Business Continuity Plan

Reference: FPD0170A-2022

Version: 1

Owner: Lesley (new) Reeve

First Issued Date: 15/11/2023

Revision Issued Date: 15/11/2023

To outline FISCAL Technologies' Business Continuity strategy supporting FISCAL's provision of the AP Forensics® and NXG Forensics® Cloud Platforms

Prepared for:
All Employees, select Contractors,
Partners and Customers

Prepared by:
James Pobgee

FISCAL Technologies Ltd
448 Basingstoke Road,
Reading, RG2 0LP
Tel: 0845 680 1905

FISCAL TECHNOLOGIES

1 CONFIDENTIALITY

Table of Contents

2 DOCUMENT CONTROL

Item	Description
Document Title:	Business Continuity Plan
Associated Controls:	B.5.29 B.5.30 B.5.5 B.5.6 B.8.14
Reference ID:	FPD0170A-2022
Version:	1
Status:	Published
Approver:	
Approval Date:	
First Issued Date:	14/11/2023
Revision Issued Date:	15/11/2023
Reference Documents:	Linked Policies: • Business Continuity Management Policy Linked Procedures: Linked Records: • ISMS Scope

2.1 DOCUMENT PUBLICATION HISTORY

(All revisions made to this document must be listed in chronological order, with the most recent revision at the bottom)

Version	Date	Author
1	15/11/2023	James Pobgee

3 LIST OF TABLES

3.1 CONTACT LIST

Title	Name	Phone	Mobile
CEO	David Griffiths	01344 989482	07973 822779
COO / CISO	Lesley Reeve	01344 988769	07922 157267
Director of IT and Security / TISO	James Pobgee	01348 989483	07375 994606
VP of Engineering	Paul Ireland	Via MS Teams	

3.2 KEY SUPPLIER CONTACTS

Supplier/Service	Name	Phone	Notes
Zen Internet	support@zen.co.uk	01706 902902 01706 902001	Site ID 102726
Telappliant / VOIP	support@voiptalk.org	0161 713 3633	Account Manager
Zendesk	support@zendesk.com	N/A	
The Bunker	support@thebunker.net	01304 814800 07919 155618 01304 814890	Account Manager (24hr)
Microsoft	Azure Support tickets logged in Azure Portal	0344 800 2400	https://portal.azure.com/#blade/Microsoft_Azure_Support/HelpAndSupportBlade/overview
Landlord	Ultima Properties Limited		Landlord
Property Management	Hicks Baker		https://www.hicksbaker.co.uk/

3.3 CONTACT WITH AUTHORITIES

FISCAL TEC Group are:

- Under no FSA obligations
- Under no PCI DSS obligations
- voluntarily registered as a Data Controller by ICO
    - https://ico.org.uk/ESDWebPages/Entry/ZA115827

Emergency Services Contacts:

- Thames Valley Police – Reading: 01865 841148 (non-Emergency)
- Emergency services (Police, Fire, Ambulance): 999

3.4 SPECIAL INTEREST GROUPS

CISO, TISO and/or delegates are members of Information Security and Vendor alert mailing lists:

Microsoft Security Response Centre: https://msrc.microsoft.com/update-guide

TechNet: http://technet.microsoft.com/en-us/security/dd252948.aspx

National Cyber Security Centre: https://www.ncsc.gov.uk/

Crowdstrike: https://www.crowdstrike.com

Mimecast: https://www.mimecast.com

Fortinet: https://www.fortinet.com/

Center for Internet Security: https://www.cisecurity.org/

US-CERT: https://www.cisa.gov/about/contact-us/subscribe-updates-cisa

4 OVERVIEW AND SCOPE

4.1 OVERVIEW

The purpose of this plan is to detail the Business Continuity strategy supporting FISCAL's provision of the AP Forensics® and NXG Forensics® Cloud Platforms (Service).

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 environmental event that partially or totally affects a service facility including, fire, flood, wind, and earthquakes.
- A malicious act that partially or totally affects a service facility including acts of terrorism.
- A widespread pandemic rendering restrictions on travel and attending workplaces.
- Loss of utilities including power, water, and communications.
- 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 the Service infrastructure or facilities.
- Malicious damage to the Service infrastructure or facilities.
- Incompetence.
- Loss of personnel; and
- Insolvency.

IT hardware and software problems local to FISCAL's Reading Office, while they might in some instances be significant, will be resolved through normal incident and problem management and resolution methods.

A disaster declaration begins the formal disaster recovery process described later in this document.

4.2 AIM

The aim of this plan is to set out the mitigation, preparation, warning, response, and business continuity arrangements for the Service.

4.3 OBJECTIVES

The objective is to provide for restoration and continuation of the Service when a disaster occurs. This is accomplished by developing and maintaining a detailed Business Continuity Management Plan (BCP) that will organise and govern a disaster recovery operation. The BCP must:

- provide the information and procedures necessary to respond to an occurrence, notify personnel, assemble recovery teams, recover data, and resume processing at the current or alternate site as soon as possible after a disaster has been declared.
- create a disaster recovery structure strong enough to provide guidance to all interrelated groups, yet flexible enough to allow FISCAL personnel to respond to whatever type of disaster may occur.
- provide specific action plans for each functional area.
- identify those activities necessary to restore each of the Service components to full service; and
- establish a return to a "business as usual" environment.

5 GENERAL PRINCIPLES AND ACTIVATION OF THIS PLAN

5.1 AUTHORITY TO ACTIVATE THIS PLAN

The Director of IT and Security, VP of Engineering, CISO or DevOps personnel may activate this plan.

FISCAL will consult with customers during the process of activating this plan to ensure that they are aware of incident severity and schedule.

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

5.2 RECOVERY STRATEGY

Following the occurrence 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, the Customers and other service providers 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 the above three processes, in all but the severest of disasters that are likely to affect the wider society, the resiliency of the Service infrastructure will continue to provide service to the Cloud Platform Customers.

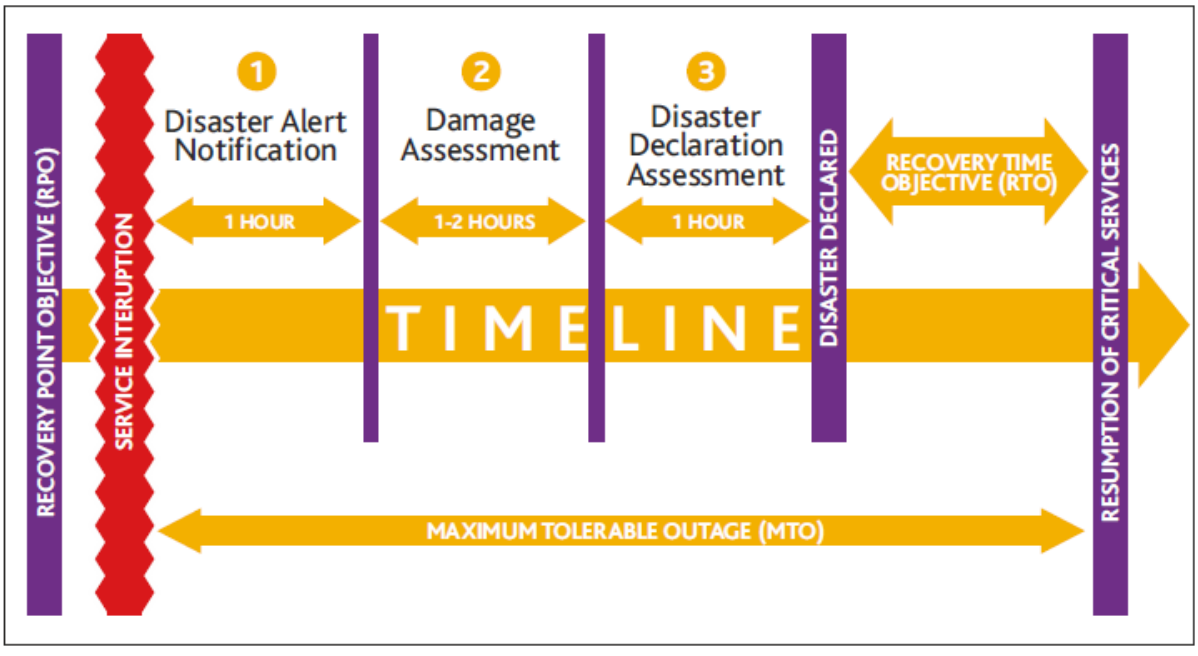

Figure 1 Disaster Recovery Strategy Overview

5.3 BUSINESS RESUMPTION PROCESS

Once a Disaster Declaration Statement has been made the Business Resumption Process will be applied. The aim will to be return to Business as Usual as quickly as possible. It is however likely that the recovery will be gradual and that services may be reintroduced in order of criticality, risk, and importance. See *Figure 2 Business Resumption Process*.

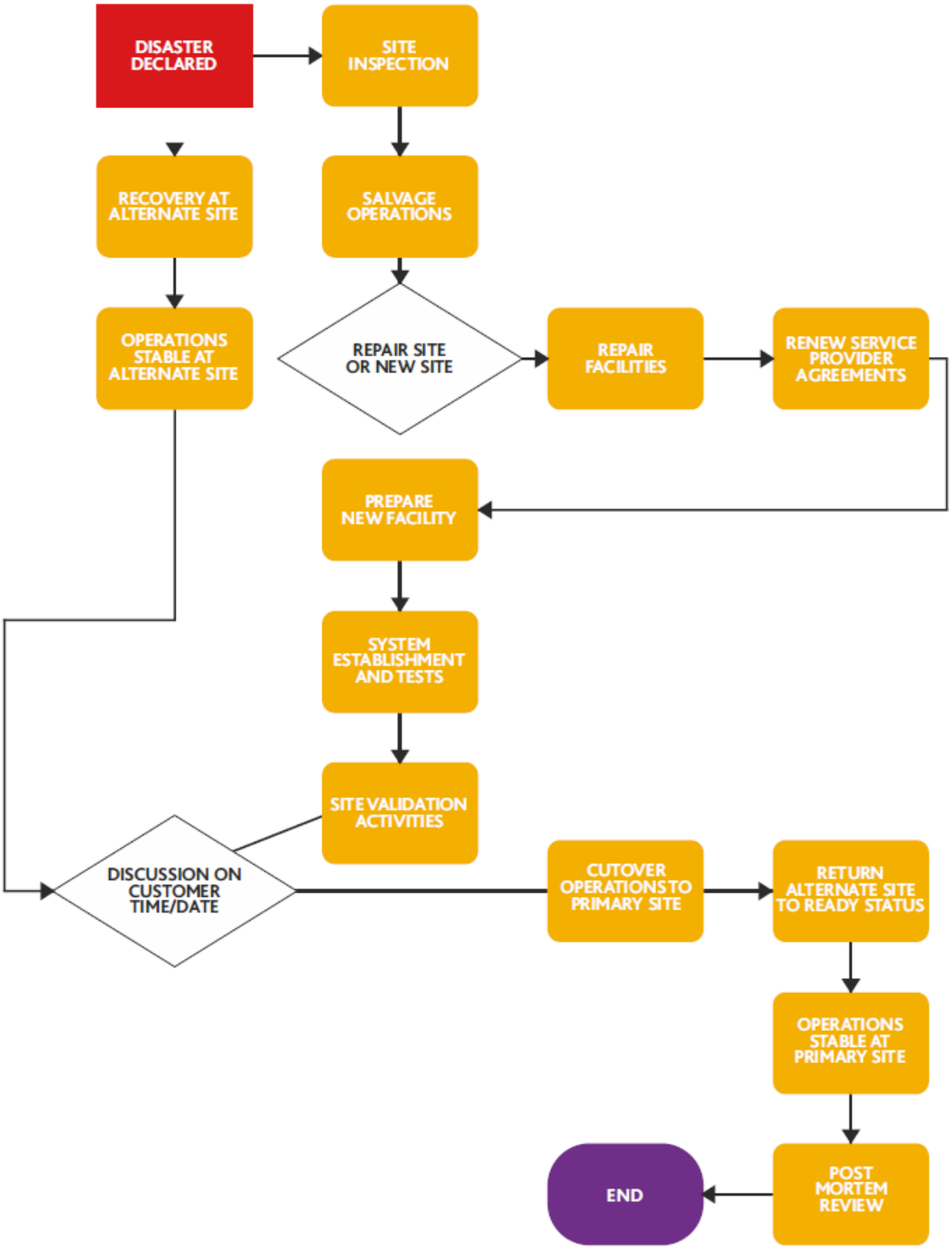

Figure 2 Business Resumption Process

5.4 POST INCIDENT REVIEW

After closure of a disaster situation and standing down of the FISCAL Response Team a post incident review of the process and how it could be improved will be conducted. This review may be conducted at the next scheduled Information Security Forum meeting.

The review shall ensure that:

- FISCAL can understand the cause, nature, and impact of the incident on the organisation and its customers.
- Financial impacts are clearly identified and documented for insurance claims or customer SLA penalties.
- 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.

6 RESILIENCE MEASURES

The following represents the main resilience measures which have been put in place by FISCAL. These measures are aimed at, where possible, preventing or reducing the likelihood of a disaster situation.

6.1 SERVER REDUNDANCY

Regardless of the specific service, the service component topology is designed using Microsoft and industry best practices for redundant deployment.

For example, the following components are deployed with active/active redundancy to keep the system up in the case of server failure:

- Highly available Web Application Firewall
- Azure Load Balancers for IIS and SFTP (AP Forensics only)
- Redundant Microsoft IIS Servers
- Redundant SFTP Servers (AP Forensics only)
- Highly available Azure Active Directory

6.2 NETWORK REDUNDANCY

Remote support and management of the service is primarily performed from the Reading, UK offices of FISCAL. Connectivity is provided via a 1000MB leased line with an ADSL backup. In the event of failure of the leased line traffic will immediately route via the ADSL backup ensuring no loss of service.

In the event of complete connectivity failure at the Reading offices, access for remote support and management will be permitted from compliant FISCAL devices using appropriate conditional access controls.

All access is via appropriately secured VPN and is audited.

6.3 DATA BACKUP AND RECOVERY

FISCAL's Services are protected by automated online backup of the configuration files and customer data files. All Customer data on the SQL Servers is compressed, encrypted, and backed up.

7 RISK MANAGEMENT

7.1 BUSINESS IMPACT ASSESSMENT

The FISCAL Service has been designed to, as far as possible, eliminate Single Points of Failure within the infrastructure. FISCAL assesses the levels of risk using the parameters outlined in the Risk Management Policy and Procedures.

8 RECOVERY TIME REQUIREMENTS

The following requirements are a result of the Business Impact Analysis process which forms part of the FISCAL business continuity programme. See also *Figure 4 Recovery Time Requirements*.

- **Maximum Tolerable Outage (MTO)**
  The maximum tolerable outage is the amount of time the service 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. The FISCAL target for MTO is 4 days.
- **Recovery Time Objective (RTO)**
  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. The FISCAL target for RTO is 3 days.
- **Recovery Point Objective (RPO)**
  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. The FISCAL target for RPO is 1 day (from Service interruption).

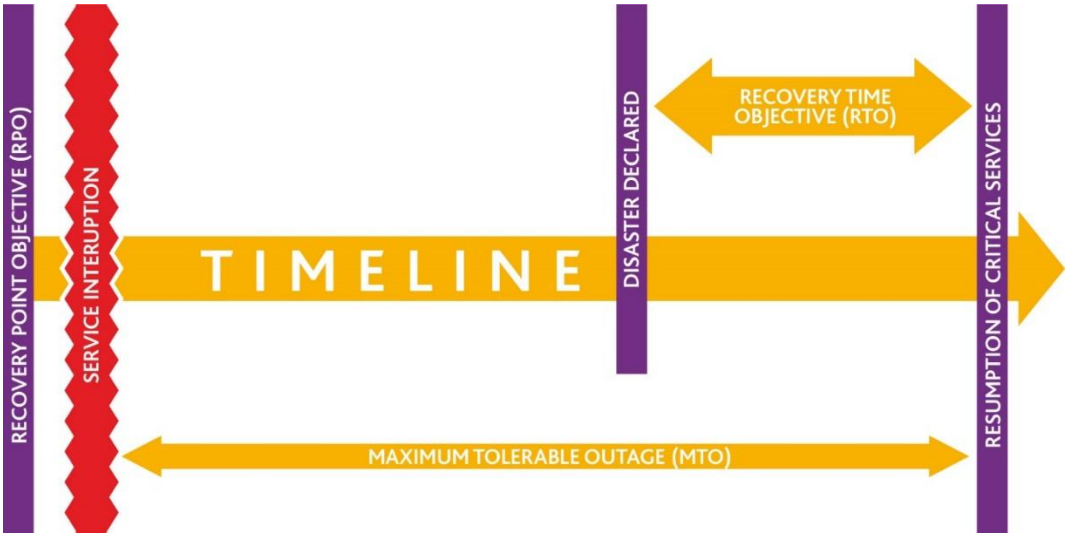

Figure 4 Recovery Time Requirements

8.1 SCOPE

This plan is devised to address a significant outage of the Service.

9 EXCLUSIONS

This Business Continuity Plan does not address:

- The recovery of any corporate functions within FISCAL during a disaster.
- Any development, test, or staging environments.
- An incident or disaster of such a scale that it renders recovery outside of the reasonable control of FISCAL. (e.g., affecting the wider metropolitan area)

10 FISCAL RESPONSE TEAM

The FISCAL Response Team includes those roles responsible for the successful execution of the BCP. Due to the size of the organisation multiple roles may be performed by the same individuals.

The FISCAL Response Team is responsible for deciding on the course of action and coordinating and undertaking all activities during the recovery period. See Figure 5 FISCAL Response Team Activities.

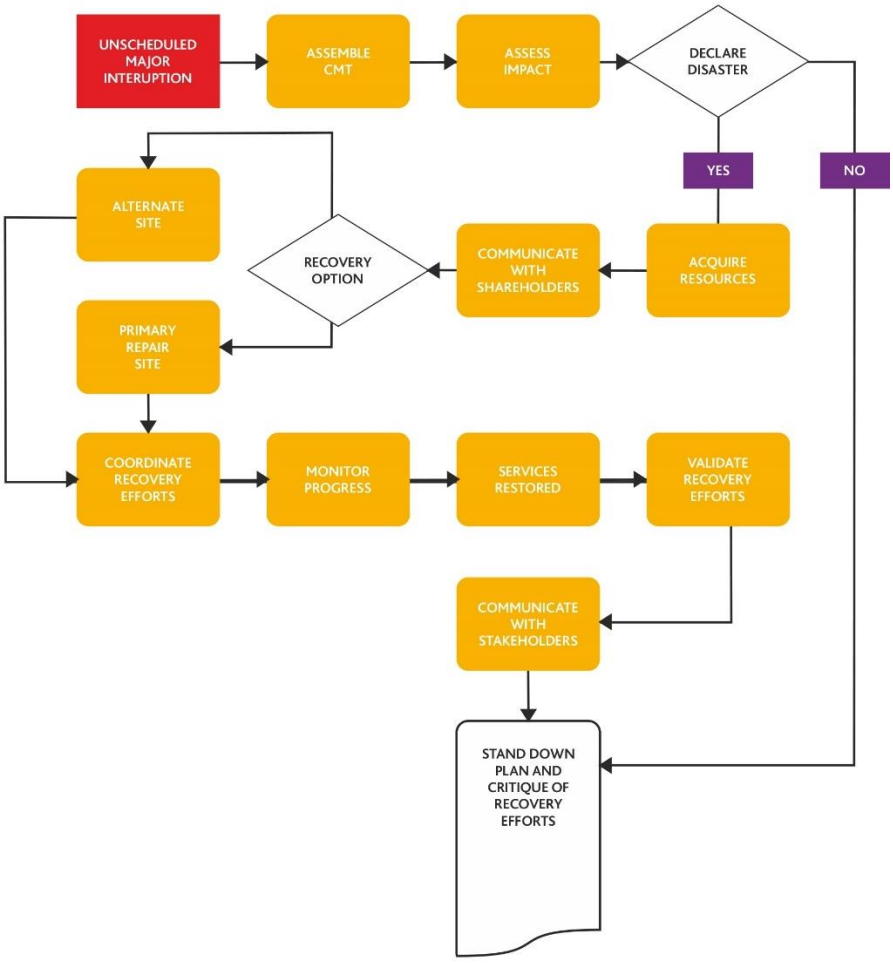

Figure 5 FISCAL Response Team Activities

11 FISCAL RESPONSE TEAM ACTIONS

No.	ACTION STEP	WHO	TIME	RESOURCES	PROCESS TIME	COMMENTS
	What do I have to do?	*Who is responsible for the step to be completed?*	*How Long will it take?*	*What additional resources are required?*	*When did I start and finish the action step?*	*What happened when I completed the action step?*
1.	Assemble Key Staff	Response Team Leader		Contact List		
2.	Assess Damage	CISO / DevOps / TISO				
3.	Decide Whether to Declare a Disaster or Not. If **YES, go to Step 6.**	Response Team Leader with input from the Team				
4.	Restore Functions at Primary Site	CISO / DevOps /TISO				
5.	Finish	Team stand down.				
6.	**DECLARE A DISASTER** Initiate recovery to alternate site	CTO, CISO, DevOps				
7.	Acquire Equipment and Supplies	CISO / DevOps /TISO				
8.	Communicate with Groups and coordinate recovery	Response Team Leader				
9.	Build New or Rebuild Primary Site	Devops / TISO				
10.	Monitor Progress	Response Team Leader				
11.	Move to New or Rebuilt Primary Site	Devops / TISO				
12.	Discontinue Use of Alternate Site	Devops / TISO				
13.	Debrief of Plan	Response Team Leader				
14.	Finish	Team stands down.				

12 FISCAL MANAGEMENT TEAM ROLES/RESPONSIBILITIES

The table below describes the skills, authority levels and responsibilities for each member of the Management Team.

	Role/Responsibility
FISCAL Response Team Leader **IT Director, CISO or equivalent**	Senior manager to oversee recovery. Authority to declare a disaster.
FISCAL Alternate Team Lead	Full authority to act if Team Leader is not available.
FISCAL Manager, Communications	Authority to speak for the organisation.
FISCAL CISO	Oversee facility, security, damage assessment, salvage and reconstruction.
FISCAL DevOps / TISO	Authority and knowledge to act in place of the team leader.
IT Director, or equivalent Director	Authority to spend the amounts required to fund recovery in the first days.
COO, or equivalent Director	Ability and authority to make legal/contractual decisions.

13 BUSINESS CONTINUITY

13.1 OVERVIEW

For the purposes of this section, Business Continuity refers to the non-technical functions and processes that enable and support the normal delivery of the Service.

13.2 APPROACH

The extent and timing of the recovery activities will vary depending upon the nature of the incident or disaster. These activities will need to be coordinated and planned as a parallel stream to re-establish stable operations.

The decision concerning the approach to re-establishing FISCAL's Service should be made as soon as practically possible after an incident or disaster occurs. This allows all the affected areas including the individual customers to adapt their procedures and staffing according to the expected length of the outage. The following should be considered when assessing incident severity.

13.3 ENVIRONMENTAL EVENT OR DISASTER

For the purpose of this plan, an Environmental Event or Disaster is fire, flood, wind, or earthquake damage that partially or fully prohibits the use of a FISCAL facility.

13.3.1 Cloud Datacentres (MS Azure)

All systems and processes are replicated within datacentres operated by Microsoft Azure within the UK, EU, and US. Failure of power, telecommunications or hardware in the Azure datacentres are designed to automatically failover with no perceived downtime.

FISCAL will take guidance from the customer during onboarding regarding the region location of the datacentre they wish to use. However, for the avoidance of doubt, by default:

- UK customer data will only be stored on and accessible by UK datacentres
- EU customer data will only be stored on and accessible by EU datacentres
- US customer data will only be stored on and accessible by US datacentres

FISCAL's risk assessment indicated that the possibility of multiple elements within our hosting partner's datacentres failing simultaneously is very unlikely – and would fall into the category of a large-scale disaster.

13.3.2 FISCAL Office (Reading)

The FISCAL Office network topology has been designed such that it is not required to be available for the service to be accessed for management and support purposes. In the event of the FISCAL Office becoming unavailable, no downtime of the service will be experienced.

13.4 LOSS OF PERSONNEL

Key personnel contracts of employment provide appropriate notice periods to ensure that recruitment for replacements can be processed within a reasonable time frame. Key personnel have nominated deputies who may assume key responsibilities for a limited period of time in the event of unplanned absence.

Support staff resourcing is monitored to ensure service level standards are maintained. The staff resourcing model is supplemented by a roster of trained additional staff who are available to support unexpected and unplanned levels of staff absence.

Succession planning is in place to identify and train personnel who can both act up for key staff for short periods of absence and also enable these staff to act up for longer unplanned periods of absence. The Risk

Assessment has considered the loss of key staff and risk treatment plans include consideration of this fact. At the early stages of any event an assessment will be carried out of staff requirements and where gaps are identified these will be filled through staff acting up, cross use of staff within the FISCAL group or recruitment from external sources.

14 DISASTER RECOVERY

14.1 OVERVIEW

This section details the approach to assessing, managing and restoring the technical and infrastructure elements of the Service.

14.2 APPROACH

The extent and timing of the recovery activities will vary depending upon the nature of the incident or disaster. These activities will need to be coordinated and planned as a parallel stream to re-establish stable operations.

The decision concerning the approach to re-establishing FISCAL's Service should be made as soon as practically possible after an incident or disaster occurs. This allows all the affected areas including the individual customers to adapt their procedures and staffing according to the expected length of the outage.

The following should be taken into account when assessing incident severity.

14.2.1 Datacentre Network or Power Failure

Failure of connectivity within the data centres.

Our hosting partners maintain redundancy and fail over systems to ensure uptime and connectivity from outside the network to the Cloud Platform is 99% available.

14.2.2 Single Server Failure

Failure of a single server within the Cloud Platform.

If a non-network or power related problem causes a FISCAL server to fail, the Cloud Platform will fail over to that server's failover partner. All elements of the platform include multiple servers to facilitate this uptime. No downtime expected.

14.2.3 Multiple Server Failure

Failure of multiple servers within the Cloud Platform (affecting our planned redundancy).

If both machines in a failover pair suffer non-network or power related problems, it is likely that the Cloud Platform would become unavailable. Immediate steps to restore one of the affected servers to full service would take place. The underlying platform's virtualisation backup features mean that all non-database systems can be restored within 1 business day. In practice, it is unlikely that all servers in an availability group would fail concurrently.

14.2.4 Management Network Failure

Failure of connectivity between the Management Network (Reading HQ) and the datacentres. See section on Network Redundancy.

15 REVIEW & AMENDMENT OF THE BCP

The plan will be reviewed annually or when a significant service or infrastructure change occurs and should be maintained as illustrated in Figure 6.

On an on-going basis, the CISO/TISO/DevOps will:

- periodically assess the conditions, status, capabilities and availability of service resiliency and backup facilities.
- perform special studies requested by the FISCAL Management Team or to improve the efficiency of equipment and recovery procedures.
- prepare periodic status reports for the Information Security Forum.
- coordinate business recovery tests with the customers and prepare test results and recommendations for plan improvement; and
- maintain and distribute this plan.

The above activities will be enforced through the ISO 27001 Management Systems.

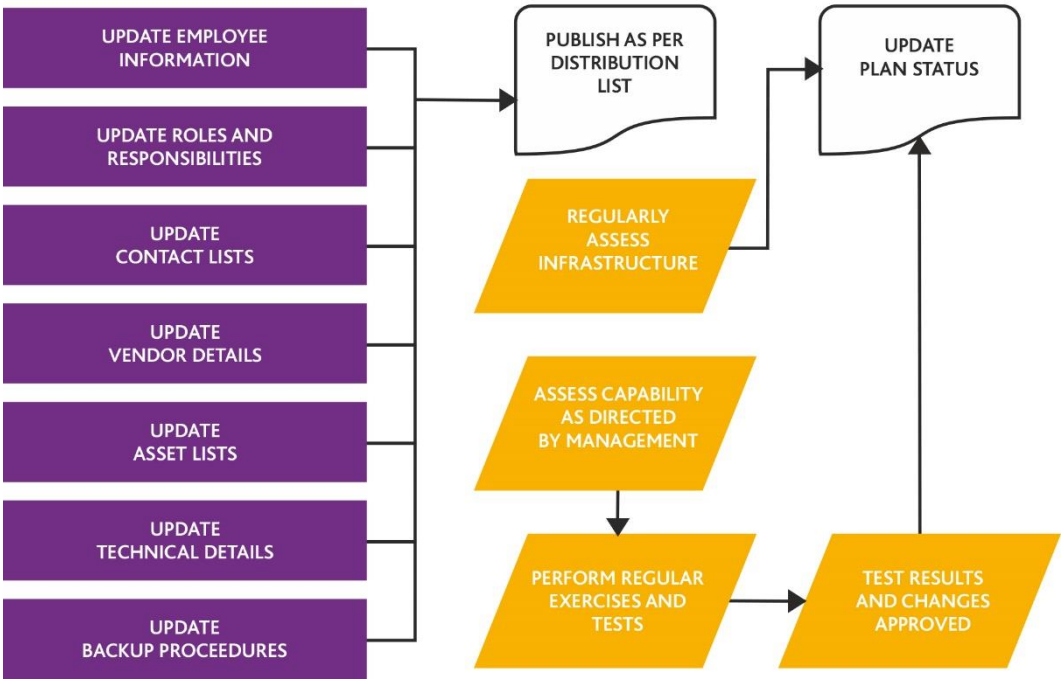

Figure 6 Maintain BCP Documentation Activities

16 TESTING OF THE BCP

In accordance with industry standards and best practice, this plan will be tested on an annual basis.

All testing activities including schedules, plans and outcomes will be recorded and provided to the Director of IT and Security for review.

16.1 TESTING OF THE TECHNICAL INFRASTRUCTURE

On an annual basis, selective desktop scenario-based tests will be executed. These tests put forward an incident or disaster scenario which is role played and predefined recovery steps tested. This testing is non-disruptive and will be used to ensure that invocation procedures are robust. This testing will not require the participation of the customers.

16.2 TESTING OF SERVICE OPERATIONS

Testing of Service Operations includes the invocation of support services to secondary sites. This testing will not require the participation of the customers.

On an annual basis, elements of the Support Operations will be invoked to a BCP site. Records of all of the above tests will be maintained.

16.3 REMEDIATION

The purpose of testing is to ensure that the plan is robust and that its evolving scope is sufficient to ensure that the service can continue after a significant event or disaster.

Following testing, any identified shortfall or opportunity for improvement will with the co-operation and agreement of stakeholders be identified and remedial measures planned and implemented as soon as possible via discussion at the ISF.

The plan will be updated to reflect any subsequent changes.