**Business Continuity Plan**

Based on identified threats such as: database crash, network failure, DDoS attacks, untested code, unauthorized access or insider threats.

I investigate the components and steps of a Business Continuity Plan.

Risk Assessment- I identified threats and documented mitigation strategies for potential pitfalls.

Roles and Responsibilities – assign people to handle key tasks (e.g., Martin backend, Julia fallback UI)

Understanding requirements, stakeholders and dependencies – LLM, MySQL, Flask API  
Business Impact Analysis – determined critical LLM feature and MySQL crash.

**Disaster Recovery Plan**

Backup and recovery – automate backups, use mysqldump daily and test restore.

Disaster Recovery Sites – backup server on different cloud.  
Disaster Recovery Test – MySQL database crash

Scenario: Crash the MySQL database to validate the recovery process.

Expected RTO: < 30 mins

1. Verify MySQL crash detection.

2. Ensure Flask, react.js handles error.

3. Test data backup restore process.

4. Measure RTO (Recovery Time Objective) and RPO (Recovery Point Objective).

To measure Recovery Time Objective (RTO) and Recovery Point Objective (RPO), we should enhance incident logs with timestamps marking the failure and recovery points; in our case, we utilized browser developer tools to observe when routes became responsive. We could further support this by logging request sizes, database activity, and leveraging Flask middleware for detailed request tracking.