Disaster Recovery Plan — IT Department

(Hybrid IT Environment)

Week 7 Research Paper

Alan B. Palayil

University of the Cumberlands

Course: ITS-834: Emerging Threats & Countermeasures

Instructor: Dr. Michael Grabinski

Date: October 12th, 2025

Abstract

This Disaster Recovery Plan (DRP) lays out a solid foundation for the IT Department of a financial company that uses hybrid IT architecture, which means it uses both cloud infrastructure and on-premises applications. It lays out the steps, roles, and recovery plans for getting ETL applications, databases, accounting systems, files, schedulers, and automation frameworks back up and running after a problem. The strategy makes sure that the firm can keep going, that it follows the rules, and that the data is safe by using dual-database architecture, frequent testing, and a culture of cybersecurity awareness. This DRP follows **ISO/IEC 27031** and **ISO/IEC 24762** and includes initiative-taking planning, organized reaction, and learning from past events to keep financial operations going in the face of technical and environmental challenges.

1. Introduction

The IT Department oversees important financial tasks such transaction processing, closing the books, and reporting to regulators. These businesses need **hybrid IT architecture** that blends **on-premises systems** for sensitive financial data with **cloud-based platforms** for automation and ETL services that can grow with the business.

This DRP gives you a plan for getting these systems back up and running if they go down because of cyber-attacks, hardware issues, or natural catastrophes.

Objectives

- Make sure that operations can continue by getting systems back up and running within the set RTO and RPO limits.

- Keep data safe, private, and in line with financial and regulatory norms.
- Write out defined roles and technical steps for quick recovery from a disaster.
- Encourage a culture of learning in the workplace to make resilience better all the time.

2. System Architecture and Dependencies

The IT ecosystem is **hybrid and redundant**:

- **On-Premises:** Primary database, backup/test database, accounting servers, and file sharing.
- **Cloud:** ETL workloads, automation pipelines, schedulers, and object storage.
- **Interdependencies:** Secure APIs, secrets management (KMS), and centralized authentication (IdP).

Critical Components

System	Hosting	Function	RTO	RPO
Primary IT Database	On-prem	Core trade & position data	2 hours	15 min
Backup/Test Database	On-prem	DR testing and standby replica	4 hours	24 hours
ETL Applications	Hybrid	Data ingestion & transformation	4 hours	30 min
Accounting Applications	Hybrid	Financial reporting & reconciliation	4 hours	1 hour
Scheduler (Airflow/Control-M)	Hybrid	Workflow orchestration	1 hour	N/A
File & Automation Services	Hybrid	Data exchange & reports	2 hours	15 min

3. Roles and Responsibilities

Role	Responsibilities
Incident Commander (IC)	Authorizes plan activation, coordinates communications, and sets recovery priorities.
IT DR Lead	Executes technical recovery procedures; verifies RTO/RPO compliance.
Database Administrator (DBA)	Performs restoration, log replay, and data validation across both databases.
Cloud Operations Lead	Rebuilds ETL clusters and automation pipelines in alternate regions.
Accounting Apps Lead	Restores accounting servers and validate financial data.
Scheduler Owner	Freezes/resumes batch processes and redeploys scheduler instances.
Business Continuity Manager (BCM)	Tracks recovery progress and ensures alignment with enterprise BCP.
Information Security Officer	Validates system integrity, monitors threats, and preserves forensic evidence.

4. Incident Response and Plan Activation

Criteria for Activation

- Ransomware encryption or database corruption.
- Cloud region outage that affects ETL tasks or reporting.
- A protracted failure of the scheduler that stops end-of-day (EOD) procedures.
- Compromised data integrity or access without permission.

First 2-Hour Response Protocol

1. Tell the recovery team and turn on the incident bridge.
2. Keep forensic snapshots of affected servers and keep them separate.
3. Stop the scheduler and file transfers.
4. Start restoring to the Backup/Test Database or a different cloud location.
5. Start doing hourly SitReps until everything is back to normal.

5. Recovery Procedures

5.1 Restoring the Database (Primary → Backup/Test)

1. Stop all writes to the primary database.
2. Check that the most recent complete and log backup sets are correct.
3. Restore the Backup/Test Database and use logs for an RPO of 15 minutes or less.
4. Check the consistency of the data (positions, NAVs, and transactions).

5. Change the connections for the application and ETL to the DR database alias.
6. Make sure the data is correct and the system works well.

5.2 ETL Platform (Hybrid)

1. Pause active pipelines and export the states of the jobs.
2. Use IaC templates to set up clusters in a different location.
3. Get back your passwords, secrets, and mounts from the artifact repository.
4. Run important EOD activities again, such data ingestion, pricing, and NAV.
5. Check to make sure everything is correct against the checkpoints that were set up before the occurrence.

5.3 Accounting Applications

1. Rebuild the servers that were damaged and set up the applications again.
2. Send connection pools to the Backup/Test Database instead.
3. Check the journal entries and financial statements.
4. After verification, start the closure steps again.

5.4 Scheduler and Automation Systems

1. Suspend non-critical jobs and triggers.
2. Launch DR scheduler instance and import latest workflow definitions.
3. Resume priority chains (database restore → ETL → accounting).

4. Reconcile missed tasks and log exceptions.

5.5 File and Storage Systems

1. Restore from immutable backups or cloud object versioning.
2. Scan restored data for malware.
3. Validate checksums before reattaching to applications.
4. Resume automated file exchanges once cleared.

6. Testing, Validation, and Maintenance

Evaluate	**Frequency**	**Scope**	**Success Criteria**
Database Failover Drill	Quarterly	Restore DB to Backup/Test instance	≤2-hour RTO, ≤15-min RPO
ETL Cloud Failover	Semiannual	Deploy alternate region cluster	Jobs complete within 4 hours
Scheduler DR Simulation	Semiannual	Validate workflow migration	100% workflow execution
Full DR Exercise	Annual	End-to-end departmental test	CFO signoff, data variance ≤0.1%

Evaluate	Frequency	Scope	Success Criteria
Backup Integrity Validation	Monthly	Verify random backup samples	100% pass rate

7. Training, Awareness, and Security Culture

IT staff complete **annual cybersecurity and DR training**, including:

- Recognizing phishing and insider threats.
- Using CSIRT channels to report problems.
- Following the rules for communication during DR incidents.
- Taking part in both live and table-top disaster recovery exercises.

This cultural reinforcement encourages responsibility and readiness, which shortens recovery periods and lowers the chance of making mistakes (Back & Guerette, 2021; Ahmad et al., 2020).

8. Review Cycle and Document History

Version	Date	Summary of Change	Author
2.0	[Insert Date]	Added hybrid cloud recovery flow and dual DB failover	[Your Name]
1.0	[Previous Date]	Initial DRP draft for IT systems	[Your Name]

Review Frequency: Every six months or after an SEV-1 occurrence.

Approval: CISO and Business Continuity Manager.

9. Conclusion

This Disaster Recovery Plan makes sure that the IT Department can manage cyberattacks, system failures, and operational interruptions by combining cloud resiliency, database redundancy, and human readiness. The department is ready for a strong comeback while keeping client confidence and regulatory integrity by doing regular tests, having ethical leaders, and following worldwide standards.

Appendix A: Key Contacts

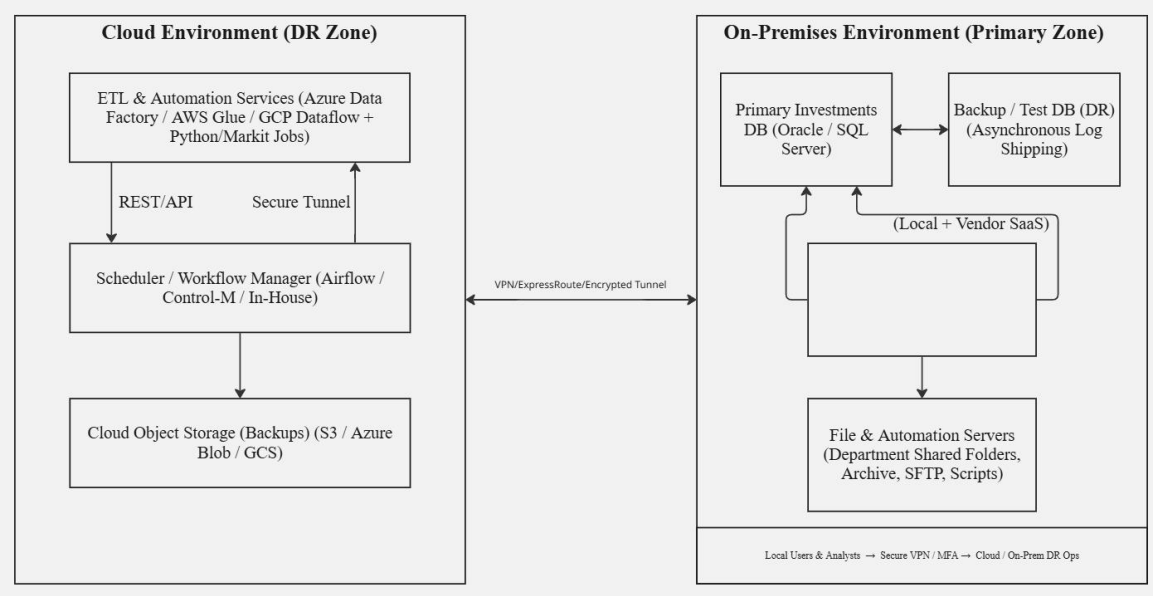
Role	Name	Phone	Email
Incident Commander	[Name]	(555) 010-1200	ic@org.com
IT DR Lead	[Name]	(555) 010-1210	drlead@org.com
DBA Lead	[Name]	(555) 010-1220	dba@org.com
Cloud Operations Lead	[Name]	(555) 010-5555	cloudops@org.com
Accounting Apps Lead	[Name]	(555) 010-1240	acctapps@org.com
Scheduler Owner	[Name]	(555) 010-1250	scheduler@org.com

Role	Name	Phone	Email
BCM	[Name]	(555) 010-3333	bcm@org.com

Appendix B: Runbook Summary

Scenario	Primary Action	Responsible Role
Database Outage	Restore to Backup/Test DB	DBA Lead
Cloud ETL Failure	Deploy alternate region cluster	Cloud Ops Lead
Accounting Server Crash	Rebuild servers, reconnect to DR DB	Apps Lead
Scheduler Failure	Promote DR scheduler instance	Scheduler Owner
File Corruption	Restore from immutable backup	IT DR Lead

Appendix C: Hybrid Architecture Diagram



References

Ahmad, A., Desouza, K. C., Maynard, S. B., Naseer, H., & Baskerville, R. L. (2020). How integration of cyber security management and incident response enables organizational learning. Journal of the Association for Information Science and Technology, 71(8), 939–953. https://doi.org/10.1002/asi.24306

Back, S., & Guerette, R. T. (2021). Cyber place management and crime prevention: The effectiveness of cybersecurity awareness training against phishing attacks. Journal of Contemporary Criminal Justice, 37(3), 427–451. https://doi.org/10.1177/10439862211014120

Brown, M. (2019). Technologies and infrastructure: Costs and obstacles in developing large-scale computer-based testing. Education Inquiry, 10(1), 4–20. https://doi.org/10.1080/20004508.2018.1464428

Kennedy, M., Gonick, S. A., & Errett, N. A. (2021). Are we ready to build back "healthier?" An exploratory analysis of U.S. state-level disaster recovery plans. International Journal of Environmental Research and Public Health, 18(15), 8003. https://doi.org/10.3390/ijerph18158003