“Inadequate Data Backup Redundancy and Disaster Recovery Preparedness”

MD 3

IT PROJECT MANAGEMENT & SCHEDULING

Table of Contents

1. Quality management plan:

Quality Management Checklist

S.no	Quality Metric	Description	Measures to be taken
1	Data Integrity	All data stored in the cloud should be accurate, complete, and consistent with the organization's original data sources.	1. Implement data validation and cleansing procedures to ensure the accuracy and consistency of data before migration to the cloud storage system. 2. Establish data quality governance processes to maintain data integrity throughout its lifecycle. 3. Employ data integrity monitoring tools to detect and address data anomalies or corruption. 4. Conduct regular data audits to verify data quality and adherence to established standards.
2	Data Availability	Data should be readily accessible to authorized users when needed, with minimal downtime or interruptions.	1. Implement redundant data storage mechanisms, such as mirroring or replication, to ensure data availability in case of hardware failures or disruptions. 2. Employ high availability cloud storage services with built-in failover mechanisms to maintain data accessibility. 3. Establish disaster recovery procedures to restore data and system functionality in the event of a major outage. 4. Monitor system performance and uptime metrics to identify and address potential availability issues promptly.

3	Data Security	Data should be protected from unauthorized access, use, disclosure, disruption, modification, or destruction through appropriate security measures and access controls.	1. Implement strong access controls, including role-based access permissions, multi-factor authentication, and data encryption, to protect sensitive data from unauthorized access. 2. Employ data encryption techniques to safeguard data at rest and in transit. 3. Conduct regular security audits and penetration testing to identify and remediate vulnerabilities. 4. Educate users on data security best practices and raise awareness of potential threats.
4	Data Recovery	In case of a disaster or data loss, the cloud should have robust data recovery mechanisms in place to restore lost or corrupted data.	1. Establish regular data backup routines to create multiple copies of critical data for recovery purposes. 2. Utilize offsite data backup solutions to safeguard data in case of a localized disaster at the primary data centre. 3. Implement data recovery procedures that can restore lost or corrupted data from backups efficiently. 4. Test data recovery procedures regularly to ensure their effectiveness.
5	System Performance	The cloud should meet the organization's performance requirements in terms of speed, responsiveness, and scalability to handle	1. Perform thorough load testing and capacity planning to ensure the cloud storage system can handle the organization's data volumes and usage patterns.

		increasing data volumes.	2. Optimize data storage configurations and utilize caching mechanisms to enhance system performance. 3. Employ cloud storage services with scalable architecture to accommodate future growth in data volumes. 4. Monitor system performance metrics, such as response times and throughput, to detect and address performance bottlenecks.
6	User Satisfaction	Users should be satisfied with the functionality, usability, and overall performance of the new cloud storage system.	1. Conduct user surveys and feedback sessions to gather insights into user satisfaction levels and identify areas for improvement. 2. Establish user support channels to provide prompt assistance and address user concerns effectively. 3. Implement user training programs to educate users on the new cloud storage system's features and functionality. 4. Continuously monitor user adoption rates and address any usability issues that hinder user satisfaction.
7	Training Effectiveness	Users should receive comprehensive training on how to use the new cloud system effectively and efficiently, minimizing adoption challenges.	1. Develop comprehensive training materials and modules that cover all aspects of the new cloud storage system. 2. Employ a variety of training methods, such as hands-on workshops, online tutorials, and user guides, to cater to different learning styles.

			3. Provide ongoing training opportunities and support to ensure users stay up to date with the latest features and functionalities. 4. Conduct post-training assessments to evaluate user knowledge and identify areas for further training.

2. Staffing management plan:

Responsibility Assignment Matrix (RAM)

Role / Task	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Project Manager	R, P	R, P	R, P												R, P
Systems Analyst			R, P			R, P	R, P	R	R			R, P	R		
Database Designer				R, P	R, P			R, P		R, P		P			
Cloud Engineer				R, P	R, P	R, P			R, P	R, P		R, P	R, P		
Trainer														R, P	
Construction team/Contractor															
QA											R, P	P			
Network and Infrastructure Engineer							R, P	P	P	R, P		P	P		

R = Responsible organizational unit P= Performing organizational unit

WBS Task Dictionary

Task ID	Task
1	Project Planning and Initiation
2	Project Plan and Communication Plan
3	Requirement Gathering
4	Designing of physical and virtual servers
5	Cloud architecture setup
6	Establish network setup.

7	Firewall Setup
8	Backing up the current environment before migrating
9	Migrate the application servers to the VMware environment.
10	Developing the network specifications
11	Testing servers in test environment
12	Piloting some of the selected users on the test environment
13	Disaster Recovery Plan Testing
14	User acceptance and training
15	Go live and lessons learned

RACI Chart:

Below is the breakdown of the RACI roles:

1. **Responsible (R):** The person who is responsible for completing the task.
2. **Accountable (A):** The person who is ultimately accountable for the success or failure of the task.
3. **Consulted (C):** The people who should be consulted before the task is completed.
4. **Informed (I):** The people who should be informed of the progress or outcome of the task.

Task	Project Manager	Systems Analyst	Database Designer	Cloud Engineer	Trainer	QA	Network and Infrastructure Engineer
Planning	R, A, I	C, I	C, I	C, I	C, I	C, I	C, I
Analysis	A, I	R	C, I	C, I			C, I
Design	A, I	C, I	R, C	R		I	R, C
Implementation	A, I	C, I	C, I	R	I	I	R, C
Testing	A, I	I	I	C, I	I	R	C, I
Training	A, I	C, I	C, I	C, I	R	C, I	C, I

3. Risk Management plan:

Risk Register

No.	Risk	Description	Likelihood	Impact	Mitigation Strategy
1	Data Loss	Data could be lost due to hardware failure, software corruption, or human error.	Medium	High	Implement regular data backups and disaster recovery procedures, including offsite backups and data replication.
2	Unauthorized Access	Sensitive data could be accessed by unauthorized users.	Low	Medium	Implement strong access controls, including multi-factor authentication, role-based access permissions, and data encryption.
3	Data Corruption	Data could be corrupted due to viruses, malware, or human error.	Medium	Medium	Implement anti-virus and anti-malware software, data integrity checks, and regular data validation processes.
4	System Outage	The cloud storage system could go down, causing data loss and disruption to business operations.	Low	High	Implement a high availability solution, such as a redundant cloud storage system or failover mechanisms, to ensure continuous data access.
5	Cost Overruns	The project could cost more than expected due to unforeseen expenses or changes in cloud storage provider pricing.	Medium	Medium	Develop a detailed project budget, carefully track expenses, and consider contingency plans for cost overruns.

6	Project Delays	The project could take longer than expected to complete due to unforeseen challenges or delays in implementation.	Medium	Medium	Develop a detailed project schedule, carefully monitor progress, and identify potential risks that could impact project timelines.
7	Technical Challenges	There could be technical challenges implementing or integrating the cloud storage system with existing systems.	Medium	Medium	Conduct a thorough feasibility study, carefully select the cloud storage provider, and involve IT personnel in the implementation process.
8	User Resistance	Users may resist the change to the new cloud storage system due to unfamiliarity or fear of change.	Low	Medium	Develop a comprehensive training program, provide ongoing support, and communicate the benefits of the new system effectively.
9	Regulatory Compliance	The cloud storage system may not comply with all applicable data privacy regulations or industry standards.	Low	Medium	Conduct a thorough legal review, implement compliance measures, and choose a cloud storage provider that adheres to relevant regulations.
10	Change Management	The change to the new cloud storage system may disrupt business operations and cause workflow disruptions.	Low	Medium	Develop a change management plan, communicate the changes effectively to stakeholders, and provide support during the transition.

Probability/Impact Matrix.

Sl no	Likelihood	Impact
1	Very Low	Insignificant
2	Low	Minor
3	Medium	Moderate
4	High	Major
5	Very High	Catastrophic