**Group Assignment**

**Topic: IT Disaster Recovery and Business Continuity Planning**

**Table of Contents**

|  |  |
| --- | --- |
| **Group members** | **3** |
| **Introduction** | **4, 5** |
| **Project Charter** | **6, 7** |
| **Gantt chart** | **8** |
| **Risk and issues management strategy** |  |
| **Screenshots** |  |
| **Conclusion** |  |
| **Reference** |  |

**Group Members**

|  |  |  |  |
| --- | --- | --- | --- |
| ID | Name | Email | Tasks |
| 61085 | Osman Akif  Barut | os61085@student.vit.edu.au | Project Charter,  Gantt chart |
| 65358 | Asfi Amman  Oytizzho | as65358@student.vit.edu.au | Risk and issues management strategy |
| 61835 | Muhammad Hamaet  Uddin | mu61835@student.vit.edu.au | Conclusion |
| 45673 | Vincent  Wijaya | vi45673@student.vit.edu.au | Version Control |
| 64722 | Isanka Anjana Munasinghe | is64722@student.vit.edu.au | Introduction |

**Introduction**

In today’s monetary field, which functions largely through information technologies, an inclusive IT Disaster Recovery and Business Continuity Plan is more than best practice—it is critical need. Since banking systems manage large volumes of data on customers, must execute transactions in real time, and handle various regulations, a single point of failure can disrupt operations badly. It can be a cyberattack, a simple hardware failure; even human error or natural disaster can lead to huge disruption in operations, loss of money, and damage to the reputation.

This report elaborates a structured project plan to develop and **implement IT Disaster Recovery and Business Continuity Planning for a banking environment**. The plan is to ensure the bank maintain or be able to resume critical operations within a short period in the face of unforeseen disruptions. It shall focus on potential risks to be identified, and the related response and recovery procedures to be defined, plus technologies and protocols supporting system resilience and continuity to be implemented.

The report has major components:

* A wide scope statement that spells out the project’s objectives, deliverables, boundaries, assumptions, and constraints.
* A Gantt chart showing the timeline and milestones of the project activities and tasks with interdependencies.
* A risk and issues management strategy detailing how to identify, assess, and mitigate risks likely to affect either success on this project or operational continuity for the bank.
* A change request management process that gives a clear structure for handling changes in project scope, resources, and timelines making sure that any modifications are noted assessed and approved in a systematic way.
* The use of a configuration management tool like GitHub to handle version control help teamwork among project members make sure transparency and traceability all through the project lifecycle.

Through the amalgamation of technical planning with governance and operational safeguards, the project seeks to enhance the bank’s capacity to manage shocks and recover in the event of IT-related disruptions. In doing so, it will also bring the bank in line with explicit regulatory expectations and industry standards on business continuity and disaster recovery, not to mention improve the bank’s resilience.

This project report acts as a plan of strategy for the stakeholders and project members, outlining a path to follow in the process of implementation while setting a structure for continuous assessment and enhancement.

Project Charter

Project Title: IT Disaster Recovery and Business Continuity Planning for a Banking System

Objectives:

To create and carry out an IT Disaster Recovery and Business Continuity Plan for a banking system that can be measured and follows the rules;

* Recovery Time Objective (RTO) <6 hours
* Recovery Point Objective (RPO) <1 hour
* Zero data loss during disruption
* Full service restoration within 12 hours after a major outage

Scope:

In Scope

* Business Impact Analysis (BIA)
* Risk assessment and mitigation planning
* Escalation paths and emergency communication protocols
* Design of DR/BC frameworks (including hot/cold site)
* DR drill simulation plan
* GitHub repository with version control

Out of Scope

* Real-time disaster simulation in production
* Hiring of new staff or consultants

Stakeholders and Roles:

Project Sponsor:

* Approves budget, timeline, and major deliverables
* Provides executive-level support
* Resolves scope or resource escalations

Project Manager:

* Oversees entire project execution and timeline
* Coordinates between team roles
* Ensures tasks are completed according to Gantt Chart and scope

Technical Lead:

* Designs disaster recovery architecture
* Leads cloud backup strategy, recover site setup
* Ensures RTO/RPO targets are technically feasible

Security Officer:

* Conducts risk assessments
* Ensures alignment with cybersecurity standards
* Handles incident response playbook design

Compliance Officer:

* Ensures all processes meet banking regulations
* Maintains documentation for audits
* Verifies backup policies follow legal and data sovereignty requirements

Assumptions

* All team members will contribute a minimum of 5 hours per week
* Sandbox environment is available of DR testing
* GitHub and Jira are approved tools by the sponsor
* No external consultancy will be used due to budget constraints

Constraints

* Must be completed within 3 months
* Total project budget is capped at $10,000
* Only 4 team members are allowed
* Must comply with financial sector regulatory policies

Timeline Overview

* Initiation and planning (1-2 week): Project Scope Document and Risk Register
* Requirement Analysis (BIA) (3-4 week): List of Critical System and Dependency Map
* Strategy Development (5-6 week): DR/BC Framework and Backup plan
* Gantt and Risk Management Plan (7-8 week): Gantt Chart, Risk Matrix and Mitigation Plans
* Testing and Validation (9-10 week): DR Drill Simulation Report and Incident Response Logs
* Finalization and Presentation (11-12 week): Final Report, GitHub Repo and Presentation Slides

Success Criteria

* Project deliverables submitted on time and match rubric standards
* GitHub repository includes version history and collaboration records
* Team collaboration evidenced through Jira board and logs
* DRBC framework validated through a successful mock drill

Gantt Chart

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Tasks/Weeks | 1-2 | 3-4 | 5-6 | 7-8 | 9-10 | 11-12 |
| Initiation and Planning |  |  |  |  |  |  |
| Requirement Analysis (BIA) |  |  |  |  |  |  |
| Strategy Development |  |  |  |  |  |  |
| Gantt and Risk Management Plan |  |  |  |  |  |  |
| Testing and Validation |  |  |  |  |  |  |
| Finalization and Presentation |  |  |  |  |  |  |

**Version Control**

As the foundation for preserving code integrity, facilitating quick recovery, & guaranteeing reliability in emergency scenarios, version control systems are an essential part of IT Disaster Recovery and Business Continuity Planning for banking systems. Version control serves as both a preventive & a recovery method for banking infrastructure, protecting the organization's software assets and offering the resources required for a prompt service restoration after any disruptive incident.

First, distributed archive designs that reflect the institution's regional redundancy needs must be established in order to strategically deploy version control inside banking disaster recovery frameworks. To prevent a single point of failure from compromising the entire codebase, modern banking systems usually use distributed version control systems based on Git that keep track of full project histories across several data centers. Because each repository has the complete history of all crucial programs, payment processing systems, and regulatory compliance tools, this distributed method complies with banking laws that require geographically distinct backup systems. In addition to data duplication, the redundancy includes automated synchronization protocols that update distant archives continuously, forming a real-time safety net that may be activated instantly in the event that primary systems fail.

In banking settings, recovery time goals need that version control systems have instant deployment capabilities. This calls for automated deployment pipelines that are incorporated into the disaster recovery plan and complex branching methods. In order to be prepared for various crisis situations, banking organizations usually maintain a number of environment branches, such as production, disaster recovery, and emergency response configurations. Rebuilding complete banking platforms in a matter of minutes as opposed to hours is possible thanks to the disaster recovery branch's pre-configured deployment scripts, database migration tools, as well as system configuration files. With this method, technical teams can deploy known-good versions of all important systems in a crisis without needing to perform a lot of manual intervention or running the risk of introducing untested code in high-stress scenarios.

In banking disaster recovery situations, when regulatory agencies demand thorough documentation of all system modifications & recovery protocols, the audit trail & compliance features of version control become very important. Version control solutions create a thorough audit trail that meets internal governance standards & external regulatory scrutiny by keeping unchangeable records of all code modifications, deployments, & rollbacks. Because it shows the integrity of the recovery process and offers indisputable proof of the institution's adherence to set protocols, this paperwork is extremely helpful during post-incident assessments, regulatory inspections, and legal processes. Version control records' timestamped nature also makes it possible to precisely rebuild system states at any given moment, which aids in forensic analysis and helps pinpoint the underlying reasons for failures.

In banking disaster recovery situations, when regulatory agencies demand thorough documentation of all system modifications & recovery protocols, the audit trail & compliance features of version control become very important. Version control solutions create a thorough audit trail that meets internal governance standards & external regulatory scrutiny by keeping unchangeable records of all code modifications, deployments, & rollbacks. Because it shows the integrity of the recovery process and offers indisputable proof of the institution's adherence to set protocols, this paperwork is extremely helpful during post-incident assessments, regulatory inspections, and legal processes. Version control records' timestamped nature also makes it possible to precisely rebuild system states at any given moment, which aids in forensic analysis and helps pinpoint the underlying reasons for failures.

Version control solutions that are integrated with change management procedures guarantee that they support the strict approval workflows of banking institutions while preserving the adaptability needed for emergency responses. Banking software deployments during regular business hours adhere to stringent change advisory board protocols, which include numerous approval gates and comprehensive testing specifications. Disaster recovery plans, however, require that specific approval processes be circumvented while still ensuring proper supervision & documentation. This balance is made possible by version control systems, which keep thorough records of every action taken in emergency scenarios and offer emergency deployment branches with pre-approved emergency fixes. This two-pronged strategy gives emergency reactions the speed required for efficient disaster recovery while maintaining control & traceability.

Secure communication channels, encrypted storage systems, and automatic backup processes that guard against technical malfunctions and security breaches are all part of the technical architecture that supports version control in banking disaster recovery. Digital signatures for all code commits, encrypted vault communication, and access constraints that limit emergency deployment capabilities to approved individuals are just a few of the multi-layered security mechanisms that banking institutions employ. Version control solutions must preserve the same degree of security as major systems while yet allowing crisis response teams the accessibility they need at disaster recovery sites. Regardless of the type or extent of the disruption impacting the primary infrastructure, the end result is an adaptive framework that can provide recovery teams with essential software resources.

References

[1] Australian Prudential Regulation Authority,

“CPS 232 - Business Continuity Management,” Jul. 2017. [Online].

Available: https://www.apra.gov.au/sites/default/files/CPS\_232\_July\_2017.pdf

[2] International Organization for Standardization,

“ISO/IEC 27031:2011 - Information technology — Security techniques — Guidelines for information and communication technology readiness for business continuity,”

1st ed., ISO, Geneva, Switzerland, 2011. [Online].

Available: https://www.iso.org/standard/44374.html

[3] National Institute of Standards and Technology (NIST),

“Contingency Planning Guide for Federal Information Systems, Special Publication 800-34 Revision 1,”

Jun. 2010. [Online].

Available:https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-34r1.pdf