Information Systems

Disaster Recovery Test Plan

(Scenario 1 – Loss of Core System)

Dept.	IS
Team	Service Delivery
Author	Rob Hodges
Date	Dd/mm/yyyy
Document Version	Draft V1.0

DOCUMENT CONTROL

Disaster Recovery Test Plan

Owner(s)	Project/Organisation Role

Distribution

Name	Role

Plan Version control

Version	Status	Date	Author	Change description
0.1	Draft	Dd/mm/yyyy	Rob Hodges	New first draft

Plan approved by

Name	Project / Organisation Role	Version	Sign Off Date

Plan location

TABLE OF CONTENTS

1. PURPOSE

The purpose of this document is to define and detail the scope and objectives of the planned "Scenario 1 – Loss of Core System" Disaster Recovery Test Scenario. This event is scheduled to be carried out in Pre-Production and start on dd/mm/yyyy and complete dd/mm/yyyy with testing and validation following Failover and Failback.

Following completion of the Test, a Test Report will be produced.

2. EXECUTIVE SUMMARY

Why

The exercise to failover and failback the Core System Cloud service between the Primary and Secondary Data Centre provides assurance that Core System Services are sufficiently resilient for go-live. Without the execution of this DR scenario, stakeholders will not have the confidence that planned migrations of inventory are being done to a resilient platform.

Scope

The scope is a failover of the Core System only (referred as Scenario 1 of 3) from the Oracle Primary Data Centre to the Secondary Data Centre. It is anticipated that the failover will take 2 hours, before a full failback to the Primary data centre which is also anticipated to take 2 hours. Oracle and Client Testing and Validation activities will be conducted before, during and after each failover / failback activity in a period expected to take 4 hours (2 hours each following failover and failback).

Scenarios 2 and 3 defined below are outside the scope of this Test Plan and will be planned and documented separately.

Scenario 2 - Loss of Azure/AWS integration layers only. Failover to another availability zone or region and demonstrate that integrations into and out of the Core System via the Integration Layers from backend systems.

Scenario 3 - Loss of the backend systems only (upstream and downstream) failover and still provide integrations via AWS/Azure integration layers into and out of the Core System.

Advantages

- Validation that the Core System can be recovered into the secondary data centre, proving the RTO and RPO and the ability to process operations in the Secondary Region.
- Internal and external interfaces to be validated.
- Gives the business confidence in the ability to operate the Core System in the Secondary Region should it be necessary to do so.

Risks

- We plan to run the Core System's EOD following failover. There is a risk that we may not be able to run the EOD in the Secondary Region and it fails to complete following failback. A light touch Command & Control process between Oracle and the Client will be established to agree actions should this risk become an issue.
- There is a risk that interchanges with the Core System may not function following failover and failback. A light touch suite of integration tests will help mitigate this.
- The creation of dummy order help mitigate this risk.

When

The test will take place over a two-phase approach.

Phase 1 - Failover from Oracle Primary Data Centre to Secondary Data Centre

- Overnight from 23:00 hours UTC on dd/mm/yyyy – 01:00hrs UTC dd/mm/yyyy.
- Testing and Validation and EOD run from 01:00hrs dd/mm/yyyy – 03:00hrs dd/mm/yyyy.

Phase 2 – Failback from Oracle Secondary Data Centre to Primary Data Centre

- 03:00hrs UTC dd/mm/yyyy – 05:00hrs UTC dd/mm/yyyy.
- Testing and Validation from 05:00hrs UTC dd/mm/yyyy – 07:00hrs UTC dd/mm/yyyy.
- BAU operations confirmation thereafter.

The overall DR Test activity is scheduled to take 8 hours with the activity planned to formally close at 07:00hrs UTC dd/mm/yyyy following BAU confirmation from the Operations Team.

Impact

During the timeframes outlined above in phase 1 and 2, the Core System will be unavailable whilst the failover / failback occurs. The Core System will then be fully operational in the Pre-Prod environment for the time in between each phase.

All impacted parties and Client Business Units will be advised in advance of testing.

Key Stakeholders

- Jack Jones etc.

3. SCOPE

The following are included within the scope of testing:

- To prove the Business can recover from a Core System outage.
- To obtain measurable RTO and RPO values for the given scenario.
- To validate the recovery steps documented in the plan and to execute a successful recovery.
- Validate the agreed test level was attained through functional and integration tests supported by evidence gathering.
- Validate Design assumption that integrations will not be affected by the failover and failback through integration checks including interface connectivity checks testing of critical Business Process transactions and validation of data.

3.1. Out of Scope

- Failover of integrations and back-end systems.

These out-of-scope items will be covered in future DR events as per Scenarios 2 & 3 defined within the Executive Summary Section

3.2. Test Level

Agreed Test Level (Appendix A)	Level 4

4. POSSIBLE OUTCOMES

Immediately prior and during the DR exercise the following outcomes may be observed:

4.1. Outcome 1 - Test does not start or has to be cancelled due to production issues

There is a ‘Go / Delay /No Go’ decision communicated on dd/mm/yyyy 22:45 hrs UTC.
If there is a serious operational incident (MI, P1 or P2) relating to the Core System or supporting network infrastructure or there are other reasons, such as unplanned unavailability of key staff, the decision may be taken to postpone the DR test in favour of resolving this.
It is recommended that an alternate date for the test be planned to mitigate the risk of this situation.

4.2. Outcome 2 - Test completes successfully with no significant issues

Test completes successfully as planned, with only minor adjustments to the recovery documentation.

4.3. Outcome 3 - Test completes successfully with problems encountered and fixed

Test completes successfully, problems encountered and fixed during the test or raised as issues to be tracked to completion post-test.
Undertake analysis and take action to address identified issues, as per normal process. Details of the issues and associated resolution actions taken will be recorded in the test results document.

4.4. Outcome 4 - Test fails

The test is unsuccessful and, depending on the point of failure, may be re-planned. The decision to re-plan and run the test again is made by the Senior Business Owner.

5. ASSUMPTIONS

The following assumptions are made:

- Client staff and additional third-party representatives clearly understand their responsibilities.
- There are no known issues with the Oracle backup and recovery processes.
- No data centre infrastructure services will be taken offline for this test.
- There are no scheduled activities relating to in scope servers, e.g. upgrades, patching, etc.
- Supporting network infrastructure is operational.
- That people resources will be available to perform recovery work as detailed in the plan.
- That members of staff can be reached by telephone should they be away from the office location.
- All 3rd parties provide heightened support for the test.

6. PRIMARY OBJECTIVES

Description	Owner
1. To ensure the Disaster Recovery Plan is fit for purpose and that the exercise/process and procedures demonstrate confidence in support of the Plan	Client
2. To ensure an exercise report is issued providing a summary of the exercise, its findings / recommendations and continued service improvement	Client
3. To obtain actual RTO and RPO values for the given scenario	Oracle
4. To validate the recovery steps documented in the disaster recovery plan(s)	Client & Oracle
5. To ensure the test does not impact the business production services (except where agreed as part of the test scope)	Client & Oracle
6. Ensure that the secondary recovery environment meets requirements	Client & Oracle
7. Recover in scope (infrastructure, OS and application) into the DR environment	Oracle
8. If issues are encountered, do problem determination and apply fixes	Oracle
9. If unable to fix occurred issues during the change window, take available evidence for further analysis	Oracle
10. Gather evidence to satisfy test level validation (Appendix B) and validate data integrity and volumes	Client & Oracle
11. Complete test schedule and evidence findings	Client & Oracle
12. Take screen shots that demonstrate system availability following recovery to DR site and again after fall back to production	Client
13. Lessons learnt recorded and Disaster Recovery Plan updated as appropriate	Client

7. EXERCISE CONTROL

7.1. Test Execution

Rob Hodges will facilitate the test preparation, execution and reporting.
Oracle Rep will lead the team at Oracle and attend all conference calls.
TechOps Rep will lead the team at and attend all conference calls.
Rob Hodges will issue email comms to stakeholders at regular checkpoints defined within the Runbook

7.2. Conference Calls

Intention for all involved to dial in to MS Teams meetings as listed in the timeline. Otherwise, to be used to either report that tasks have been completed or to flag issues to the Exercise Lead (Rob Hodges). Teams details to be attached to calendar invitation.

7.3. Timeline

Once a stage is complete, please confirm to:
Pre-test – DR Event Distribution List (See Appendix F)
During test – via conference bridge (a single bridge for all attendees/3rd parties) and Teams instant message to Night Shift and Morning Shift Team
Post-test – DR Event Distribution List (See Appendix F)

8. RISKS

Risk	Impact	Probability	Mitigation	Owner
BAU issue may impact the exercise	H	L	Go / No Go decision scheduled prior to start of exercise. Oracle, Digital and Fujitsu to confirm.	Client
Delays in DR failover steps	L	L	Test is cancelled, and failback activities commence.	Client
Failback issues cause delay	L	L	Restart production Core System without DR to meet agreed uptime. Risk to be accepted by the Client	Client
Connectivity issues encountered whilst running in DC2	L	M	Heightened support from 3rd parties	Client

9. DEPENDENCIES

Dependency	Owner
Operational backups for in-scope services	Oracle
Datacentre infrastructure	Oracle
Testing & Validation	Oracle & Client

10. RESPONSIBILITIES

The following parties are responsible and accountable for the exercise:

Role	Assignee	Description
Disaster Recovery Assurance	Rob Hodges	Agree scope, expected outcome and actual outcome. Run the exercise.
3rd party Technicians and Engineers	3rd Parties (Oracle)	Action the Disaster Recovery plan
3rd party Service Delivery	3rd Parties (Oracle)	Incident management
Application Validation	Oracle	Tests & Checks on DC2 post failover and DC1 post failback
Testing & Validation	Technical Operations	Testing of Core System on DC2 following failover and DC1 following failback
Confirmation of Business As Usual	Business Operations	Places and validates dummy order before Disaster Recovery Event closes.

11. SUCCESS CRITERIA AND AGREEMENT

11.1. Success Criteria (Appendix B)

- The test is measured as a success if all the primary objectives are met.
- Evidence that recovery time and point objectives have been met.
- Evidence showing that the agreed test level has been achieved.

Note: The test not being measured as a success does not mean a re-test is necessarily appropriate.

11.2. Remediation

Any issues resulting from the Disaster Recovery test will be recorded and identified as minor, medium or major. Minor and medium will be tracked and reported through ad hoc / Service Review meetings. Major will require a re-test within a timescale agreed by both parties, typically within 90 days of the original test date.

11.3. Agreement

The scope and objectives defined in this document will provide defined measurable criteria that will allow the business to compare what was agreed prior to the exercise against what was achieved.
These exercises may change from time to time and may deviate from the original solution or contract.
This scope document needs to be signed off via email.
Stakeholder Contact:

Name:	Jack Jones
Position:	Head of Technology Operations
Approval via:	Email
Date:	dd/mm/yyyy

11.4. Disclaimer

This document is not contractually binding but ensures that the deliverables of this exercise can demonstrate audit and compliance to the Client's ITSC Policy.

APPENDIX A – TEST LEVELS

Test Type	Level	Description	Details
Simple	1	Walkthrough / Desktop	A simulation of a disaster event designed to test the DR plan and procedures. Run as a roundtable workshop with all relevant parties (in the same room wherever possible). No physical recovery occurs. Preparation of the test followed by a 2-4 hour meeting typically.
Medium	2	Infrastructure only	Operating system and base level libraries/files restored, application installed
	3	Infrastructure and Application	Recovery of Production application onto the DR system, using the tape backups or failover/mirrored system. Login screen to application available and login only
	4	Technical with Interfaces	As per Level 3 with some interfaces to other systems.
	5	Full User Testing without Interfaces	As per Level 3, plus full end user testing of the core system but without interfaces to/from other systems.
Complex	6	Full User Testing with Interfaces	As per Levels 4 and 5, including interfaces and end user testing. Applicable to only one application/service, running entirely from the DR data centre, based on the assumption that primary data centre is unavailable for that application.
	7	Complete Data Centre Failure Simulation.	Simulation of total Data Centre loss. This is not only very complex and expensive; it is likely to have the biggest risk to the FULL production environment. (Included to show scale but rarely tested)

APPENDIX B - EVIDENCE CRITERIA

ID	Success Criteria list items	Test levels							Evidence
		1	2	3	4	5	6	7	
			Infrastructure only	Infrastructure and Application	Technical with Interfaces	Full User Testing without Interfaces	Full User Testing with Interfaces	Complete Data Centre Failure	
1	Test Level Agreed		x	x	x	x	x	x	Email to Client
2	Test date agreed		x	x	x	x	x	x	Email to Client
3	Invocation & recovery documentation, process validated and/or remediation items identified, and actions agreed		x						Test report
4	Invocation & recovery documentation is accessible post disaster		x						Document's location shared (must not only be in production datacentre)
5	Completion of detailed test report		x	x	x	x	x	x	Test report
6	Post-test wrap up meeting to discuss test results including action items, agreement on next steps.		x	x	x	x	x	x	Agreed actions and owners
7	All documented names, roles and contact details are up to date and valid		x	x	x	x	x	x	Confirmation in test report
8	Technical solution validated			x	x	x	x	x	Screen dumps, print outs, email confirmations Taken during the test
9	Data restored and validated by appropriate technical teams			x	x	x	x	x	Screen dumps, print outs, email confirmations Taken during the test
10	Successful user login to application			x	x	x	x	x	Screen dumps, print outs, email confirmations Taken during the test

11	User validation of restored data					x	x	x	Screen dumps, print outs, email confirmations Taken during the test
12	Functional testing completed by business users					x	x	x	Screen dumps, print outs, email confirmations Taken during the test
13	Application RTC established (recovery time capability)			x	x	x	x	x	Times logged in the test plan log
14	Application RPC established (recovery point capability)			x	x	x	x	x	Times logged in the test plan log
15	Recovery / technical script(s) validated (if applicable)			x	x	x	x	x	Screen dumps, print outs, log files
16	Database failover / restore validated (if applicable).			x	x	x	x	x	Database Engine running screen dump, database self-verification logs
17	Exceptions and failures documented in a test log		x	x	x	x	x	x	Test log
18	Remediation actions listed and assigned to owners or, risks recorded		x	x	x	x	x	x	Minutes and test report actions, sign off that remediation is completed or by subsequent test
19	Performance and capacity of the DR System is sufficient			Optional					Test logs, performance reports, load simulation software log
20	Network, data communications and firewalls all perform as per requirements					x	x		Screen dumps, firewall/network logs
21	In scope interfaces validated						x		Screen dumps, emails verifying the interfaces work from the dependent/feeder systems
22	All critical interfaces validated							x	Screen dumps, emails verifying the interfaces work from the dependent/feeder systems
23	Successful recovery of full IT estate							x	Logs, screen dumps, emails

APPENDIX C – RECORD OF TEST VALIDATION STAGES AND APPROVALS

Validation of the plan and chronology

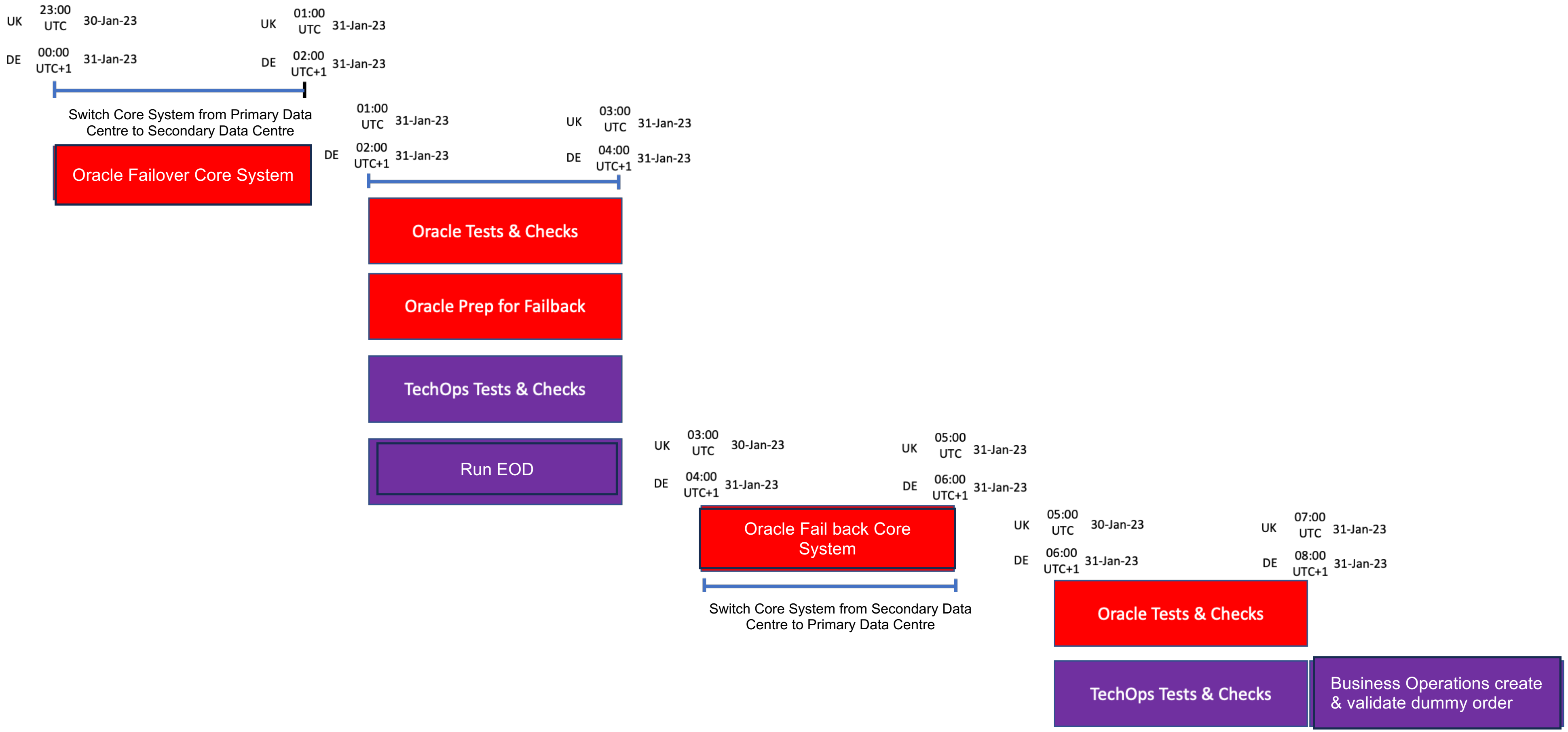
- Review dd/mm/yyyy-dd/mm/yyyy
- Final version of test plan, including chronology, approved on: dd/mm/yyyy

Approvals

Who	Date	Format (verbal, email, meeting minutes, etc)	Note
Test Plan Approvers	Dd/mm/yyyy	Jack Jones – Email TechOps – Email Business Operations – Email	

APPENDIX D – DR EVENT CHRONOLOGY

Summarised below. See separate Runbook (Teams: 05 DELIVERY -> 05 TESTING -> Disaster Recovery Testing -> DR_Scenario1_Runbook_v1.0.xls)



UK 23:00 UTC 30-Jan-23 — UK 01:00 UTC 31-Jan-23
DE 00:00 UTC+1 31-Jan-23 — DE 02:00 UTC+1 31-Jan-23

Switch Core System from Primary Data Centre to Secondary Data Centre

Oracle Failover Core System

01:00 UTC 31-Jan-23 — UK 03:00 UTC 31-Jan-23
DE 02:00 UTC+1 31-Jan-23 — DE 04:00 UTC+1 31-Jan-23

Oracle Tests & Checks

Oracle Prep for Failback

TechOps Tests & Checks

Run EOD

UK 03:00 UTC 30-Jan-23 — UK 05:00 UTC 31-Jan-23
DE 04:00 UTC+1 31-Jan-23 — DE 06:00 UTC+1 31-Jan-23

Oracle Fail back Core System

Switch Core System from Secondary Data Centre to Primary Data Centre

UK 05:00 UTC 30-Jan-23 — UK 07:00 UTC 31-Jan-23
DE 06:00 UTC+1 31-Jan-23 — DE 08:00 UTC+1 31-Jan-23

Oracle Tests & Checks

TechOps Tests & Checks

Business Operations create & validate dummy order

APPENDIX E – DR EVENT COMMUNICATION PLAN & RACI

Communication Activity	Method – Teams Meeting/Messages		Method - Email		
RACI	Client Team[1]	Oracle DR Team[2]	Client Team[3]	Oracle DR Team[4]	Stakeholders
Go/Delay/No Go Decision	A,R	C			
Communicate Decision (GO/DELAY/NO GO)	A,R	C	A,R	I	I[5]
Oracle notifies Client of completion of Failover	I	A,R			
Oracle Confirm Post Failover TechOps Tests can start	I	A,R			
Oracle confirm their Post Failover Tests are complete	I	A,R			
TechOps confirm their Post Failover Tests are complete	A,R	I			
Confirm Start of End of Day	A,R	I			
Confirm Completion of End of Day	A,R	I			
Oracle notifies Client of completion of Failback	I	A,R			
Oracle Confirm Post Failback TechOps Tests can start	I	A,R			
Oracle Confirm their Post Failback Tests are complete	I	A,R			
TechOps confirm their Post Failback Tests are complete	A,R	I			
Confirm end of DR Test			A,R	I	I[6]

[1] Client DR Team - Rob Hodges will lead activity and issue all internal Client comms, TBA will perform TechOps Tests & Checks, TechOps will run EOD and Business Ops will create and validate a dummy order following successful completion of the failback. Client and Fujitsu contacts will be on call in the event of issues & decision making.

[2] Primary contact TBA

[3] Client DR Team - as per footnote 1.

[4] Oracle DR Team – as per footnote 2

[5] Please see Appendix F – DR Event Email Distribution List

[6] The “Confirm end of DR Test” email distribution list is the same as that of the Go/Delay/No Go Distribution List on the next page

APPENDIX F – DR EVENT EMAIL DISTRIBUTION LIST

	Name	Email Address
To		
cc		