www.solvexia.com

AU: +61 2 9386 0202
UK & EMEA: +44 7914 713 481
USA: +1 888-412-3104

Business Continuity Plan (BCP)

SolveXia Pty Ltd

Suite 1506
Westfield Tower 2
101 Grafton Street
Bondi Junction NSW 2022
Australia

Table of Contents

1 Document Control

Author	Date	Last Revision	Comment
Glen Silver	25/11/2021	1.0	Original document

2 References and related documents

Title	Link
11. SolveXia Disaster Recovery Plan 2021	 11. SolveXia - Disaster Recovery Plan 2021.pdf

3 Introduction

3.1 Purpose

The objectives of this plan are to:

- Undertake a risk management assessment.
- Define and prioritise critical business functions.
- Detail immediate responses to a critical incident.
- Detail strategies and actions to be taken to enable SolveXia to continue to provide service.
- Review and update this plan regularly.

3.2 Applicability

The Business Continuity Plan applies to the functions, operations, and resources necessary to restore and resume SolveXia's operations.

3.3 Scope

The Business Continuity Plan includes all procedures and critical systems covered in the Disaster Recovery Plan and referenced in References and related documents. In addition to IT Critical systems, external events (non-IT related events) that could impact business continuity have also been considered.

For simplification, those systems detailed in the Disaster Recovery Plan are duplicated in this document for ease of reading.

Environment / Application / Infrastructure	Function
AU / SolveXia / Web, Engine, Reporting, SQL	Provides SolveXia process automation service for Asia, Australia, and New Zealand clients
EU / SolveXia / Web, Engine, Reporting, SQL	Provides SolveXia process automation service for EU, Africa, and US clients

TAL / SolveXia / Web, Engine, Reporting, SQL	Provides SolveXia process automation service for a specific client
TIER / SolveXia / Web, Engine, Reporting, SQL	Provides SolveXia process automation service for prospective clients for 30 days evaluation
FTP	Provides FTP storage for all above-mentioned clients

Support may be required from external suppliers in the event of a disruption to continuity at SolveXia. These include the following:

External Party	System
Microsoft Azure	All production and QA systems
Yellowfin Reporting	All production and QA systems
Westfield Scentre Group	Westfield Tower 2, 101 Grafton Street, Bondi Junction, NSW 2022

Non-IT Event
Natural disaster
Work health and safety
Staffing/Key personnel

3.3.1 Planning Principles

SolveXia has followed the widely accepted guidelines for Business Continuity Planning illustrated in the following planning process:

Figure 1 Business Continuity Planning Process

Various scenarios were considered to form a basis for the business continuity plan, and multiple assumptions were made. The applicability of the plan is predicated on the following key principles:

- SolveXia provides Software-as-a-Service to clients and is resilient to interruptions caused by restricted physical access to Head Office.
- SolveXia does not have inventory that is critical to business continuity.
- A natural disaster is an event that could restrict physical access to Head Office.

3.4 Prerequisites

For business continuity planning to be effective, it is agreed that:

- Insurers will be made fully aware of these arrangements.
- A list of primary staff contacts will be distributed, including home numbers and addresses.
- A current signed agreement to this plan is in force.

3.5 Business Continuity Policy

The Business Continuity Plan documents the response plans, roles and responsibilities, critical internal and external stakeholders to effectively manage critical events in accordance with SOC2 requirements.

This Disaster Recovery Plan complies with SolveXia's Disaster Recovery Planning policy as follows:

- Personnel responsible for target systems shall be trained to execute contingency procedures.
- The plan, recovery capabilities, and personnel shall be tested to identify weaknesses in its execution at least annually.

4 Operations Profile

4.1 Geographic footprint

SolveXia's head office is in Bondi Junction, Sydney, NSW. The head office is in a multi-storey office building located within one of the largest shopping precincts in Australia. Bondi Junction is located on the Sydney train network within 6 km of the Sydney central business district.

SolveXia has remote offices located in the UK.

4.2 System Description

The environment is hosted on Microsoft Azure infrastructure. It uses Terraform and Azure ARM templates for infrastructure deployment and Azure Storage Accounts to store backup data.

Maintaining this separation of backup files from the base environment infrastructure provides an added layer of protection against loss of access to virtual machines, ransomware, data centre disasters, and other system issues that may arise.

Database backups are taken daily, encrypted, and stored in Azure Storage Accounts. The data is replicated in two different data centres located in two different cities. This ensures a high degree of confidence in the availability of backup data and restoration of complete systems in the event of a disaster.

4.3 Governance and Accountability

SolveXia sets forth an order of succession to ensure that decision-making authority for the Business Continuity Plan is uninterrupted. The Business Continuity Officer is responsible for ensuring the execution of procedures documented within this Business Continuity Plan.

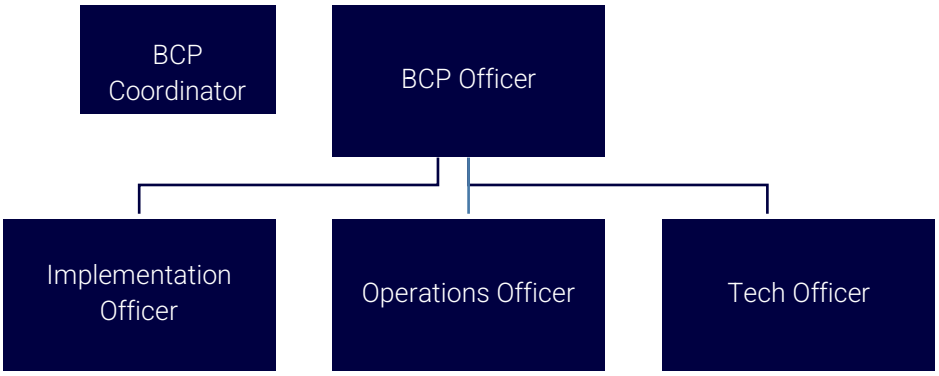

Figure 2 BCP Org Chart

4.4 Roles & Responsibilities

In general, the Business Continuity Plan establishes several teams, each assigned to participate in recovering separate SolveXia operations.

The Technology Team is responsible for the recovery of the infrastructure and all applications. Members of the team include personnel also responsible for the daily operations and maintenance of the SolveXia system.

The Implementation Team is responsible for ongoing communication with clients, providing reassurance and updates on disaster recovery. Additionally, the team is responsible for thoroughly testing recovered systems to meet client requirements during the ongoing recovery process.

The Operations team is responsible for communicating with all other stakeholders and providing updates on the disaster recovery to all relevant parties. This could include the media, regulatory authorities, and any other relevant parties.

5 Risk Management Plan

						Consequence		
				Insignificant	Minor	Moderate	Major	Catastrophic
				1	2	3	4	5
	Is expected to occur in most circumstances	Almost Certain	5	5	10	15	20	25
	Will probably occur	Likely	4	4	8	12	16	20
Likelihood	Might occur at some time in the future	Possible	3	3	6	9	12	15
	Could occur but doubtful	Unlikely	2	2	4	6	8	10
	May occur but only in exceptional circumstances	Rare	1	1	2	3	4	5

Risk Description	Likelihood	Impact	Priority	Preventative Action	Contingency Plan
Natural Disaster	Rare	Moderate	4	Evacuation procedure Staff awareness training	Prepare for remote working
Work health and safety	Rare	Moderate	4	Staff awareness training	Health contacts First aid kit
Staffing/Key personnel	Rare	Moderate	4	Staff awareness training	SolveXia sets forth an order of succession
Pandemic	Unlikely	Major	4	Staff awareness training	Prepare for remote working

6 Business Impact

6.1 Key Business Activities

	Business Activity
01	Finance
02	IT Operations
03	Client communications
04	Client support
05	Marketing and Sales

6.2 Business Impact Analysis

If the SolveXia system becomes inoperable, the following recovery periods are required to recover the minimum required business operations.

Critical Business Activity	Impact of loss	Recovery Period
Finance	Loss of clients Loss of staff Cash flow	14 days
IT Operations		

AU / SolveXia / Web, Engine, Reporting, SQL		24 Hours
EU / SolveXia / Web, Engine, Reporting, SQL		12 Hours
TAL / SolveXia / Web, Engine, Reporting, SQL		12 Hours
TIER / SolveXia / Web, Engine, Reporting, SQL		12 Hours
FTP / SolveXia / FTP Server		6 hours
Client communication	Loss of clients Reputational damage	48 Hours
Client support	Loss of clients	48 hours
Marketing and Sales	Reputational damage	48 hours

7 Incident Response Plan Checklist

In the event of an incident, have you:

☐	Evacuated the site if necessary?
☐	Accounted for everyone?
☐	Identified any injuries to any individual?
☐	Contacted Emergency Services?
☐	Implemented your Incident Response Plan?
☐	Started an Event Log?
☐	Activated staff members and resources?
☐	Appointed a spokesperson?
☐	Gained more information as a priority?
☐	Briefed team members on the incident?
☐	Allocated specific roles and responsibilities?
☐	Identified any damage?
☐	Identified critical activities that have been disrupted?

☐	Kept staff informed?
☐	Contacted key stakeholders?
☐	Understood and complied with any regulatory/compliance requirements?
☐	Initiated media/public relations response?

8 Roles and responsibilities

Key internal contacts:

Name	Role	Phone number	Email address
Adem Turgut	CEO	0411 164 232	adem.turgut@solvexia.com
Alex Murzina	CTO	0413 359 734	alexandra.murzina@solvexia.com
Noel Trillo	Head of Implementation	0403 016 418	Noel.trillo@solvexia.com
Jonathan Glass	Director	0407 585 605	jonathan.glass@solvexia.com
Mark Schneider	Director	0412 040 151	mark.schneider@solvexia.com

Key external contacts:

Police	000
Emergency Services	000
Ambulance	000
Medical	Poisons information: 13 11 26 Diabetes Australia: 1300 136 588

	Asthma Australia: 1800 645 130 St Vincent's Hospital: 02 8382 1111
Insurance company	PSC Insurance Brokers Steve Alman (02) 8234 0400
Utilities	Scentre Grid: (02) 9602 6633
Telephone	Zoom
Internet Service Provider	TPG

9 Recovery

Recovery is the return to a pre-emergency condition. Performing critical activities as soon as possible after a critical incident is a primary focus.

Critical Business Activity	Preventative/Recovery Actions	Resource requirements/Outcomes	Recovery Time Objective	Responsibility
Finance	Maintain a minimum of 2 people with access privileges to all finance systems, service providers and bank accounts Monthly backups of financial data Insurance policies in place	Temporary staff to migrate to alternative finance platform Data entry from financial database export	14 days	CFO
IT Operations	See disaster recovery plan			CTO
Client Communications	Decentralised client contacts	Leverage appropriate resources	48 hours	Head of Implementation
Client support	Multiple levels of knowledge exist across teams to	Leverage appropriate resources	48 hours	Head of Implementation

	perform this function			
Marketing and Sales	Monthly website backups Multiple levels of knowledge exist across teams to perform this function	Leverage appropriate resources	48 hours	CEO

10 Notification & Activation Procedures

Based on the assessment of the event, the plan will be activated by the Business Continuity Planning Coordinator.

1. Employee notifies the respective team leader.
2. The team leader notifies the management officers and informs them of the event.
3. Management officers appoint a Business Continuity Officer.
4. The Business Continuity Planning Coordinator instructs the Tech Team to begin assessment procedures.
5. The team members complete the assessment procedures to determine the extent of damage and estimated recovery time.

10.1 Criteria for activating the Business Continuity Plan

Activate the Business Continuity Recovery Plan if one or more of the critical business activities is interrupted. The interruption may continue for a period greater than the Recovery Time Objective for that activity.

10.2 Damage Assessment Procedure

- Determine the cause of the disruption.
- Evaluate the affected critical business activity(s).
- Estimate time to recover services to normal operations.

If the plan is to be activated, the following steps occur:

1. The Business Continuity Planning Coordinator will notify all Team Leaders and inform them of the event’s details.
2. Upon notification from the Business Continuity Recovery Planning coordinator, Team Leaders will notify their respective teams. Team members are to be informed of all applicable information and prepared to respond accordingly.
3. The Business Continuity Planning Coordinator will notify the remaining personnel on the status of the incident.

11 Response Checklist

The response procedure is critical to efficiently managing a disaster situation and reducing the impact on business operations.

The responsible party must complete the following tasks and be used as the trigger for the initial response to the business interruption. This checklist ensures that all relevant activities have been performed within the required time frames.

Ref	Activity	Responsibility	Timeframe	Signoff
1	Conduct initial assessment of incident and determine severity and formulate salvage operation	BCP Officer	Within 60 minutes of incident	
2	Hold team leaders meeting	CEO CTO, Head of Implementation, Head of Sales, Directors	Within 24 hours of incident	
3	Announce activation of the Business Continuity Plan	BCP Officer	Within 24 hours of incident	
4	Contact backup facilities as necessary	CEO/BCP Officer	60 minutes of incident	
5	Monitor and review the recovery procedures	BCP Officer	Continuously	
6	Contact vendors	CEO	Immediate	

12 Testing & Maintenance Procedures

12.1 Testing Approaches

Testing of the Business Continuity Plan may include, or exclude, a combination of the following approaches:

1. Scenario testing.
   This involves stepping through the recovery procedures to ensure they remain relevant to current operations against hypothetical situations.
2. Disaster recovery testing.
   This involves confirming the ability to restore and rebuild an environment. The goal of the testing is to ensure that the systems can be restored within the required time frames.
3. Structured walk-through.
   This is an evaluation of the Business Continuation Plan designed to expose errors or omissions without incurring the level of planning and expense associated with performing a full operations test.

12.2 Testing Tasks

Testing validates the usability of contingency and recovery plans and helps identify changes that need to be made to keep these plans current.

Ref	Task	Responsibility	Timeframe	Signoff
1	Determine the testing approach to be adopted	PMO	Twice annually	
2	Hold testing meeting with participants	PMO	At least 1 week prior to test	
3	Test developed plans	PMO	Twice annually	

4	Identify gaps / needs in the current plan	PMO/CEO	BCP test report following each test	
5	Incorporate changes into BCP	PMO	Action items from BCP report	
6	Publish and distribute final copies	PMO	Update in IT Controls following BCP test	

12.3 Schedule

The business continuity plan will be tested annually.

13 Communications Plan

13.1 Communications Schedule

The following table shows the communication for the plan.

What	Audience	Frequency	Prepared By	Media
Brief senior management on the situation.	Senior Management	Daily until resolved	BCP Officer	Slack/Zoom
Identify and brief the company spokesperson on the situation.	Company Spokesperson	Daily or as required	BCP Officer →CEO/Marketing	Slack/ Email/ Zoom
Prepare and issue company statements to the media and other organizations.	Media	As required	BCP Officer/Marketing	Email
Communicate situation information and procedural instructions to employees and other stakeholders.	Employees and Stakeholders	As required	BCP Officer	Slack/Email
Organize and facilitate broadcast media coverage.	Media	As required	CEO/Marketing	Email

13.2 Message to Employees

- The Business Continuity Officer will provide employees with a safe alternative-working environment as required.
- The Business Continuity Officer has ensured that facilities will be available to ensure employee safety.
- The Business Continuity Officer will rapidly alleviate the current problem and provide continuous updates on the situation.
- The Business Continuity Officer will provide appropriate contact information to all employees.
- The Business Continuity Officer is the single point of contact for inquiries.

13.3 Message to Clients

- SolveXia can continue the expected service to our clients.
- SolveXia can continue to meet all financial, legal, and contractual obligations.
- SolveXia is rapidly working to alleviate the current problem and provide continuous updates on the situation.
- SolveXia spokesperson provides a single point of contact for such inquiries.

14 Appendices

14.1 Glossary

Term or Acronym	Meaning
BCP	Business Continuity Plan - this document describes the methods and procedures for recovering business operations from disaster scenarios.
BIA	Business Impact Analysis - measures the effect of resource loss and provides management with data upon which to base decisions on risk mitigation and continuity planning.
Disaster Recovery Plan	Disaster Recovery Plan - this focuses on the recovery of the IT systems infrastructure that supports the recovery of the business. The Disaster Recovery Plan is referred to by the Business Continuity Plan to completely recover the site business.
MTO	Maximum Tolerable Outage - The maximum period that business processes can operate before the loss of resources affects their operations.
Recovery Strategy	An approved course of action to be employed in response to business disruption, interruption, or disaster.
Task Requirement	Activities required to be performed within the time frame by the responsible person.
Testing and Maintenance Schedule	This is the expected testing schedule to confirm the accuracy of the Disaster Recovery Plan.

15 Reviews

Date	Amended / Revied by	Reviewed / Approved by	Reviewed / Approved by
11Jan22	Alexandra Murzina	Mark Schneider	Jonathan Glass