party platforms. To mitigate this risk:

1. Multi-Cloud Strategy:
    - The recovery system should adopt a multi-cloud strategy, spreading the data services and applications across multiple cloud providers. This reduces dependence on a single vendor and ensures reliability.
2. Standardized Interfaces:
    - The system should ensure that all applications and services use standardized interfaces and APIs. This makes it easier to migrate between platforms if necessary.
3. Data Portability:
    - Keep data portability in mind. This is to ensure data can be easily transferred from one platform to another.
4. Vendor-Neutral Tools:
    - Where possible, vendor-neutral management and orchestration tools should be used, to maintain flexibility in managing services and resources.
5. Regular Evaluation:

- To keep up with current market competition, it is important to periodically evaluate the performance and cost-effectiveness of your chosen platform to determine if a change is needed.

REFERENCES

Morrow, T., LaPiana, V., Faatz, D., Hueca, A. & Richmond, N. (2021) *Cloud Security Best Practices Derived from Mission Thread Analysis.* Carnegie-Mellon Univ Pittsburgh PA.

Opara-Martins, J., Sahandi, R., & Tian, F. (2014) Critical review of vendor lock-in and its impact on adoption of cloud computing. *In International Conference on Information Society* (i-Society 2014) (pp. 92-97). IEEE.

Alhazmi, O. & Malaiya, Y. (2013) Evaluating Disaster Recovery Plans using the Cloud. *2013 Proceedings Annual Reliability and Maintainability Symposium* (RAMS) 1(1): 1-6

Andrade, E., Nogueira, B., Matos, R., Callou, G. & Maciel, P. (2017) Availability modeling and analysis of a disaster-recovery-as-a-service solution. *Computing*, 99(10), pp.929–954

Olson, D.L. & Desheng D.W (2020) *Enterprise risk management models*. Berlin, Germany: Springer.

Gunasekaran, S. and Janani, C. (2021) ‘Multidisciplinary Research- Vol2 (3) (1)’, in, p. 978 93 90996 57 5.

Sørensen, B.T. (2018) ‘Digitalisation: An Opportunity or a Risk?’, *Journal of European Competition Law & Practice*, 9(6), pp. 349–350. Available at: https://doi.org/10.1093/jeclap/lpy038.

Walke, R.C., Topkar, V.M. and Matekar, N.U. (2011) ‘An Approach to risk quantification in construction projects using EMV analysis’, *International Journal of Engineering Science and Technology*, 3(9).