# Appendix B: Constraints & Considerations

One of the key constraints when designing the new document management service outside of i-Prompt is downtime. Below is a breakdown of potential downtime scenarios, their causes, and mitigation strategies.

## 1. Potential Downtime Scenarios

|  |  |  |  |
| --- | --- | --- | --- |
| Scenario | Cause | Impact | Mitigation Strategy |
| AWS Service Disruptions | Temporary outage in AWS services (e.g., S3, DynamoDB, API Gateway, Lambda) | Document retrieval, storage, or metadata operations may fail | Use multi-region redundancy, enable DynamoDB Global Tables, and leverage S3 Cross-Region Replication |
| Deployment Downtime | Service updates or infrastructure changes | Temporary unavailability of APIs | Use blue/green deployment or canary releases to minimize impact |
| Network Failures | Issues with AWS Direct Connect or API-C on-prem | API requests may fail due to connectivity loss | Implement retry mechanisms and graceful degradation (e.g., fallback to an alternative region) |
| Data Consistency Delays | Eventual consistency in DynamoDB or replication lags in S3 | Data updates may not be instantly reflected across all services | Use strongly consistent reads where necessary and implement event-driven notifications |
| Security & Access Control Issues | Incorrect IAM policies, expired credentials, or misconfigurations | Users may be blocked from accessing documents | Implement IAM role monitoring, automated policy validation, and logging with AWS CloudTrail |

## 2. Mitigation Strategies for High Availability

To minimize downtime and ensure business continuity, the following strategies should be implemented:

✅ Multi-Region Redundancy – Deploy key services (S3, DynamoDB, API Gateway) across multiple AWS regions.

✅ Failover Mechanisms – Use Route 53 health checks to reroute traffic in case of an API failure.

✅ Retry & Backoff Logic – Ensure API clients retry requests in case of transient failures.

✅ Event-Driven Monitoring – Use AWS CloudWatch Alarms to detect service issues and trigger automated recovery actions.

✅ Disaster Recovery (DR) Plan – Maintain automated backups, replication policies, and failover mechanisms to quickly restore services in case of a major failure.

## Conclusion

While downtime risks exist, a well-architected solution with failover, redundancy, and monitoring will ensure high availability and minimized service disruption for the document management service.