MI Skills Development Centre

Business Continuity Plan

2025-26

RISK MANAGEMENT STRATEGY and BUSINESS CONTINUITY PLANS

CONTENTS

Business Continuity and Contingency planning are integrated into our planning at all levels. We operate a comprehensive risk management strategy which is developed at Board level and cascades down to individual project management. This entails compiling a detailed Risk Register once a year that identifies potential risks, determines their impact and likelihood, and establishes measures to mitigate them.

Risk mitigation activity is considered under two headings:

(i) activities that reduce the likelihood of the risk and

(ii) those which reduce the impact of risks should they occur. Management reviews the Risk Register regularly in the light of changing circumstances, to ensure that planned mitigation measures have been implemented, and to identify if the level of risk has changed. Special attention is paid to risks that have become significantly more likely or mitigation measures that are failing, and if necessary additional mitigation measures are identified.

Among the critical areas which are addressed by the Risk Register are:

* Staff loss due to sickness, pandemic influenza, response to The Department of Health & Social Care (DHSC) and Public Health England (PHE), industrial disputes, etc: a register of alternative available qualified staff is maintained and updated regularly;
* IT failures: data is backed up nightly and stored off site.
* Accommodation problems: agreements with partners are in place for temporary re-housing.
* Supply chain and logistics problems: we maintain a list of alternative suppliers.
* Early termination of contracts, the loss of continuation funding or the failure of funders to provide agreed resources:

We deploy external consultants and our director to continuously seek out contingency funding and new opportunities for the continuation of funding for the activity. We then continuously submit tenders for commissioned activity or for project-based activity. This business development function is reviewed on a three-monthly basis by our senior management.

INTRODUCTION

Risk can be defined as:

> 'the threat or possibility that an action or event will adversely or beneficially affect an organisation's ability to achieve its objective'

Risk is normally considered in terms of impact and likelihood of an incident occurring. By assessing risks, the Organisation will be able to prioritise risk reduction activities. It is worth noting, as covered in the definition, that risks can have upsides as well as downsides, and risks strategies should therefore seek to maximise the upsides involved rather than simply guarding against the downsides.

There are many risks which may affect the organisation and its ability to achieve its objectives. The significant risks need to be identified and included in a Risk Register.

Risk management forms part of the system of internal control. A sound system of control should include:

- the nature and extent of the risks facing the organisation.
- the extent and categories of risk which it regards as acceptable to bear.
- the likelihood of the risks concerned materialising; and
- the costs of operating particular controls relative to the benefit thereby obtained in managing the related risks.

Potential benefits from risk management include the following.

- quick grasp of new opportunities;
- reassure stakeholders;
- fewer shocks and unwelcome surprises;
- help focus internal audit programmes;
- promote continuous improvement;
- supports strategic and business planning; and
- enhances communication between departments.

RISK MANAGEMEMT POLICY

The risk management policy (the policy) forms part of the organisation's internal control and corporate governance arrangements.

The policy explains the organisation's underlying approach to risk management, documents the roles and responsibilities of the directors, the risk management group and other key parties. In addition, it describes the process the directors will use to evaluate the effectives of the organisation's internal control procedures.

Underlying Approach to Risk Management

The following key principles outline the organisation's approach to risk management and internal control;

- the directors have responsibility for overseeing risk management within the organisation;
- an open and receptive approach to solving risk problems is adopted by the directors;
- the organisation makes conservative and prudent recognition and disclosure of the financial and non-financial implications of risks;
- all managers are responsible for encouraging good risk management practice within their designated managed areas; and
- key risk indicators will be identified and closely monitored on a regular basis.

Role of the Directors

The directors' role in the management of risk is to set the tone and influence the culture of risk management within the organisation, including;

- determining whether the organisation is 'risk taking' or 'risk averse' as a whole or on any relevant individual issue;
- determining what types of risk are acceptable and which are not, and setting the standards and expectations of staff with respect to conduct and probity;
- approve major decisions affecting the organisation's risk profile or exposure;
- monitor the management of significant risks to reduce the likelihood of unwelcome surprises or impact;
- satisfy itself that the less significant risks are being actively managed, with appropriate controls in place and working effectively;
- annually review the organisation's approach to risk management and approve changes or improvements to key elements of its processes and procedures.

Role of the Risk Management Group

The key roles of the risk management group are to:

- take overall responsibility for the administration and implementation of the risk management process.
- identify and evaluate the significant risks faced by the organisation.
- provide adequate information on a timely basis to inform the Board and the business planning process; and
- report on risk management action plan implementation on a regular basis to the board. Undertake annual review of effectiveness of the system of internal control and provide a report to the board.

Annual Review of Effectiveness

The directors are responsible for reviewing the effectiveness of the internal control of the organisation, based on information provided by the risk management group. Its approach is as follows:

- review the previous year and examine the organisation's track record on risk management and internal controls; and
- consider the internal and external risk profile of the coming year and consider if current internal control arrangements are likely to be effective.
- recognise the need for timely identification and assessment of significant risks and allocate resources to address the areas of high exposure.

This approach to risk management will also be extended to major subcontractors.

RISK MANAGEMEMT GROUP

The Risk management team will initially be made up of senior staff across the business representing all key functions:

Managing Director
Business Development Director
Finance Director
Operations Director

When the process is fully embedded the make- up of the Group will be reviewed.

RISK REGISTER

The Risk Register reflects the current significant risks facing MI ComputSolutions.

The Register also identifies the potential impact of each hazard, any mitigation in place or possible and the Risk Score.

The layout is of the Risk Register as follows;

Risk Area	**Impact**	**Risk Owner**	**Risk score**	**Controls & additional actions**
lists the risk type	list the physical disruption that may be caused	Identifies the manager best placed to manage this risk	Identifies the higher priority risks for the organisation.Risks can then be rated as High, Medium or Low	list current controls in place to prevent or reduce the likelihood and or the impact of the hazard on the organisation, as well as additional actions to be taken.

The Managing Director has overall responsibility for risk management within the organisation and is the organisation's Risk Champion.

Risks levels have been assigned to each risk:

Probability * Impact;

12 or above = high
8 - 12 = medium
below 8 = low

The Risk Register will be reviewed on a regular basis but at least annually. Management teams will be encouraged to review their operations and to highlight emerging risks on a timely basis. These will be considered by the Risk Management Team and built into the Risk Register as appropriate.

BUSINESS CONTINUITY

BUSINESS CONTINUITY - Introduction

The objective of the business continuity plan is to coordinate all departments within the organisation in the event of a major incident to ensure business critical functions are reinstated as soon as possible whilst minimising the long term impact on the organisation.

BUSINESS CONTINUITY - Aims

Aims of the policy:

- to create awareness of the need and use of the business continuity plan;
- to provide a framework for responding to major incidents;
- to establish an emergency management team to agree strategies and allocate resources to minimise the impact on the organisation;
- to secure all asset and resources: buildings, employees, business records, systems; and
- to coordinate the full reinstatement of organisation's services as soon as possible

BUSINESS CONTINUITY – Scope

Once notification takes place, the Plan will be activated, in full or part, when access to its facilities is denied, services and systems interrupted or in response to health and safety issues.

These incidents include but not limited to:

- Flooding
- Utility failure (electricity, water, telephones and gas)
- Fire or explosion
- Transport accident
- Extreme weather
- Serious vandalism
- Pandemic/Medical/ health & safety issues
- Loss of critical systems
- Terrorism
- Major loss of sensitive data
- Loss of Contract/Contract end

Whilst impossible to anticipate all disasters/ major incidents, many can be identified and plans made to avoid them, minimise their impact, contain or transfer their impact.

The organisation will follow best practice in:

- Undertaking a continuous programme of review, maintenance and replacement schedule for fire detection/prevention/fighting equipment;
- Regular risk assessments;

- Promote positive staff attitudes through awareness and training;
- Regularly evaluate fire evacuation procedures;
- Regular maintenance and testing of alarms;
- Undertake regularly inspection and maintenance programmes of essential equipment e.g., lifts, boilers, gas appliances;
- Back up all critical IT systems to be stored off site or in fireproof safes;
- Carryout internal audits of compliance with policies and procedures;
- Regular visits to sub-contractors to test contractual compliance including security of sensitive data;
- Regular sourcing of new opportunities prior to contract end;
- Regular review of project staff to promote Staff security;
- Back up all critical contracts and identify the most suitable provider to support learner transfer.

BUSINESS CONTINUITY – Business Response and Recovery Teams

The Business Continuity process will:

- confirm the nature and extent of the incident;
- take control of the situation;
- contain the incident; and
- communicate with stakeholders.

Two teams will carry out these activities:

- Emergency Response Team
- Business Recovery Teams

Emergency Response Team - Key responsibilities:

- **notifies the Board, DfE, GLA ASF, LA and DWP**;
- determines overall organisational needs and recovery priorities;
- notifies emergency services;
- mobilise **Business Recovery Teams**;
- **coordinate and manage immediate incident (at a strategic level);**
- notifies insurers;
- **coordinates continuous update to Board, DfE, GLA ASF, LA and DWP**;
- **approve budget for additional resources.**

Business Recovery Team - Key responsibilities:

- notifies Business Recovery Team members;
- mobilises their own Business Recovery Teams;
- coordinates and manage incident (at an operational level);
- notifies suppliers, contractors; and
- informs Emergency Management Team of additional resources required.

The decision to implement the Recovery Plan must be made by the Managing Director or member of senior management team.

BUSINESS CONTINUITY – Business Recovery Team Plans

Business recovery plans will be produced for all business teams and will be tested and updated on a regular basis.

The current plans are attached.

Section 1 Estates and related services, buildings, alarms, repairs

Section 2 IT, Telecoms *including:*

- Components of an IT business continuity plan
- Testing your IT business continuity plan
- Education and training in IT business continuity

Communications *including:*

- Identify how the organisation's stakeholders can be contacted.
- Consider the implications of the Data Protection Act when deciding what personal details you may want to list.
- Have a means to communicate to a significant amount of learners/clients as quickly as possible.
- Provide an Emergency Action Checklist of actions that may be required in an emergency.

Section 3 Curriculum and other delivery teams

Section 4 Administration: Finance

Human Resources

Delivery support (DWP, ESFA, etc.)

Healthy and Safety

Safeguarding and Prevent

Infection Control

TRAINING

Reason for training:

- to formalise the MISDCs business continuity policy;
- to reinforce 'ownership' of plans;
- to gain reassurance from regular testing; and
- to embed the risk management culture throughout the organisation.

An introduction into the organisation's risk management approach will be covered by the line manager as part of the induction process. This will be followed by regular awareness training as part of the organisation's training plan.

Document Control	
Version	**1**
Author	**Bola Sobowale**
Issue Date	**December 2012**
Updated	**October 2021** **July 2023** **February 2024** **August 2025**
Reviewed	**December 2022** **August 2024**
Approved	**Board**
Next Review	**August 2026**

Review Arrangements

We will review the policy annually as part of our self-evaluation arrangements and revise it as and when necessary in response to customer and learner feedback, changes in our practices, actions from the regulatory authorities or external agencies or changes in legislation.