NXG DR – Test Plan

NXG

23rd August 2023

Version: 0.1

This document details the details of disaster recovery plans and testing procedures for NXG.

Prepared for:

Infrastructure Team
DevOps Group
Executive Leadership Team

Approved by:

FISCAL TECHNOLOGIES

1 CONFIDENTIALITY

Table of Contents

1 CONFIDENTIALITY 1
2 STATEMENT OF INTENT 3
3 CONTACT INFO – KEY PERSONNEL IN A DISASTER RECOVERY EVENT 4
4 DISASTER DECLARATION AND ALERT RESPONSE INFORMATION 5
4.1 AUTHORITY TO ACTIVATE THIS PLAN 5
4.2 RECOVERY STRATEGY 5
4.3 RECOVERY TIME REQUIREMENTS 5
4.3.1 Maximum Tolerable Outage (MTO) 6
4.3.2 Recovery Time Objective (RTO) 6
4.3.3 Recovery Point Objective (RPO) 6
4.3.4 Maximum Time To Repair (MTTR) 6
4.4 BUSINESS RESUMPTION PROCESS 6
4.5 POST INCIDENT REVIEW 6
5 COMMUNICATION STRATEGY 7
6 ESCALATION RATINGS AND PROCEDURE 7
7 INFRASTRUCTURE OVERVIEW 8
7.1 ABED 8
7.2 GLOBAL 8
7.3 REGION 8
8 RESTORATION STEPS AND DETAILS 9
9 SYSTEM CONFIGURATION AND BACKUP CONFIGURATION 9
10 DATA RESTORATION 9
11 INSURANCE INFORMATION 9
12 LEGAL INFORMATION 9
13 TEST SUMMARY 10
13.1 RESULTS – SUMMARY 10
13.2 KEY RECOMMENDATIONS – SUMMARY 11
14 DETAILED TESTS RESULTS 12
14.1 CONTEXT 12
14.2 TERRAFORM STATE FILES 13
14.2.1 Account Failover 13
14.2.2 Blob Deleted or Overwritten 14
14.3 GLOBAL 14
14.3.1 Failover to Paired Azure Region 15
14.4 ABED 16

14.4.1 Failover to Paired Azure Region 16
14.5 AZURE VPN 17
14.5.1 Failover to Paired Azure Region 17
14.6 CUSTOMER REGION 18
14.6.1 Failover to Paired Azure Region 18
14.6.2 Accidental Customer Deletion 19
15 REPORTING / TEST IMPROVEMENT 20

2 STATEMENT OF INTENT

In event of a disaster that stops, prevents, or significantly interrupts (or threatens to do so) the company's ability to perform operate the NXG Forensics platform.

The aim is to ensure that the details provided in this plan will allow a recovery process to run with minimal decision-making steps and ensure the essential personnel and partners are identified and informed of their duties and responsibilities in the wake of a disaster.

The detailed processes should allow those individuals to know the steps required to get the organisation up and running as soon as possible.

A disaster is an event that significantly reduces FISCAL's ability to provide access to or support of the Service. Typically, this will be one or more of the following:

- An outage in one or more of the Azure regions from which NXG is hosted.
- A malicious act that partially or totally affects a service facility including acts of terrorism.
- Prohibition of access to any FISCAL site by a Police Officer, Fire Officer, HSE Officer or other representative on the business of an official body.
- Accidental damage to infrastructure.
- Malicious damage to infrastructure.
- Hardware or Software Failure.
- Incompetence.
- Loss of personnel

3 CONTACT INFO – KEY PERSONNEL IN A DISASTER RECOVERY EVENT

This is the key contact information of all involved parties, specifically key personnel in the IT and Engineering departments, external assets or networks, third-party resources, and key stakeholders.

Name	Role	Company	Email	Phone Number	Notes
James Pobgee	Head of IT	Fiscal Technologies	jpobgee@fiscaltec.com		
Dan Searle	Senior Infrastructure Engineer	FISCAL Technologies	dsearle@fiscaltec.com	07718 127 481 01344 512 183	IT Engineer, required for VPN configuration.
Justin Pealing	Senior Software Engineer	FISCAL Technologies	jpealing@fiscaltec.com		
Kevin Deenoo	Platform Engineer	FISCAL Technologies	kdeenoo@fiscaltec.com		
Daniel Earwicker	Chief Software Architect	FISCAL Technologies	dearwicker@fiscaltec.com		
Jamie Mulcahy	Senior Software Engineer	FISCAL Technologies	jmulcahy@fiscaltec.com		
Adam Awan	Senior Software Engineer	FISCAL Technologies	awan@fiscaltec.com		
Microsoft Azure	Vendor	Microsoft		0344 800 2400	Use Azure Portal https://portal.azure.com/#blade/Microsoft_Azure_Support/HelpAndSupportBlade/overview
Softcat Ltd	Vendor	Softcat Ltd	mccormickp@softcat.com	0161 274 5132	
Cloudflare	Vendor	Cloudflare			https://support.cloudflare.com/hc/en-us
Auth0	Vendor	Auth0			https://support.auth0.com/

4 DISASTER DECLARATION AND ALERT RESPONSE INFORMATION

4.1 AUTHORITY TO ACTIVATE THIS PLAN

The CISO / TISO, Head of IT, Chief Architect or Platform Engineers may activate this plan. These personnel make up the primary part of the response team.

The CISO, or delegated representative will assume business continuity and recovery responsibilities. If the CISO is unavailable, another member of the named Contacts (above) may assume the Team Leader role during the event.

FISCAL will consult with customers during the process of activating this plan to ensure that they are aware of incident severity and schedule if it affects customer operations or data security.

4.2 RECOVERY STRATEGY

In the event of a suspected disaster, there are three processes that will take place prior to the activation of the actual recovery process. An overview is provided in Figure 1 Disaster Recovery Strategy Overview.

- Disaster Alert Notification – to notify FISCAL's Response Team that a disaster may have occurred or is evolving.
- Damage Assessment – to ascertain whether a disaster has occurred, assess the extent of the damage, and to assemble the response teams if necessary.
- Disaster Declaration Assessment – to ascertain if the predetermined Maximum Tolerable Outage is likely to be compromised and that invoking the Business Continuity Plan and its associated procedures is necessary. During this step we will notify FISCAL's Response Team, the Customers and other service providers that a disaster may have occurred or is evolving.

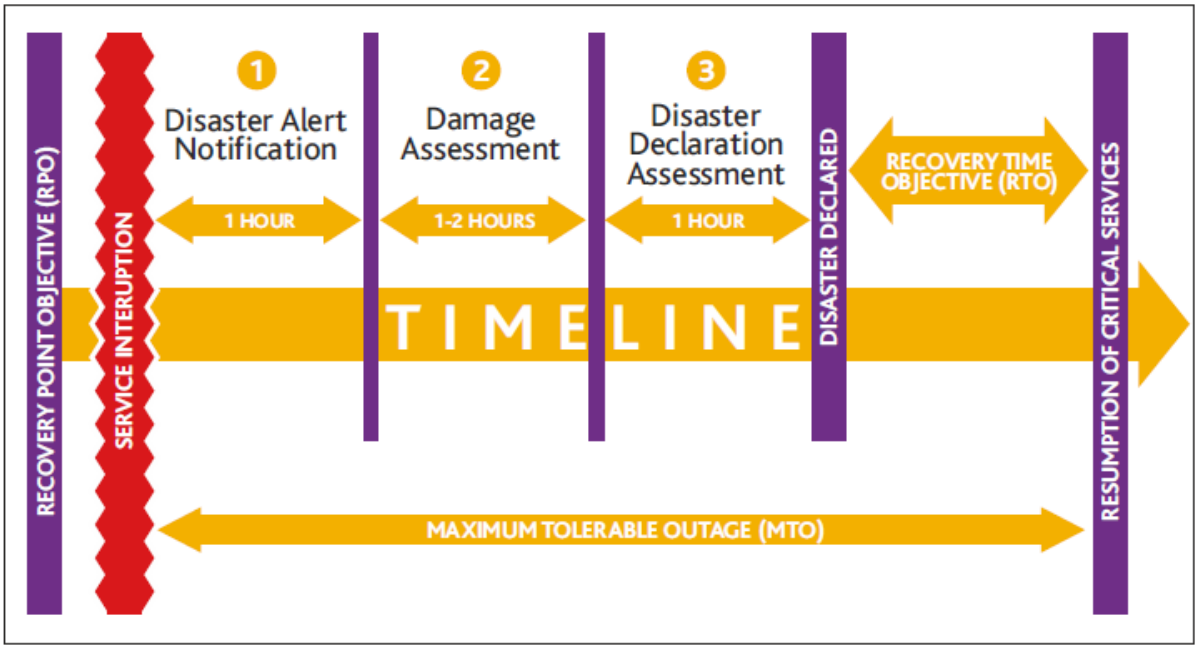

Figure 1 Disaster Recovery Strategy Overview

4.3 RECOVERY TIME REQUIREMENTS

The following requirements are a result of the Business Impact Analysis process which forms part of the FISCAL business continuity programme as described in the Business Continuity Plan.

4.3.1 Maximum Tolerable Outage (MTO)

Target: 4 days.

The maximum tolerable outage is the amount of time services may be unavailable before FISCAL's business operations are severely impacted and this in turn has a severe impact on the Customer. The MTO encompasses all activities from point of impact to point of recovery completion as described in the Recovery Strategy Section.

4.3.2 Recovery Time Objective (RTO)

Target: 3 days.

The recovery time objective is the time taken to recover the in-scope services of the Service from disaster declaration to the point where the platform is handed over to FISCAL's business teams.

4.3.3 Recovery Point Objective (RPO)

Target: 1 day (from Service interruption).

The recovery point objective is the target set for the status and availability of data (electronic and paper) at the start of the recovery process. In other words, this is the point from which recovery of lost data must take place. The Cloud Platform is designed in such a way as to minimise the amount of data lost in the event of a BCP invocation.

4.3.4 Maximum Time To Repair (MTTR)

Target: Dependant on the criticality of the service / hardware agreements. These should be designed to ensure FISCAL can meet the RTO and RPO objectives set in event of a disaster.

The maximum time to repair is the target that represents the maximum time it takes to repair and restore a component or system to functionality. As such, MTTR is a primary measurement of the maintainability of FISCAL's systems, equipment, applications and infrastructure, as well as its efficiency in fixing that equipment when an IT incident occurs.

4.4 BUSINESS RESUMPTION PROCESS

Please refer to BCP for detailed information.

4.5 POST INCIDENT REVIEW

After closure of a disaster situation a post incident review of the process and how it could be improved will be conducted.

The review shall ensure that:

- FISCAL can understand the cause, nature and impact of the incident on the organisation and its customers.
- Lessons learned are clearly identified and incorporated into a knowledge base for future Business Continuity Plan development and disaster management.
- Deficiencies in the current processes are clearly identified in a way that projects can be established to rectify or mitigate them.

The results of this review will be recorded as part of the ISF meeting and held in the ISF minutes archive. Lessons learned shall be incorporated into future Business Continuity Plans.

5 COMMUNICATION STRATEGY

This is the information regarding how personnel and employees will maintain contact and communication throughout a disaster, including phones, alerts, media, and other communication methods.

Please refer to BCP for detailed information.

6 ESCALATION RATINGS AND PROCEDURE

Determine the severity of a disaster based on a rating system and react to the disaster accordingly. Ratings include:

- Intolerable
- Undesirable
- Tolerable
- Acceptable

Please refer to BCP for detailed information.

7 INFRASTRUCTURE OVERVIEW

NXG primarily operates out of 3 Azure regions, each of which has a paired Azure region used for the purpose of disaster recovery:

- West Europe (paired to North Europe)
- UK South (paired to UK West)
- West US 2 (paired to West Central US)

Each of these regions contains a set of core services used to host NXG customers, in addition:

- The West Europe region hosts additional "global" services, such as log aggregation and storage accounts used for terraform state files.
- The UK West region hosts virtual networking infrastructure used to provide engineering access to the environment.

7.1 REGION INFRASTRUCTURE

Core region infrastructure consists of several services, including:

- Virtual Network
- Kubernetes (AKS)
- App Service
- Azure SQL Server
- Storage Accounts
- Azure Cache for Redis

In the event of a failure of the Azure Region these services will be re-deployed into the paired Azure region. To ensure that data is not lost:

- Storage accounts are configured with geo-replication (RA-GRS)
- For SQL Server we make use of geo-redundant backups to restore databases to the newly deployed region.

7.2 GLOBAL INFRASTRUCTURE

Additional global infrastructure consists of:

- Storage accounts used for terraform state files, configured with geo-replication (RA-GRS)
- Azure Functions App used for global management, with a backing storage account (RA-GRS) used for persistence of application state
- Application Insights
- Additional Azure SQL Servers containing databases with geo-redundant backups.
- Additional Storage Accounts (RA-GRS)
- Azure Container Registry, with a replica in the West US 2 region

7.3 VIRTUAL NETWORK INFRASTRUCTURE

In addition, the UK West region contains a Virtual Network Gateway used to provide VPN access to the production environment deployments and engineering / support access.

8 RESTORATION STEPS AND DETAILS

Detailed processes for each of these recoveries held on Azure DevOps Wiki under "Playbooks".

- Terraform state files
- Azure VPNs
- ABED
- Global
- Customer Regions

9 SYSTEM CONFIGURATION AND BACKUP CONFIGURATION

Azure Storage Accounts are configured to use geo-replication (RA-GRS), as well as blob versioning to allow restoration of deleted or corrupted blobs.

Azure SQL Databases are configured to use geo-redundant backup, to allow recovery of databases in the case that the primary region is inaccessible. In addition, point-in-time restore can be used to recover from accidental corruption of data.

10 DATA RESTORATION

As stated in the relevant recovery procedures.

11 INSURANCE INFORMATION

This is the insurance coverage of the IT department and other relevant policy information.

Please refer to BCP for detailed information.

12 LEGAL INFORMATION

These are the steps to be taken in order to deal with both the financial and legal impacts of a disaster.

Please refer to BCP for detailed information.

13 TEST SUMMARY

13.1 RESULTS – SUMMARY

Testing showed that backups are configured correctly, and that data would be accessible in the event of DR, with the following exception:

- Global makes use of Azure tables, which do not support point in time restore. This could result in data loss in the case of accidental deletion / corruption of data (e.g. due to a software bug).

In only a few cases the recovery process was risky enough that it could not be validated on the live environment:

- Global – Failover to paired Azure Region
- Abed – Failover to paired Azure Region
- Restoration of customer to paired Azure Region

Global failover was largely successful, however a failure in Global affects all live regions and so it is especially important that recovery processes for Global are fast and reliable.

Issues with the structure of the Abed terraform prevented the DR process from being followed as documented.

Identified risks for restoration of customers to paired Azure Region:

- We do not make use of Reserved Capacity. In the event of an extended Azure outage other Azure customers will also be enacting their DR processes, making it more likely that creating Azure resources in the paired Azure region will fail due to lack of capacity.
- RTO for geo-restore is 12 hours, with only 4 concurrent restore operations allowed per elastic pool. In the UK region we have 2 elastic pools and ~200 customer databases to restore, meaning that the total time take to recover all databases could exceed 2 days. While this is within RTO it consumes a significant portion of the allowed recovery time, leaving little margin for error.
- Only limited testing of the restored customer is performed. To be confident that all NXG features will work as expected following DR an extended test with real customers should be performed.

Risk	Severity	Likelihood	Risk Level	RPO	RTO	MTTR	Restore Time	Backup Status	Acceptability	Remediation
Terraform State Files – Account Failover	TOLERABLE	IMPROBABLE	LOW	MET	MET	ACCEPTABLE	ACCEPTABLE	Backed up	ACCEPTABLE	Not Required
Terraform State Files – Deleted	TOLERABLE	IMPROBABLE	LOW	MET	MET	ACCEPTABLE	ACCEPTABLE	Backed up	ACCEPTABLE	Not Required
Global – Failover to paired Azure Region	INTOLERABLE	IMPROBABLE	HIGH	MET	MET	UNDESIRABLE	UNDESIRABLE	UNDESIRABLE	UNDESIRABLE	Required
Abed – Failover to paired Azure Region	TOLERABLE	IMPROBABLE	LOW	NOT MET	NOT MET	ACCEPTABLE	ACCEPTABLE	No Backup	INTOLERABLE	Required
VPN – Failover to paired Azure Region	TOLERABLE	IMPROBABLE	LOW	N/A	MET	N/A	N/A	N/A	ACCEPTABLE	Not Required
Region – Failover to paired Azure Region	INTOLERABLE	IMPROBABLE	HIGH	MET	NOT MET	ACCEPTABLE	ACCEPTABLE	Backed up	UNDESIRABLE	Required
Accidental Deletion of Customer	UNDESIRABLE	POSSIBLE	HIGH	MET	MET	ACCEPTABLE	ACCEPTABLE	Backed up	ACCEPTABLE	Not Required

13.2 KEY RECOMMENDATIONS – SUMMARY

- Update global to use SQL, which supports point-in-time restore.
- Enable geo-replication of global databases to allow faster recovery.
- Improve Global DR process to the point where it is safe to test in live.
- Consider purchasing reserved capacity in paired Azure regions.
- Improve customer restore process to the point where it is safe to test with live customers.
- Develop tooling to allow mass restore of customers in the event of failure of a region.

14 DETAILED TESTS RESULTS

14.1 CONTEXT

Below is a list of tests and the results or anticipated results e.g., where emulated tests were required.

Each section is segregated by risk area with details of the test and context related to it, the owners, users, and support personnel / third parties associated. It will detail the processes and outcomes from the tests and any areas highlighted including remediation actions and suggestions on improvements or concerns.

We provide a summary of the risk along with the associated results based on estimation (in event of emulated tests or the results of the test and if it meets our requirements.

This is broken down into the following sections:

- Severity – How severe would the impact be if the event occurred. (Acceptable, Tolerable, Undesirable, Intolerable)
- Likelihood – How likely is it that the event would or could occur. (Improbable, Possible, Probable).
- Risk Level – A generated rating based on comparing Severity versus Likelihood.

	ACCEPTABLE	TOLERABLE	UNDESIRABLE	INTOLERABLE
IMPROBABLE	LOW	LOW	MEDIUM	HIGH
POSSIBLE	LOW	MEDIUM	HIGH	EXTREME
PROBABLE	MEDIUM	HIGH	HIGH	EXTREME

- Recovery Point Objective (RPO) - Describes the interval of time that might pass before the quantity of data lost during that period exceeds FISCALs maximum allowable threshold.
- Recovery Time Objective (RTO) - The duration of time within which the business service must be restored after a disaster in order to avoid unacceptable consequences.
- Maximum Time To Repair (MTTR) – This represents the maximum time required to repair a failed component or device.
- Backup Status – Are there any redundancies in place to help mitigate the risk or ensure continuity during a disaster. (Replicated Backup, Local Backup, No Backup)
- Restore Time – Mostly related to backups, this metric defines the time it would take to restore data post the event.
- Remediation – Details if any remediation is required. (Not Required, Required)
- Acceptability: Details if the results and remediations in place meet requirement. (Acceptable, Tolerable, Undesirable, Intolerable)

14.2 TERRAFORM STATE FILES

14.2.1 Account Failover

Owner: Platform Team.

Support Team: Azure, Development.

User Groups: Development.

Test invocation of the account failover recovery procedures for Terraform state files.

This test was performed on the production environment.

Availability of terraform state files is required for subsequent recovery procedures, so timely recovery is essential.

Severity	TOLERABLE		**Likelihood**	IMPROBABLE		**Risk Level**	LOW	
RPO	15 mins	MET	**RTO**	1 hr	MET	**MTTR**	1 hr	ACCEPTABLE
Backup Status	ACCEPTABLE		**Restore Time**	1 hr	ACCEPTABLE	**Remediation**	Not Required	

14.2.1.1 Test Steps

1. Initiate an account failover for all affected storage accounts as per the documented recovery procedures.
2. Wait for account failover to complete.
3. Validate availability of storage account with a terraform plan via the Azure DevOps pipelines.
4. Re-enable RA-GRS for storage accounts.

14.2.1.2 Test Outcome / Acceptability

Outcome: Test completed successfully.

Acceptability: Acceptable.

14.2.1.3 Remediation Options / Areas of Improvement / Improvement Options

None

14.2.2 Blob Deleted or Overwritten

Owner: Platform Team.

Support Team: Azure, Development.

User Groups: Development.

Test invocation of the Blob deleted or overwritten recovery procedures for Terraform state files.

This test was performed on a non-production environment, but the live accounts were validated to ensure that snapshots are available.

Severity	TOLERABLE		**Likelihood**	IMPROBABLE		**Risk Level**	LOW	
RPO	15 mins	MET	**RTO**	1 hr	MET	**MTTR**	1 hr	ACCEPTABLE
Backup Status	ACCEPTABLE		**Restore Time**	1 hr	ACCEPTABLE	**Remediation**	Not Required	

14.2.2.1 Test Steps

1. Delete a terraform state file.
2. Follow recovery procedure to recover deleted state file.
3. Validate the recovery was successful by running a terraform plan, confirm that no changes are required.

14.2.2.2 Test Outcome / Acceptability

Outcome: Test completed successfully.

Acceptability: Acceptable.

14.2.2.3 Remediation Options / Areas of Improvement / Improvement Options

None

14.3.1 Failover to Paired Azure Region

Owner: Platform Team.

Support Team: Azure, Development.

User Groups: All NXG Customers.

Emulation of failover of Global to Paired Azure Region.

This test was simulated on a non-production environment, as the recovery process is destructive.

Severity	INTOLERABLE		Likelihood	IMPROBABLE		Risk Level	HIGH	
RPO	15 mins	MET	RTO	12 hr	MET	MTTR	12 hr	UNDESIRABLE
Backup Status	UNDESIRABLE		Restore Time	12 hr	UNDESIRABLE	Remediation	Required	

14.3.1.1 Test Steps

1. Follow recovery procedure for failover of Global in the "try" environment
2. Validate that the environment is working as expected
    - Playwright tests passing, which validates the ability to create a customer, log in and process files
    - Logs visible in App Insights

14.3.1.2 Test Outcome / Acceptability

Outcome: The test was completed, however additional problem solving was required:

- Function keys on the Function App were not set correctly and had to be manually set.
- The custom domain was not set correctly on the Function App.

Documented RTO for SQL Databases is 12 hours. This is within our documented RTO, however until the usage monitoring databases is restored outage would this prevents successful operation of any action that requires auditing. This would affect all regions, not just West Europe.

Documented RPO for Azure storage accounts is ~15 minutes, which satisfies our RPO. Documented RTO is 1 hour, which is acceptable.

Acceptability: Undesirable.

14.3.1.3 Remediation Options / Areas of Improvement / Improvement Options

- Improve recovery process.
    - Should be non-destructive, to allow testing on live environment.
    - Should be substantially faster than 12 hours
- Update global to use SQL, which supports point-in-time restore.

14.4.1 Failover to Paired Azure Region

Owner: Platform Team.

Support Team: Azure, Development.

User Groups: All NXG Customers.

Emulation of failover to Paired Azure Region.

This test was simulated on the "Perf" environment, as the recovery process is destructive.

Severity	TOLERABLE		**Likelihood**	IMPROBABLE		**Risk Level**	LOW	
RPO	Unknown	NOT MET	**RTO**	Unknown	NOT MET	**MTTR**	12 hrs	ACCEPTABLE
Backup Status	ACCEPTABLE		**Restore Time**	12 hrs	ACCEPTABLE	**Remediation**	Required	

14.4.1.1 Test Steps

1. Deploy and manually validate Perf environment
2. Follow recovery procedure for failover of ABED to the paired Azure region
3. Manually validate Perf environment
    a. Able to create a customer, log in and process an APT file
    b. Logs visible in App Insights

14.4.1.2 Test Outcome / Acceptability

Outcome: The process could not be completed as documented due to a failure in the DR process caused by issues in the structure of the terraform.

Acceptability: Intolerable, requires remediation.

14.4.1.3 Remediation Options / Areas of Improvement / Improvement Options

- Fixes terraform structure.

14.5.1 Failover to Paired Azure Region

Owner: Platform Team.

Support Team: Azure, Development.

User Groups: All NXG Customers.

Emulation of failover to Paired Azure Region.

Test performed on non-production environment.

Severity	TOLERABLE		**Likelihood**	IMPROBABLE		**Risk Level**	LOW	
RPO	N/A		**RTO**	2 hrs	MET	**MTTR**	N/A	
Backup Status	N/A		**Restore Time**	N/A		**Remediation**	Not Required	

14.5.1.1 Test Steps

1. Follow the recovery procedure.
2. Validate that deployments to AKS can be performed.
3. Validate that point-to-site connections allow access to AKS.

14.5.1.2 Test Outcome / Acceptability

Outcome: Process completed successfully.

Recovery process was extended as retries are required and due to time taken to destroy existing virtual network gateway.

Acceptability: Acceptable.

14.5.1.3 Remediation Options / Areas of Improvement / Improvement Options

- Refactor terraform so that DR hub can be deployed alongside existing Hub.

14.6.1 Failover to Paired Azure Region

Owner: Platform Team.

Support Team: Azure, Development.

User Groups: All NXG Customers.

Emulation of failover to Paired Azure Region.

The deployment of the disaster recovery regions was tested in live, however only the restoration of databases was tested on live due to the risk of disruption to live customers. The full failover process was tested in a non-production environment.

Severity	INTOLERABLE		Likelihood	IMPROBABLE		Risk Level	HIGH	
RPO	1 hr	MET	RTO	?	NOT MET	MTTR	?	Unacceptable
Backup Status	Backed up		Restore Time	?	Unacceptable	Remediation	Required	

14.6.1.1 Test Steps

In each live region:

1. Deploy the region, as per the documented recovery process
2. Manually validate the region by creating a customer, logging in and processing a transaction file.
3. Follow the documented instructions to restore a geo-redundant backup to the region

14.6.1.2 Test Outcome / Acceptability

Outcome: The test steps were completed successfully.

The documented RTO for geo-redundant backups is 12 hours, which for a single customer is acceptable, however a maximum of 4 restore operations can be run in parallel for each Elastic Pool, which means that the total time required to restore all customer databases is likely to exceed our RTO.

In addition the process for recovering a customer to the DR region is manual, which would further extend recovery time.

Acceptability: Undesirable, requires remediation.

14.6.1.3 Remediation Options / Areas of Improvement / Improvement Options

- Create tooling to allow mass restore of customers to minimize manual effort.

14.6.2 Accidental Customer Deletion

Owner: Platform Team.

Support Team: Azure, Development.

User Groups: All NXG Customers.

Test recovery of a customer deleted in the cloud tool.

This test was performed in a non-production environment.

Severity	UNDESIRABLE		**Likelihood**	POSSIBLE		**Risk Level**	HIGH	
RPO	1 hr	MET	**RTO**	2 day	MET	**MTTR**	12 hrs	ACCEPTABLE
Backup Status	Backed up		**Restore Time**	12 hours	ACCEPTABLE	**Remediation**	Not Required	

14.6.2.1 Test Steps

1. Delete a single-unit customer in the cloud tool, ensuring that the customer has uploaded files and allowing at least 1 hour before deleting.
2. Follow recovery procedure for accidental customer deletion.
3. Validate the restored customer
    a. Can log into the customer
    b. Files can be uploaded and processed
    c. Risks are accessible and workflow can be applied
    d. Reports are accessible

14.6.2.2 Test Outcome / Acceptability

Outcome: Test completed successfully.

This process requires high level of access to the production environment.

Acceptability: Acceptable.

14.6.2.3 Remediation Options / Areas of Improvement / Improvement Options

Develop tooling so this process can be initiated from the cloud tool.

15 REPORTING / TEST IMPROVEMENT

As part of continued improvement, we highlight in future tests follow areas should be covered as part of a disaster recovery test.

- Azure DevOps
- Cloudflare
- Auth0
- Azure B2C

Our goal should be to attempt DR tests in live environments in the future.