



Business Continuity Management System: Business Continuity Policy

Contents

1. Scope	3
2. Objectives of the BCMS	3
3. Establishing leadership and resources to implement BCMS	3
4. Business Continuity and relevant documents review arrangements	4
5. Business Continuity Training	4
6. Exercising	5
7. Yondr BCM Policy	5
Version Control	7

1. Scope

This project covers all the operations of Yondr Group (Yondr) in their sites (not JVs).

The mission statement and scope is the provision of land acquisition, data center design, data center build management and operation of data centers.

The Business Critical Activities are identified in the Business Impact Analysis (BIA) and their recovery objectives set. None of the activities of Yondr are excluded from the scope, including any outsourced activities.

There is no statutory obligation to have a Business Continuity Management System (BCMS), but it is best practice and therefore sponsored by the Board and adds protection for Yondr's clients and interested parties. It is in place to safeguard the public, staff and clients of Yondr and ensure that their interests are protected to the highest standard.

The acceptable risk for Yondr is low – i.e. risk averse as a rule. In the risk matrices, risks and impacts are scored pessimistically. Any material risks which could physically harm the organisation are considered with high importance. Each risk in the risk assessment is treated on its own merit.

The purpose of the Business Continuity Plan (BCP) is ultimately to ensure that Yondr can recover from business interrupting events, can continue to meet stakeholder requirements with minimal disruption and can remain a profitable concern.

2. Objectives of the BCMS

This project reviews the operations of the organisation from 2020. The Business Continuity Management System (BCMS) is in place to monitor, review, maintain and improve the business continuity arrangements, and to keep documentation and processes up to date to reflect the changing nature of the company.

Specifically to:-

- Ensure that there is no material impact on interested parties from disruption to Yondr's functions. Feedback is monitored to ensure that there is no or minimal disruption to services as a result of business continuity incidents.
- Meet any future regulatory and / or statutory requirements for business continuity.
- Create a level of reassurance with new and existing interested parties by demonstrating that the unexpected has been planned for.
- Monitor and act on the level of risk from current threats or accept the level of risk within the risk appetite of the organisation. The risk register is reviewed periodically and as part of the management review and maintenance procedures. This is to occur quarterly (or earlier if there is a material change to the organisation).
- Ensure all staff are aware of the emergency response actions, Business Continuity Policy and Business Continuity Plan. This is through training for all staff and their participation in business continuity exercises.

3. Establishing leadership and resources to implement BCMS

The BCMS is the overall responsibility of the Board although the first line of reporting is to the COO Global Data Centre Operations. The Board are regularly updated on the BCMS. Biscon Planning (a specialist business continuity consultancy) are retained to provide support for the BCMS.

The organisation has established three levels of Incident Management Teams – a Strategic IMT (which largely consists of the ELT) who are responsible for the strategic decision making, and a Tactical Team (which consists of the various Heads of Department) who are responsible for overseeing incidents. Furthermore, are the Bronze Teams responsible for the Operational response.

4. Business Continuity and relevant documents review arrangements

Document	Document Summary	Frequency	Responsible
Business Continuity Policy	Details the organisations policy and approach to Business Continuity	Yearly Review	Board
Business Impact Analysis (BIA)	Identifies the business critical activities, resources requirements, recovery timescales and impacts of not performing activities.	Half-yearly Review	Project Manager
Corporate Business Continuity Plan (BCP)	The organisation's Business Continuity Plan providing invocation criteria and procedures, high level response and roles / responsibilities of personnel.	Half-yearly Review	Project Manager
Summary Office / Data Center BCPs	Location specific response / escalation Plans which contain appropriate contact details.	Half-yearly Review	Location specific lead officers
Crisis Communications Plan	Procedures for dealing with communications, media and PR in relation to Business Continuity incidents.	Half-yearly Review	Director of Marketing and Communications
Business Continuity Exercise	Sessions arranged for training staff and testing / exercising the Business Continuity arrangements	Minimum two Exercise pa	Project Manager / Biscon

5. Business Continuity Training

The Incident Management Teams (IMTs) will be trained in implementation and use of the BCP. Training will be refreshed during the exercise sessions or other appropriate training sessions, e.g. media training.

All staff have training through the Learning Management System and on Induction.

6. Exercising

Exercising gives an opportunity to check procedures, resource requirements, timelines and that the plan is 'fit for purpose'. A desktop exercise will be undertaken periodically (at least twice pa). To achieve this, a series of planned and interlinked exercises will be devised with a progression of scope and complexity. The programme will:

- Exercise the technical, administrative, procedural and other operational systems of the BCP.
- Exercise the Business Continuity Management (BCM) arrangements and infrastructure (including roles, responsibilities, and any incident management locations and resource requirements stipulated).
- Validate the technology and telecommunications recovery, including the availability and relocation of staff.
- Include testing recovery sites and critical vendors, where appropriate.

7. Yondr BCM Policy

The BCMS will help to ensure that Yondr can deliver projects and services to clients to an acceptable level in an acceptable timescale and meet service level agreements. The policy is appropriate to Yondr's business activities, defines the business continuity objectives (including any limitations and exclusions) and is promoted within the business culture. Staff are aware of the Policy and it is reviewed as part of the management review process or when significant change occurs. The BCM project has been planned and delivered to an established timescale and budget. It is supported from the highest levels of the business – they have been involved in the exercises and establishment on the Plans.

The specific objectives for the BCMS are listed in Section 2 and the Scope in Section 1.

The Board has the overall responsibility for BCMS. The Board will sign off on the final version of the Policy; the Project Manager maintains and signs off on all the others including the Risk Assessment and level of residual risk.

BCM is an ongoing process implemented in new projects, incorporated in change management and embedded by regular exercising and review. Where there are failings in the System identified (such as vendor resilience issues or a failure of IT Disaster Recovery testing) then the issue will be highlighted in the Risk Assessment and / or Non-Conformance log.

Business Critical Activities have been identified, taking advantage of the skills and knowledge of the people in Yondr. Internal and third-party skills are utilised, risks assessed and addressed and business impacts analysed. Yondr have put in place a response mechanism to identify incidents and to deal with them either by using a buffer time to put recovery actions on standby, by returning to normal business operations, or by invoking the Business Continuity Plan (BCP).

The tasks to be performed to recover operations, dependent on both internal and external resources, will be recorded in the BCP. The interests of staff, clients and stakeholders are protected and the information is available to keep all parties informed. Recovery options have


been reviewed and effective solutions implemented. There is a section of the Business Continuity Plan which considers the type and scale of an incident and assists with the possible actions needed.

The recovery strategy makes use of various elements, depending on the type of incident. Highlights are:-

- There are no unique skill sets within the organisation and third-party staff can be used for some roles if there is a people based incident.
- Critical staff are able to work from home (proven during the COVID-19 Pandemic).
- Critical IT systems are hosted in G-Suite and Azure across separate nodes. Data is backed up within the primary node every hour and overnight to the secondary node.
- Hard copy documents are scanned to the network when necessary.
- Critical vendors will be audited to check that they have suitable Plans in place to mitigate a potential impact to Yondr's operations and interested parties.
- There is no over reliance on transport networks.
- Crisis Communications have been planned for, using inhouse and external resources and various media to communicate in a suitable timescale.

There is a procedure for control of the records and documentation of the BCMS and the Project Manager can be consulted to ensure that the correct documents are being used and old ones destroyed. This BCMS Policy and edited versions of the Plan may be shared with interested parties, where appropriate.

Signed for Yondr on behalf of the Board:

Signature		Signature	
Full name	<u>Paul Hoos</u>	Full name
Date	<u>17th August 2022</u>	Date

Version Control

Version	Date	Notes	Expiry
1.0	May 2020	First draft – to be presented to the Board	
1.1	May 2020	Sections 3-6 added	
1.2	Jun 2020	IMT changed to CMT	
1.3	July 2021	Reword Scope	
1.4	30 July 2021	Formatting changes	
Rev 002	10 Aug 2021	Review frequency aligned to ISO Programme	
Rev 003	16 Aug 2022	Annual update.	August 2023