

March 2026

INTERNAL

# Business Continuity and Disaster Recovery Plan

FUNDS  AXIS

<b>Policy title:</b>	Business Continuity and Disaster Recovery plan
----------------------	--

<b>Issue</b>	5.0
<b>Approved by:</b>	Trevor Dempster
<b>Approval Date:</b>	March 2026
<b>Next Review Date:</b>	March 2027

<b>Scope:</b>	The policy applies to Funds-Axis Limited and all contractors and other people working on behalf of the company.
<b>Associated documentation:</b>	<ul style="list-style-type: none"> <li>\ Information Security &amp; Technology Control Policy</li> <li>\ Team Specific BCP Plan</li> </ul>
<b>Responsibility for Implementation &amp; Training:</b>	<p>Day to day responsibility for implementation: ISO</p> <p>Day to day responsibility for training: ISO</p>

<b>Distribution methods:</b>	<p>Methods used to communicate this policy:</p> <ul style="list-style-type: none"> <li>\ Training</li> <li>\ Communications Sessions</li> </ul>
------------------------------	---

## Contents

<b>1. Introduction.....</b>	<b>4</b>
1.1 Objectives of the Plan.....	4
1.2 Principles Behind this Plan .....	4
1.3 Plan Review and Update.....	5
1.4 Contact Information.....	5
1.5 Specific Roles and Responsibilities.....	5
<b>2. Business Overview .....</b>	<b>6</b>
2.1 Premises and Locations.....	6
2.2 Main Business Activities.....	6
2.3 Key Suppliers .....	7
<b>3. BCP Summary.....</b>	<b>8</b>
3.1 Key Systems and Infrastructure for Continuity .....	8
3.2 Summary of Continuity Events .....	8
<b>4. Backup and Recovery Arrangements.....</b>	<b>14</b>
4.1 Data Backup Procedures and Schedules.....	14
4.2 Data Restoration Procedures.....	16
<b>5. BCP Activation Procedures .....</b>	<b>18</b>
5.2 Decision-Making and Approval Process .....	18
5.3 Communication Protocols.....	19
<b>6. Training and Testing.....</b>	<b>20</b>
6.1 Employee Training on BCP and DR Procedures.....	20
6.2 Testing and Exercising the BCP and DR Plan.....	20
6.3 Lessons Learned and Improvement Actions.....	21
6.4 Key BCP Tests and Exercises Overview.....	22
<b>7. Contacts with Authorities.....</b>	<b>24</b>
7.1 Emergency Contacts and Authorities .....	24
7.2 Coordination with External Agencies.....	24
<b>8. Business Impact Analysis by Team .....</b>	<b>25</b>
8.2 Recovery Time Objectives (RTO) for Each Team.....	27
8.3 Critical Resource Identification and Allocation.....	28
<b>9. Appendices.....</b>	<b>29</b>
Appendix 1: Contact Details.....	29
Appendix 2: Team Specific BCP Plans.....	29

## 1. Introduction

The Business Continuity and Disaster Recovery Plan ("BCP/DR Plan") is a vital component of Funds-Axis's commitment to ensuring the uninterrupted delivery of services and safeguarding the interests of our clients, staff, and stakeholders.

This plan outlines the strategies, procedures, and responsibilities to be followed during critical situations to maintain maximum client service levels, facilitate swift recovery from interruptions, and minimise the likelihood and impact of disruptions.

### 1.1 Objectives of the Plan

The primary objectives of this BCP/DR Plan are as follows:

- \ **Ensure Maximum Client Service Levels:** To prioritise the continuity of client services, safeguarding their confidence in Funds-Axis's ability to meet their needs even during adverse events.
- \ **Swift Recovery from Interruptions:** To establish efficient and well-defined disaster recovery procedures that enable us to restore operations promptly, minimising downtime and impact on business operations.
- \ **Risk Mitigation:** To assess and address risks comprehensively, considering both their probability and potential business impact, in order to enhance our resilience to potential disruptions.

### 1.2 Principles Behind this Plan

This BCP/DR Plan is guided by the following principles:

- \ **Integration of Business Continuity and Disaster Recovery:** We view disaster recovery as an integral part of our broader business continuity efforts, ensuring a cohesive and comprehensive approach to operational resilience.
- \ **Comprehensive Risk Assessment:** Risks are thoroughly assessed, considering the probability of occurrence and their potential impact on business operations and service delivery.
- \ **Reasonable and Practical Plans:** Business continuity plans are designed to be reasonable, practical, and achievable, tailored to our organisation's unique needs and resources.

## 1.3 Plan Review and Update

To maintain the plan's effectiveness, it undergoes periodic review and updates. These reviews are conducted at least annually, responding to changing business requirements, client needs, and technological advancements.

## 1.4 Contact Information

Contact details of key stakeholders, including staff, customers, and key suppliers, are updated and confirmed on a quarterly basis to ensure efficient communication during significant business continuity events. Refer to Appendix 1 for contact details.

## 1.5 Specific Roles and Responsibilities

The successful implementation of the BCP/DR Plan relies on the dedication and cooperation of all staff members. Specific roles and responsibilities are assigned as follows:

- \ **CISO:** As the individual responsible for ensuring the BCP remains up-to-date and aligned with best practices, The CISO plays a central role in maintaining our operational resilience.
- \ **All Staff:** All staff members are expected to familiarise themselves with the BCP/DR Plan and maintain a high level of awareness. Specific responsibilities for each staff member are detailed within this BCP/DR plan.

## 2. Business Overview

### 2.1 Premises and Locations

Funds-Axis operates primarily from its office located in Belfast at the following address:

\ The Innovation Center, Queens Road, Belfast BT3 9DT.

The Belfast office houses approximately 30 employees and serves as the main operational centre for the organisation. The premises are equipped with computers, internet access, and telecoms to support day-to-day business activities.

Additionally, the company maintains a Virtual Office at 60 Cannon Street, London, which functions as a postal address and occasional client meeting space. However, this location does not contain any technology infrastructure or physical records.

### 2.2 Main Business Activities

Funds-Axis is primarily engaged in the following main business activities, each with specific business continuity considerations:

<p><b>Galaxy Investment Compliance Monitoring and Regulatory Reporting Services</b></p>	<p>Galaxy is a cloud-based risk and regulatory reporting application hosted on Amazon Web Services (AWS).</p> <p>For daily operations, there is limited dependency on the Funds-Axis technology environment, as Galaxy can be accessed from any computer worldwide.</p> <p>Data entered into Galaxy is regularly backed up and stored at an offsite location to ensure availability in the event of a restore. Disaster recovery procedures are tested annually to ensure readiness. Funds-Axis maintains an Auto Scaling group and utilises redundancy with 2 database instances in separate availability zones.</p> <p>The company targets a Data Recovery Point Objective (RPO) of 12 hours. Funds-Axis is responsible for the implementation, support, and maintenance of Galaxy.</p>
---	---

<b>Information Portals (ATLAS Funds Training, Global Exchanges, and Global Disclosures)</b>	<p>Funds-Axis information portals, such as ATLAS Funds Training, Global Exchanges, and Global Disclosures, are built on WordPress and hosted on AWS. The web-based portals can be maintained online from any computer globally.</p> <p>Business continuity risks for the information portals relate to content, hosting arrangements, and dependencies on AWS as a key supplier.</p>
<b>Consultancy and Training</b>	<p>Funds-Axis provides consultancy and training services to clients. Important records and documents are stored on the cloud via SharePoint, with daily backups ensuring recoverability.</p> <p>Consultancy and training sessions are conducted at client offices or training and conference venues, reducing the dependency on Funds-Axis technology infrastructure.</p>

## 2.3 Key Suppliers

Funds-Axis relies on several key suppliers to support its business activities:

1. **Microsoft Cloud Applications:** Microsoft Outlook, SharePoint, and Teams are essential tools for daily communication and collaboration.
2. **Amazon Web Services (AWS):** AWS hosts the Galaxy application and Global Portals, ensuring their availability and performance.

Funds-Axis acknowledges the criticality of these suppliers and understands the potential business continuity implications if any of them experience a continuity event.

## 3. BCP Summary

The Business Continuity Plan (BCP) serves as a comprehensive framework to safeguard the seamless operation of Funds-Axis in the face of various continuity events. This plan outlines key strategies and response measures to mitigate risks, minimise disruptions, and ensure the continuous delivery of exceptional services to our valued clients.

### 3.1 Key Systems and Infrastructure for Continuity

The continuance of our operations heavily relies on critical systems and infrastructure that enable our day-to-day functions. These include:

- \ **Galaxy:** A comprehensive cloud-based risk and regulatory reporting application empowering investment managers and depositaries with robust analytics and compliance tools.
- \ **Information Portals:** Web-based portals hosted on AWS, providing clients with reliable access to essential resources, training materials, and global disclosures.
- \ **Microsoft Cloud Applications:** A suite of essential tools, including Outlook, OneDrive, SharePoint, Teams, Word, Excel, and PowerPoint, ensuring seamless collaboration, communication, and productivity.
- \ **Internet:** A crucial lifeline connecting us to vital resources and cloud-based services, facilitating seamless communication and information flow.
- \ **PCs and Laptops:** Our workstations, enabling our talented teams to contribute their expertise and drive our success.

### 3.2 Summary of Continuity Events

The following sections provide a summary of key continuity events and the corresponding contingency actions for both our Office Based Workings and Working from Home scenarios. Each event is meticulously addressed to ensure a prompt and effective response, safeguarding our operations, and providing peace of mind to our stakeholders.

Please refer to the respective tables below for the detailed contingency actions, contacts, and timeframes for each scenario.



## Galaxy Continuity Events:

No.	Continuity Event	Contact	Contingency	Timeframe for Contingency Actions
1	Galaxy Unavailable	DevOps	Engage DevOps to diagnose and resolve the issue	Engage immediately
2	AWS Hosting Disruption	AWS Support	Activate Disaster Recovery Plan for Galaxy hosted on AWS	Initiate within 1 hour
3	Galaxy Data Corruption	Automations/ TechOps	Restore from verified backups to ensure data integrity	Restore within 4 hours
4	Galaxy Application Upgrade Issue	DevOps	Rollback to the previous stable version if feasible	Rollback within 2 hours
5	Galaxy Performance Degradation	DevOps	Investigate and optimise Galaxy configuration	Resolution within 3 hours
6	Galaxy Service Outage for Maintenance	DevOps/ Relationship Management	Plan and communicate scheduled downtime for maintenance	Announce at least 48 hours prior
7	Galaxy Service Access Restrictions	TechOps/ Cyber Security	Implement secure VPN access for authorised personnel	Enable VPN access within 1 hour
8	Critical Galaxy Report Generation Failure	Automations/ TechOps	Analyse and resolve report generation issues	Fix within 4 hours
9	Galaxy Integration Failure	Automations/ TechOps	Investigate and resolve integration issues with other systems	Resolution within 6 hours
10	Galaxy User Authentication Issues	DevOps	Ensure users can access Galaxy with alternative methods	Implement workaround within 1 hour

## Information Portals Continuity Events:

No.	Continuity Event	Contact	Contingency	Timeframe for Contingency Actions
1	AWS Hosting Server Outage	Internal IT Support	Contact IT Support team to diagnose and resolve the issue	Engage immediately
2	Website Content Loss	Internal IT Support	Restore from verified backups to ensure content integrity	Restore within 4 hours
3	Website Performance Degradation	Internal IT Support	Investigate and optimise server and website configurations	Resolution within 3 hours
4	Website Security Breach	Internal IT Support	Engage Cyber Security Team to contain and resolve the breach	Containment within 1 hour
5	Domain or SSL Certificate Expiration	Internal IT Support	Renew domain and SSL certificate to ensure website access	Renewal within 24 hours
6	Plugin or Core Update Failure	Internal IT Support	Rollback to the previous stable version if feasible	Rollback within 2 hours
7	Critical Web Page Error or Malfunction	Internal IT Support	Diagnose and resolve the issue affecting critical web pages	Fix within 4 hours
8	AWS Hosting Service Access Restrictions	Internal IT Support	Implement secure VPN access for authorised personnel	Enable VPN access within 1 hour
9	Web Portal Integration Failure	Internal IT Support	Investigate and resolve integration issues with other systems	Resolution within 6 hours

## Microsoft Cloud Applications Continuity Events:

No.	Continuity Event	Contact	Contingency	Timeframe for Contingency Actions
1	Microsoft Cloud Applications Unavailable	Internal IT Support	Engage Microsoft Support to diagnose and resolve the issue	Engage immediately
2	Data Corruption in Microsoft Applications	Internal IT Support	Restore from verified backups to ensure data integrity	Restore within 4 hours
3	Security Breach in Azure Active Directory	Internal Cyber Security Team	Engage Microsoft and use Azure Live Response to contain and resolve the breach	Containment within 1 hour
4	Ransomware Attack on Office 365 Data	Internal IT Support	Recover data from Acronis backups to restore affected data	Recovery within 6 hours
5	User Account Lockout or Authentication Issue	Internal IT Support	Investigate and resolve user account authentication issues	Resolution within 2 hours
6	SharePoint Site or Mailbox Deletion	Internal IT Support	Restore from Acronis backups to recover deleted data	Recovery within 4 hours
7	Teams Communication Disruption	Internal IT Support	Use alternative communication channels or engage Microsoft Support	Resolution within 1 hour
8	Critical Document Loss in OneDrive	Internal IT Support	Restore from Acronis backups to recover lost documents	Recovery within 4 hours
9	Excel or Word File Corruption	Internal IT Support	Restore from Acronis backups to recover corrupted files	Recovery within 2 hours
10	PowerPoint Presentation Issues	Internal IT Support	Investigate and resolve PowerPoint presentation errors	Resolution within 3 hours

## Office Based Workings Continuity Events:

No.	Continuity Event	Contact	Contingency	Timeframe for Contingency Actions
1	Office Premises Not Accessible	Weavers Court (landlord)	Home working / alternative Weavers Court offices	Engage immediately
2	Internet Not Available	BT	4G Wi-Fi Hotspots are available in addition to BT Wi-Fi	Resolution within 1 hour
3	Phoneline Down	BT	Engage BT support to resolve the phoneline issue	Resolution within 1 hour
4	Outlook Email Service Unavailable	Internal IT Support	Engage Microsoft Support to diagnose and resolve the issue	Engage immediately
5	Teams Communication Disruption	Internal IT Support	Engage Microsoft Support to diagnose and resolve the issue	Engage immediately
6	SharePoint Site Unavailable	Internal IT Support	Engage Microsoft Support to diagnose and resolve the issue	Engage immediately
7	Critical Document Loss	Internal IT Support	Restore from server backup via Acronis	Recovery within 2 hours
8	PC Infected by Malware	Internal Cyber Security Team	Perform full PC security scan and cleanup or access backed-up data	Recovery within 4 hours
9	Computers Lost/Damaged/Stolen	Dell/ Other Supplier	Use contingency machines held onsite at office and offsite, pending purchase	Recovery within 2 hours

## Working from Home Continuity Events:

No.	Continuity Event	Contact	Contingency	Timeframe for Contingency Actions
1	PC Infected by Malware	Internal Cyber Security Team	Perform full PC security scan and cleanup or access backed-up data	Recovery within 4 hours
2	Internet Not Available	Home User's ISP	Engage the home user's ISP to resolve the internet issue	Resolution within 1 hour
3	Home Address Not Accessible	Funds-Axis Office	Use the office or arrange short-term hotel room space	Engage immediately
4	Critical Document Loss	Internal Cyber Security Team	Restore from Desktop/OneDrive backup via Acronis	Recovery within 2 hours
5	Computers Lost/Damaged/Stolen	Dell/ Other Supplier	Use contingency machines held onsite at office and offsite, pending purchase	Recovery within 2 hours
6	Microsoft Cloud Applications Unavailable	Internal IT Support/ Microsoft	Engage Microsoft Support to diagnose and resolve the issue	Engage immediately

## 4. Backup and Recovery Arrangements

### 4.1 Data Backup Procedures and Schedules

Data backup is a critical aspect of our Business Continuity Plan, ensuring the preservation of essential information and minimising the impact of data loss. The following procedures and schedules are implemented to maintain comprehensive and timely backups:

#### **Galaxy Data Backup:**

To provide high availability and data resilience, Galaxy is hosted entirely on Amazon Web Services (AWS) in Europe (eu-west-1).

AWS employs a highly secure architecture and controlled data centers worldwide, with precise locations accessible only to authorised Amazon employees with legitimate business needs. Multiple physical controls are in place to prevent unauthorised access.

Funds-Axis utilise various independent systems on AWS to ensure high availability and data redundancy:

- \ **Load balancing (ALB):** Efficient traffic distribution and auto-healing capabilities.
- \ **Computing (EC2 and ECS):** Scalable and redundant compute power.
- \ **Scalable and Redundant Databases (RDS):** Data integrity and redundancy.
- \ **In-memory Queues and Caching (ElasticCache):** Data processing efficiency.
- \ **Storage (S3, EFS, and Glacier):** Secure data storage and long-term archiving.

Galaxy data, including portfolio information and regulatory reports, is automatically backed up daily on the AWS infrastructure. These backups are encrypted and securely stored offsite for data availability in case of restoration requirements.

Our backup strategy utilises AWS services for enhanced data protection and resilience. Daily backups are performed on encrypted disks, replicated across multiple geographically diverse AWS regions, ensuring redundant copies of critical information.

Our data retention policy retains multiple backup versions for a predefined period, allowing us to recover data from different points in time, providing added protection against accidental data loss or malicious actions.

To ensure high availability, Funds-Axis has set up the following arrangements for Galaxy services:

## Galaxy High-Availability Summary:

The following table summarises the backup frequencies, retention periods, and high-availability configurations for core infrastructure components hosted on AWS. These details are aligned across both the Business Continuity Plan and the Galaxy Backup & Recovery Document.

- \\ **Snapshots** are automatically initiated via AWS Backup policies within predefined backup windows.
- \\ **All backups are encrypted** and stored across AWS Availability Zones.

Service	Backup Frequency	Retention	Backup Window	High-Availability
<b>Application (EC2)</b>	Not required (immutable infra)	N/A	N/A	Yes (Auto-healing, redundancy). \\ 2 Servers. \\ 2 Availability Zones.
<b>Database (RDS)</b>	Daily + Point-in-time recovery	7 days (rolling)	Between 03:00–04:00 UTC	Yes (Auto-healing, redundancy). \\ 2 Database instances (replication). \\ 2 Availability Zones.
<b>Analytics Engine (EC2)</b>	Every 12 hours	7 days (rolling)	03:00 & 15:00 UTC	Semi (Auto-healing, no redundancy). \\ 1 Server. \\ 1 Availability Zone.
<b>FTP Server</b>	Daily	7 days (rolling)	Between 03:00–04:00 UTC	Yes (Auto-healing, redundancy). \\ 2 Servers. \\ 2 Availability Zones.

## Information Portals Data Backup:

All data hosted on AWS, including content from ATLAS Funds Training, Global Exchanges, and Global Disclosures, is backed up daily. AWS perform regular backups, allowing for data restoration in case of content loss or unintended modifications. These backups are encrypted and stored securely, providing redundant copies of our Information Portals' critical data.

Our data retention policy ensures that previous versions of the portals' content are accessible for a predefined period. This allows us to recover specific content snapshots and restore the portals to their last known good state, even in the face of unexpected events.

## Microsoft Cloud Applications Data Backup:

Microsoft 365 Business Premium, encompassing Outlook, OneDrive, SharePoint, Teams, Word, Excel, and PowerPoint, features automatic backups for SharePoint sites, Exchange Online mailboxes, and OneDrive for Business files. These backups are protected using Acronis, providing an additional layer of data protection against accidental deletion, malicious actions, or ransomware attacks.

As part of our proactive data protection measures, we perform regular backups of critical Microsoft Cloud Applications data using Acronis technology. These backups are stored securely in isolated environments within Acronis data centers, ensuring the safety and availability of our essential business data.

Our Acronis backup strategy includes maintaining multiple backup points, allowing us to restore data from various timeframes. This approach enhances our ability to recover data to a specific point in time and minimise the impact of data loss events.

## 4.2 Data Restoration Procedures

In the event of data loss or system disruptions, a swift and accurate data restoration process is essential to minimise downtime and resume operations promptly. Our data restoration procedures are as follows:

### Galaxy Data Restoration:

In the event of data loss, Funds-Axis can restore Galaxy data from the latest backup set available in AWS S3 storage. The data restoration process will be initiated immediately upon confirming the scope of the data loss and identifying the relevant backup.

Our Recovery Point Objective (RPO) for Galaxy is set at a maximum of **12 hours**. This means that in the event of a data loss incident, we aim to recover Galaxy data to a state no older than 12 hours before the incident occurred. By adhering to this RPO, we ensure that the impact of data loss is minimised, and we can resume operations with minimal loss of information.

The Recovery Time Objective (RTO) for Galaxy is set at a maximum of **3 hours**. This RTO reflects our commitment to restoring Galaxy functionality within 3 hours of a disruption. Our DevOps team follows predefined restoration procedures to ensure a structured and efficient recovery process, focusing on minimising downtime and restoring services as quickly as possible.

Throughout the data restoration process, our teams work diligently to verify the integrity of the restored data and confirm that Galaxy operates as expected. Rigorous testing and verification procedures are employed to ensure the accuracy and consistency of the recovered data.



By aligning our data restoration efforts with defined RPO and RTO metrics, we demonstrate our dedication to maintaining a high level of data resilience and ensuring that Galaxy remains a reliable and secure platform for our clients.

## **Information Portals Data Restoration:**

In the event of data loss or unintended modifications, our Information Portals hosted on AWS can be swiftly restored to their latest state. AWS performs regular backups, allowing for seamless data restoration in case of content loss or unintended modifications.

Our Recovery Point Objective (RPO) for Information Portals is set at a maximum of 12 hours. This means that in the event of a data loss incident, we aim to recover the Information Portals to a state no older than 12 hours before the incident occurred. By adhering to this RPO, we ensure that any potential loss of content is minimised, and users can access the most recent version of the portals.

The Recovery Time Objective (RTO) for Information Portals is set at less than 1 hour. This RTO indicates our commitment to swiftly restoring the functionality of the Information Portals after a data loss event. Our IT and Cyber Security teams collaborate to execute the data restoration process promptly and efficiently.

## **Microsoft Cloud Applications Data Restoration:**

Microsoft 365 Business Premium's Acronis-powered backups enable us to restore data from a specific point in time. Our data restoration process involves accessing Acronis backups and restoring the required data to its original location within the Microsoft applications.

Our Recovery Point Objective (RPO) for Microsoft Cloud Applications is set at 0 (ZERO), meaning that we aim to recover data with no data loss. With Acronis-powered backups, we can restore data to the exact state it was in before any data loss incident, ensuring that no critical information is permanently lost.

The Recovery Time Objective (RTO) for Microsoft Cloud Applications is set at less than 1 hour. This RTO reflects our commitment to rapidly restoring Microsoft Cloud Applications functionality after a data loss event.

Our IT and Cyber Security teams work closely with Microsoft's support to coordinate the data restoration process effectively. By leveraging Acronis backups and following rigorous restoration procedures, we ensure a smooth and swift recovery process, minimising any impact on business operations.

With these comprehensive data backup and restoration arrangements, Funds-Axis is committed to maintaining data integrity, high availability, and swift recovery in the face of

unexpected events. Our Business Continuity Plan is designed to safeguard our operations and clients' interests, ensuring that disruptions are minimised and our services remain resilient and reliable.

## 5. BCP Activation Procedures

### 5.1 Conditions for Activating the BCP and DR Plan

The Business Continuity Plan (BCP) and Disaster Recovery (DR) plan can be activated under the following conditions:

#### **Trigger Events:**

The BCP and DR plan may be activated in response to the occurrence of various trigger events, including but not limited to:

1. Fire or Flood incidents that pose a threat to office premises or IT infrastructure.
2. Utilities Failure (e.g., power outage) affecting critical operations.
3. Server Failure causing a significant disruption to key systems.
4. Telecommunications Failure impacting communication channels.
5. Civil Incidents, such as riots or civil unrest, that disrupt normal operations.
6. Health Pandemics (e.g., Covid-19) affecting workforce availability or operations.

#### **Decision for Activation:**

Any Director of the company is authorised to initiate the activation of the BCP and DR plan. Once the trigger event has been identified and confirmed, the Incident Manager, in consultation with the Senior Management team and the Information Security Officer, will assess the severity and impact of the event to determine whether the BCP should be activated.

### 5.2 Decision-Making and Approval Process

#### **Incident Management Team:**

Upon activation of the BCP and DR plan, an Incident Management Team (IMT) will be formed. The IMT will be responsible for making critical decisions and coordinating the response to the incident.

#### **Roles and Responsibilities:**

\\ **Incident Manager:** The Incident Manager, who can be any Director, a member of the Senior Management team, or the Information Security Officer, is appointed to lead the IMT. The Incident Manager will oversee the response, communicate decisions, and ensure the efficient execution of the BCP.

\\ **Information Gathering and Log Keeping:** A designated team member will start a log of information received, decisions made, and actions taken throughout the incident response.

\\ **Resource Identification and Allocation:** The Incident Manager will identify suitable locations for the IMT and coordinate the availability of essential resources, such as communication equipment, alternative office spaces, and emergency supplies.

\\ **Communication and Coordination:** The IMT will be responsible for liaising with relevant stakeholders, including employees, clients, business partners, Health & Safety officials, and Emergency Services as required.

\\ **Impact Assessment and Prioritisation:** The IMT will assess the damage or disruption caused by the incident and prioritise critical activities and resources to ensure a coordinated recovery effort.

\\ **Decision-Making:** The Incident Manager, in collaboration with the IMT, will decide on the appropriate course of action, taking into account the critical functions and resources necessary for business continuity.

\\ **Staff and Stakeholder Communication:** The IMT will ensure that timely and accurate communications are issued to staff, clients, business partners, and other relevant stakeholders regarding the incident, actions taken, and recovery progress.

\\ **Business Continuity Plan Review:** The IMT will review and evaluate the effectiveness of the BCP during and after the incident, identifying any areas for improvement or updates.

## 5.3 Communication Protocols

### Internal Communication:

During the activation of the BCP and DR plan, the IMT will utilise pre-established communication channels to share information and decisions with all staff members.

Regular updates will be provided to keep employees informed about the incident and the recovery efforts.

### External Communication:

The IMT will liaise with clients, business partners, regulatory authorities, and other external stakeholders to keep them informed about the incident and the measures being taken to mitigate its impact.

Clear and accurate communications will be provided to external parties throughout the response and recovery process.

### **Communication Escalation:**

If the incident escalates or requires additional support or expertise, the Incident Manager has the authority to escalate communication to higher management, company Directors, or relevant authorities as necessary.

### **Review and Updates:**

The IMT will regularly review and update the communication protocols to ensure they remain effective and aligned with the company's business continuity objectives. Feedback from incidents will be used to improve the communication process and enhance response efficiency.

By incorporating these additional details, your BCP Activation Procedures section will provide a clearer outline of the processes and responsibilities during plan activation and help ensure a well-coordinated and effective response to various continuity events.

## **6. Training and Testing**

### **6.1 Employee Training on BCP and DR Procedures**

Training employees on Business Continuity Plan (BCP) and Disaster Recovery (DR) procedures is essential to ensure that all staff members understand their roles and responsibilities during a continuity event. The following training arrangements are in place:

\\ **Induction Training:** All new staff members undergo BCP awareness training as part of their induction process. This training familiarises them with the BCP objectives, key procedures, and their roles in executing the plan.

\\ **Annual BCP Awareness Briefings:** Regular briefings are conducted to update all staff on BCP awareness and any changes or updates to the plan. These briefings reinforce the importance of business continuity preparedness and ensure that employees remain aware of the locations of BCP documents.

\\ **Incident Response Team Training:** Staff members designated to invoke the BCP or be part of the Incident Response Team receive specialised training and briefings tailored to their roles and responsibilities.

### **6.2 Testing and Exercising the BCP and DR Plan**

Routine testing and exercising of the BCP and DR plan are crucial to evaluate its effectiveness, identify gaps, and ensure that employees are familiar with their roles during a real incident. The following elements are tested as part of the company's BCP testing process:

\\ **Data Integrity and Backup:** Regular testing of data integrity and backup procedures is essential to ensure the preservation of critical information and minimise the impact of data loss. Funds-Axis conducts routine checks and simulations to verify that all data, including Galaxy, Information Portals, and Microsoft Cloud Applications, is being properly saved and backed up as per the defined backup schedules. These tests help identify any discrepancies or potential issues with data backup procedures, allowing us to take corrective measures promptly.

\\ **Recovery Capabilities:** Testing the recovery capabilities of Galaxy, Information Portals, and Microsoft Cloud Applications is crucial to evaluate their resilience and readiness to handle continuity events. Funds-Axis performs simulated recovery exercises to validate the failover mechanisms and auto-healing capabilities of each component. These exercises ensure that our systems can seamlessly recover and continue operations in the event of server failures, data loss, or disruptions.

\\ **Restoration Timeframes:** Determining restoration timeframes is a critical aspect of our BCP and DR plan. Funds-Axis conducts regular assessments to validate the restoration timeframes for Galaxy, Information Portals, and Microsoft Cloud Applications. These assessments ensure that data can be restored within the specified Recovery Point Objectives (RPOs) and Recovery Time Objectives (RTOs). Any deviations from the desired timeframes are addressed promptly to maintain business continuity.

\\ **Annual Key IT Supplier Review:** To uphold the integrity of our BCP and DR plan, Funds-Axis performs an annual review of key IT suppliers, including those responsible for Galaxy, Information Portals, and Microsoft Cloud Applications. This review assesses the performance, reliability, and security of our IT suppliers' services to ensure they meet our business continuity requirements. Any identified areas for improvement or potential risks are addressed with the respective IT suppliers.

\\ **BCP Contact Details:** Maintaining up-to-date contact details is crucial during continuity events. Funds-Axis regularly updates and distributes the contact details of the Incident Response Team, Incident Managers, and other key personnel involved in the BCP and DR processes. These contact details include primary and alternate means of communication, ensuring that all essential personnel can be reached promptly in case of plan activation.

## 6.3 Lessons Learned and Improvement Actions

Following each test or exercise, a comprehensive review of the results is conducted to capture lessons learned and identify areas for improvement. Key personnel involved in the testing process participate in a post-test debriefing session to discuss findings and propose

enhancement actions. The lessons learned are then documented and analysed to implement necessary improvements to the BCP and DR plan.

## 6.4 Key BCP Tests and Exercises Overview

### Galaxy:

Test Type	Description
Galaxy Data Backup Test	Validate the adequacy of Galaxy data backups and their secure storage in offsite locations. Ensure successful restoration of critical data within the Recovery Point Objective (RPO).
Galaxy Application Test	Test the resilience and availability of the Galaxy application by simulating various failure scenarios and validating the auto-healing and redundancy mechanisms.
Galaxy Database Failover Test	Evaluate the Galaxy database failover process to verify seamless transition to the standby database and minimal impact on data access.
Galaxy Sisense Build Test	Confirm the successful execution of the daily Sisense build process, ensuring that the data is available for timely decision-making and reporting.
Galaxy Easymorph Test	Validate the reliability of Easymorph batch builds and identify and address any errors that may impact data processing and reporting.
Galaxy FTP Server Test	Test the FTP server's functionality and data transfer capabilities to ensure smooth operations for clients and secure data transmissions.

### Information Portals:

Test Type	Description
Information Portals Data Backup Test	Verify the adequacy of data backups for Information Portals, ensuring that all content from ATLAS Funds Training, Global Exchanges, and Global Disclosures is appropriately backed up.
Information Portals Content Test	Evaluate the integrity and availability of content within Information Portals by conducting tests to ensure proper access and display of information for users.
Information Portals Hosting Test	Validate the functionality of AWS hosting services by simulating various scenarios to assess their ability to recover and restore portal data.
Information Portals Performance Test	Assess the performance and responsiveness of Information Portals, ensuring that they can handle the expected user load and deliver content efficiently.
Information Portals Security Test	Conduct security testing to identify and address potential vulnerabilities in Information Portals, ensuring data protection and safeguarding against cyber threats.

### Microsoft Cloud Applications:

Test Type	Description
Microsoft Cloud Applications Data Backup Test	Validate the effectiveness of data backups for Microsoft 365 Business Premium, including Outlook, OneDrive, SharePoint, Teams, Word, Excel, and PowerPoint, to ensure data availability and recoverability.

Microsoft Cloud Applications Data Restoration Test	Test the data restoration process from Acronis backups, ensuring the ability to recover specific data from various points in time within Microsoft applications.
Microsoft Cloud Applications User Access Test	Verify the accessibility and usability of Microsoft Cloud Applications by conducting tests to ensure that users can access and utilise the applications from various devices and locations.
Microsoft Cloud Applications Collaboration Test	Assess the collaborative features of Microsoft Teams and SharePoint, testing communication, file sharing, and document collaboration capabilities to facilitate effective remote work.
Microsoft Cloud Applications Security Test	Conduct security assessments to identify and address potential vulnerabilities within Microsoft Cloud Applications, safeguarding against unauthorised access and data breaches.

## Office Based Workings:

Test Type	Description
Office Premises Accessibility Test	Evaluate the accessibility and usability of the main office premises and alternative sites (Hotel/Hub Offices) to ensure that staff can operate effectively during continuity events.
Internet and Telecoms Connectivity Test	Verify the availability and reliability of internet connections and telecommunications to ensure seamless communication and access to critical systems.
PC and Laptop Functionality Test	Test the functionality of PCs and laptops, including hardware, software, and remote access capabilities, to ensure staff can work efficiently from various locations.
Document Retrieval and Restoration Test	Validate the process of retrieving and restoring critical documents from cloud-based storage and local backups to minimise data loss and support operational continuity.
Communication Protocols Test	Test communication protocols to ensure timely and effective dissemination of information among staff, management, and stakeholders during continuity events.
Alternative Working Arrangements Test	Conduct exercises to verify the effectiveness of alternative working arrangements, such as working from home or using contingency office spaces, for business operations.

## Working from Home:

Test Type	Description
Home Internet and Telecoms Connectivity Test	Verify the availability and reliability of internet connections and telecommunications in employees' home environments to ensure seamless communication and system access.
Work Device Functionality Test	Test the functionality of employees' work devices (e.g., laptops, PCs) used for remote work, including hardware, software, and VPN connectivity, to ensure productivity.
Document Retrieval and Restoration Test	Validate the process of retrieving and restoring critical documents from cloud-based storage and local backups in employees' home setups to minimise data loss.



Communication Protocols Test	Test communication protocols to ensure timely and effective dissemination of information among remote employees, management, and stakeholders during continuity events.
Alternative Working Arrangements Test	Conduct exercises to verify the effectiveness of alternative working arrangements, such as using 4G Wi-Fi hotspots or temporarily working from the office if necessary.
Data Security and Privacy Compliance Assessment	Conduct assessments to ensure remote employees comply with data security and privacy policies to safeguard sensitive information during remote work.

By regularly conducting a variety of BCP tests and exercises, Funds-Axis can proactively identify areas for improvement, enhance response capabilities, and increase the overall resilience of the BCP and DR plan.

## 7. Contacts with Authorities

### 7.1 Emergency Contacts and Authorities

During emergency situations, it is essential to have quick and direct access to the appropriate authorities for immediate assistance. Funds-Axis maintains the following emergency contact numbers for essential services:

- \ **Police Emergency:** 999
- \ **Police Non-Emergency (Northern Ireland):** 0845 600 8000
- \ **Ambulance:** 999
- \ **Hospital (Royal Group of Hospitals):** 028 9063 4700
- \ **Fire & Rescue:** 999
- \ **Landlord (Catalyst):** 028 9073 7800

### 7.2 Coordination with External Agencies

In the event of a major disruption or disaster, Funds-Axis recognises the importance of coordinated efforts with external agencies and partners to ensure a timely and effective response. We maintain communication channels and coordination protocols with the following external agencies:

- \ **Emergency Services:** We coordinate with local emergency services, including police, fire, and ambulance, to ensure a swift response and collaboration during emergency situations.
- \ **Insurance Broker (Integra):** Our insurance broker, Integra, plays a crucial role in the event of an insurance claim. We have established communication channels to facilitate the claims process and ensure a smooth resolution.
- \ **Utility Companies:**
  - **NIE Networks:** 03457 643 643 (for electricity supply disruptions)



- **Northern Ireland Water Leakline:** 0800 028 2011 (for reporting lack of water supply)
- **Floodline:** 0300 2000 100 (for reporting flooding incidents)
- **Waterline:** 03457 440088 (for flooding from burst watermain or blocked sewers)

By maintaining these contacts and coordination arrangements, Funds-Axis aims to ensure a comprehensive and efficient response during emergency situations and maintain compliance with regulatory requirements.

## 8. Business Impact Analysis by Team

The Business Impact Analysis (BIA) is crucial for identifying and assessing the potential impact of continuity events on critical business functions across various teams and departments. The table below outlines the impact analysis of each team, including the example of impact to service, client impact, and internal impact:

Team	Example of Impact to Service	Client Impact	Internal Impact
Technology - Infra	IT infrastructure supports critical business operations. Timely resolution of infrastructure issues and maintenance is essential to minimise disruptions and maintain system availability.	Moderate to Significant	Moderate to Significant
Technology - Developers	Developers play a vital role in implementing changes and resolving application-related issues. Prompt resolution of development-related concerns is crucial to ensure seamless service delivery.	Moderate to Significant	Moderate to Significant
Technology - BA / Testing	Business analysts and testing teams are essential for implementing changes and ensuring application quality. Efficient testing and prompt bug resolution are critical for service continuity.	Moderate to Significant	Moderate to Significant
Investment Compliance & Risk	Clients rely on the Company to meet their daily investment compliance requirements. Daily investment compliance processes, including data analysis, reporting, and risk assessments, must be completed to avoid breaches of SLAs/agreements.	Moderate to Significant	Moderate to Significant
Liquidity Risk	Clients depend on the Company to fulfil their daily liquidity risk requirements. Daily liquidity risk processes, such as liquidity analysis, forecasting, and reporting, must be executed to prevent SLA/agreement violations.	Moderate to Significant	Moderate to Significant

EU Regulatory Reporting	Clients rely on the Company to meet their daily regulatory reporting obligations. Daily reporting processes, data submissions, and filing activities are essential to avoid SLA/agreement violations and regulatory non-compliance.	Moderate to Significant	Moderate to Significant
US Regulatory Reporting	Clients rely on the Company to meet their daily regulatory reporting obligations. Daily reporting processes, data submissions, and filing activities are essential to avoid SLA/agreement violations and regulatory non-compliance.	Moderate to Significant	Moderate to Significant
Shareholder Disclosures	Clients depend on the Company to meet their daily shareholder disclosures requirements. Daily disclosure processes, data verification, and reporting are crucial to prevent SLA/agreement breaches and regulatory non-compliance.	Moderate to Significant	Moderate to Significant
Alternatives Assets	Clients rely on the Company to meet their daily regulatory reporting requirements. Daily reporting processes, data submissions, and filing activities are essential to avoid SLA/agreement violations and regulatory non-compliance.	Moderate to Significant	Moderate to Significant
Investor Comms	Communication with investors is critical for maintaining relationships and providing timely updates. Investor communication processes, including reporting and engagement, must be carried out to avoid client dissatisfaction.	Minor to Moderate	Minor to Moderate
Global Exchanges	Delays in updating Portal information and other client interactions do not have immediate or same-day criticality.	Low	Low
Projects & Automation	Main client reliance is for implementations of changes, such as additional funds, rule changes, or new client onboarding. These are less time-dependent than BAU activities.	Minor to Moderate	Minor to Moderate
Finance	Specific Finance systems (QuickBooks and Online Banking) can be accessed via the internet to manage finance activities.	Low	Low
Brand and Marketing	Primarily focused on marketing activities and dealing with potential	Low	Low

	new clients/sales prospects. Non-critical.		
Relationship Management	Building and maintaining client relationships is crucial for client retention. Regular communication and engagement with clients must be upheld to prevent client attrition and dissatisfaction.	Minor to Moderate	Minor to Moderate
HR	HR plays a pivotal role in managing employee well-being and workforce continuity. HR processes, including payroll, benefits, and employee support, must be maintained to sustain the organisation's workforce.	Minor to Moderate	Minor to Moderate
Cyber Security	Cybersecurity is crucial for protecting sensitive data and preventing security breaches. Prompt detection and mitigation of cybersecurity incidents are essential to safeguard client data and business operations.	Moderate to Significant	Moderate to Significant

## 8.2 Recovery Time Objectives (RTO) for Each Team

The Recovery Time Objective (RTO) represents the maximum acceptable downtime for each critical business function in the event of a continuity event. The RTO is defined in terms of hours, and it indicates how quickly each team should recover its operations. The RTO for each team is as follows:

- \ Technology - Infra: 3 hours
- \ Technology – Developers: 8 hours
- \ Technology - BA / Testing: 8 hours
- \ Investment Compliance & Risk: 4 hours
- \ Liquidity Risk: 4 hours
- \ EU Regulatory Reporting: 6 hours
- \ US Regulatory Reporting: 6 hours
- \ Shareholder Disclosures: 6 hours
- \ Alternatives Assets: 6 hours
- \ Investor Comms: 8 hours
- \ Global Exchanges: 8 hours
- \ Projects & Automation: 12 hours
- \ Finance: 12 hours
- \ Brand and Marketing: 24 hours
- \ Relationship Management: 8 hours
- \ HR: 6 hours
- \ Cyber Security: 4 hours

## 8.3 Critical Resource Identification and Allocation

During continuity events, certain critical resources may be in high demand, and their efficient allocation is essential for business continuity. Funds-Axis identifies and allocates critical resources to support each team's recovery process. These resources may include:

- \ Data Centers and IT Infrastructure
- \ Key Personnel and Expertise
- \ Communication Systems
- \ Office Space and Alternative Work Sites
- \ Financial Resources
- \ External Vendors and Suppliers

By conducting a thorough business impact analysis and defining recovery time objectives, Funds-Axis ensures that each team's critical functions are prioritised during recovery efforts, thereby minimising the impact of continuity events on business operations and stakeholders.

## 9. Appendices

### Appendix 1: Contact Details

- \ Staff Contact Details [Redacted]
- \ Customer Contact Details [Redacted]
- \ Other Key Contact Details [Redacted]

### Appendix 2: Team Specific BCP Plans

- \ Investment Compliance & Risk team BCP
- \ Liquidity Risk team BCP
- \ EU Regulatory Reporting team BCP
- \ US Regulatory Reporting team BCP
- \ Shareholder Disclosures team BCP
- \ Alternatives Assets team BCP
- \ Investor Comms team BCP
- \ Global Exchanges team BCP
- \ Projects & Automation team BCP
- \ Finance team BCP
- \ Brand and Marketing team BCP
- \ Relationship Management team BCP
- \ HR team BCP
- \ Cyber Security team BCP