Modini business continuity plan

Version: 1.0

Date: 23 Jan 2023

Author: Owen Candy

Contents

---

1. Introduction

Businesses are prone to a host of threat and disruption events that can have a negative effect on the company's ability to operate and can range from minor to catastrophic. This Business Continuity Plans (BCP) provides a framework which will assist the company to continue operating in the event of threats and disruptions.

2. Risk methodology

2.1 Definition

'A holistic management process that identifies potential impacts that threaten an organisation and provides a framework for building resilience with the capability for an effective response that safeguards the interests of its key stakeholders, reputation, brand and value-creating activities.' (Business Continuity Institute, 2001.)

2.2 Methodology framework

2.2.1 Analyse your business
2.2.2 Assess the risks
2.2.3 Develop your strategy
2.2.4 Develop your plan
2.2.5 Rehearse your plan

3. Governance

3.1 Company structure

3.1.1 Private Limited Company, registered in England and Wales.
3.1.2 Principle Governance: Executive and Board of Directors

3.2 Registered addresses

3.2.1 Suite 3, Bignell Park Barns, Chesterton, Bicester, Oxfordshire, OX26 1TD, United Kingdom

3.3 Registered offices

3.3.1 Top Floor, SSI House, Fordbrook Business Centre, Marlborough Road, Pewsey, Wiltshire, SN9 5NU, United Kingdom

3.4 Accountability officer

3.4.1 Owen Candy – Email: owen.candy@modini.co.uk Phone: +44 (0)20 3004 5595

4. Mitigations – Loss of work to competitors

4.1 **The principle income of Modini is from the [design, development, test, evaluation and operational delivery of complex Remotely Piloted Aircraft Systems (RPAS).]**

4.2 **The principal outgoing is staff remuneration, subcontractor fees and RPAS components and control systems costs.**

4.3 **Projections are made on a month-month cashflow basis and the business is set up such that the income from RPAS design, engineering, operation and consultancy services covers this on an annual basis.**

4.4 Worst Case Scenario

Loss of business to the extent that the month-month cashflow requirements cannot be met. This might mean that staff would have their pay suspended or made redundant, external liability obligations might be missed.

4.5 Mitigation

Facilities are in place to borrow money to cover several months of deficit while new business is sought. A cashflow runway is to be maintained for six months into the future to cushion the need to draw down on the facility.

5. Mitigations – Failures within your supply chain

5.1 **Modini is an aviation consultancy and RPAS engineering company and relies on a wide array of subconsultants, subcontractors and material and systems suppliers.**

5.2 Worst Case Scenario 1 – Engineering Designs are compromised

If a client's engineering designs were to have a fatal security breech, then there would be risk to customers deliverables and intellectual property.

5.3 **Mitigation**

All designs are versioned and only sourced from internal repositories. In the first instance we would use an un-compromised version from our repository, fixing any legacy issue ourselves. We would advise customers and re-released un-compromised deigns, deprecating and removing the affected designs.

5.4 **Worst Case Scenario 2 – A cloud vendor ceases serving data**

If there were a significant failure of a cloud vendor, then we would not be able to access company intellectual property and information prepared for our customers.

5.5 **Mitigation**

All data hosted on the current cloud/SaaS provider is backed up daily to a different/separate cloud object storage provider infrastructure within the EU. This can be accessed at any moment and can be restored to a different cloud/SaaS provider to provide access to data required.

Assuming there is complete and catastrophic failure of current cloud/SaaS provider, with current backup solution there would be a significant period of downtime involved to restore access to ALL files/folders while access is set up on the replacement cloud/SaaS provider, however specific individual file access is possible on a per user basis within a reasonable time period if required.

Historical mail requires current cloud/SaaS provider to be operational, however specific access to critical mailboxes is possible on a per user basis within a reasonable time period if required, whist remaining company is brought back online.

6. Mitigations – Loss of reputation

6.1 **As a small company, Modini is heavily reliant on its reputation. Loss of reputation would be similar in financial terms and could cause a cascade failure to obtain new work or loss of current work.**

6.2 **Worst Case Scenario**

A client takes action due to a failure on the part of Modini to secure their data or similar resulting in the loss of work and public loss of reputation.

6.3 **Mitigation**

Reputational clauses are written into all contracts and there are mechanisms in place to prevent situations from becoming public and recover damages if they do. Furthermore, a plan of publicity to counter public allegations would be enacted to mitigate fall-out. It is likely that there would be short term financial pain to be weathered. Facilities are in place to access funds to cover several months of deficit while new business is sought. A cashflow runway is maintained for six months into the future to cushion the need to draw down on the facility.

7. Mitigations – Human resources issues

7.1 **As a growing company of 13 staff permanent staff operating globally we are more reliant than larger organisations on key person dependencies. However, have succession plans in place to eliminate single points of failure wherever they exist within the business through growth, knowledge transfer, flat and evolving organisational structure.**

7.2 **Worst Case Scenario 1 – Key personnel problems**

Key personnel are either unavailable or leave the company with little / no notice or the withholding of services due to a disagreement. This might lead to a situation where services were disrupted due to unavailability of intellectual property.

7.3 **Mitigation**

All staff agree to a level of conduct and have a notice period that means they cannot leave the Company without a reasonable handover of work. Access credentials are controlled and accessible through administrator access. All functions have a backup and reasonable care is taken to prevent an incident occurring. Worst Case Scenario 2 – Denial of

access to facilities

Key personnel usually work together in one of the office facilities. If these were to become unavailable then this could present issues.

7.4 Mitigation

Modini is a modern consultancy and engineering company who operate a post COVID hybrid working approach. We use cloud services for every aspect of the day-to-day operations. Each service has a backup and all staff have laptops that are taken home daily. In the event that laptops are not available all services can be recovered from the internet without a single point of failure.

Modini also has an alternative facility. This would become the temporary centre of operations and engineering until either, access to the head office facility is regained or, a new facility is secured.

8. Mitigations – Health and safety liabilities

8.1 **Modini runs a full and comprehensive Health & Safety policy relevant to our industry and conducts regular and appropriate audits on all paperwork, systems, processes, and procedures practices of Health & Safety.**

8.2 **We take care to ensure all staff are trained, competent and have the necessary support to undertake their role and the required tasks.**

9. Key client contacts

A key **clients contacts** list has been created of those people that would need to be contacted in the event of an incident.

10. Plan training

The BCP is covered during the onboarding process of new employees and is part of all employees' annual review.

11. Plan testing

The plan will be tested annually.

12. Plan review date

The plan will be reviewed regularly or in the event of a significant change to the business.

Document control

Review schedule

Review interval	Next review due by	Next review start
Annually	January 2024	September 2023

Version history

Version	Date	Approved by	Notes
V1	23/01/2023	Board	Initial version