ROCK
COMPLIANCE

Business Continuity Policy

Document: RCPO0002
Version: 4
Issue date: March 2024

RCPO0002	**Business Continuity Policy**
ISSUE DATE June 2023 **REVIEW DATE** March 2024 **NEXT REVIEW DATE** March 2026 **VERSION** 04	**AUTHORISED BY:** Perry - Davis **Colin Perry-Davis** **CEO**

Version Change Summary		
New Version ID	Date of Change	Summary of Changes
1	3/12/2021	Creation
2	15/03/2023	Reviewed (no change)
3	07/06/2023	Major re-write
4	19/03/2024	Revised key services and appendix 2 sample plan

Contents

1 General Procedures

1.1 BUSINESS CONTINUITY MANAGEMENT Policy Statement:

This Policy serves to establish our unwavering commitment to the Business Continuity Management System. The primary objective of the BCMS is to ensure that our customers receive an uninterrupted level of service from all divisions of the company and from all offices to the greatest extent feasible, in the event of a business disruption incident.

It is the responsibility of the Chief Executive to:

- Ensure that top management exhibits leadership and commitment in maintaining the effectiveness of the Business Continuity Management System.
- Ensure the establishment of policies and objectives that are compatible with the strategic direction of the organization.
- Ensure the integration of BCMS requirements into business processes.
- Ensure the provision of necessary resources to deliver such Business Continuity Plans.
- Communicate the significance of effective business continuity management and adherence to BCMS requirements.
- Ensure that the BCMS achieves its intended outcomes.
- Direct and support personnel in contributing to its effectiveness,
- Promote continual improvement and support other relevant management roles in demonstrating their leadership and commitment within their respective areas of responsibility.

Signed:

GJT Perry - Davis

(Chief Executive of Rock Compliance Limited Group of Companies)

1.2 Introduction

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

The implementation of Business Continuity Management Systems is essential due to the potential occurrence of incidents that can threaten business operations. In the event of a serious disruption, there is a risk that the business may not recover. As a result, clients are increasingly ensuring that the organisations they engage have robust procedures in place to guarantee business resilience and protect their own operations.

1.3 Accreditation

Rock Compliance Limited work in general accordance with ISO22301.

1.4 Scope

These procedures shall cover all aspects of the business outlined within section 2.1. This BCMS shall cover all offices and operations so far as reasonably practicable. Given the varied nature of services provided across the group of companies, it is not intended to cover every site operation in place, nor replace existing requirements, policy, or procedures in relation to health and safety.

1.5 Objectives and Purpose

The objectives of this BCMS are to ensure a reduction in the possibility of a disruptive incident occurring through the systematic analysis of risk and through the implementation of control measures. Should an incident occur, this BCMS intends to ensure that business operations continue to a minimum, stated level and the overall improvement of the business resilience of Rock Compliance Limited.

1.6 Responsibility

This document shall be reviewed, distributed, and amended by the person assigned as Business Continuity Manager.

1.7 Amendment Procedures.

The Business Continuity Manager shall record amendments to this document, and all appendices including the Business Impact Assessment and Business Continuity Plans, and any subsequent appendices in the Disaster Recovery Plan Log, which will contain all pertinent details of the changes made. All amendments shall be highlighted.

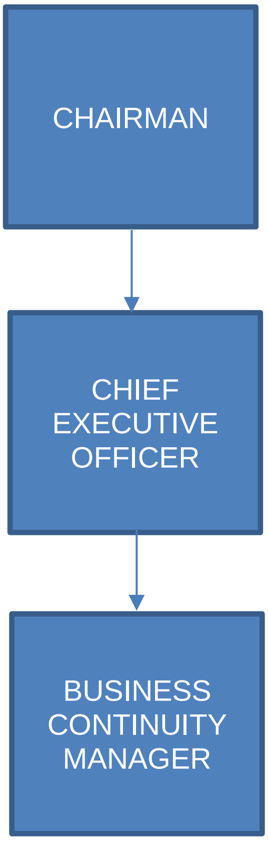
2 ORGANISATION AND STRUCTURE

2.1 Organisation

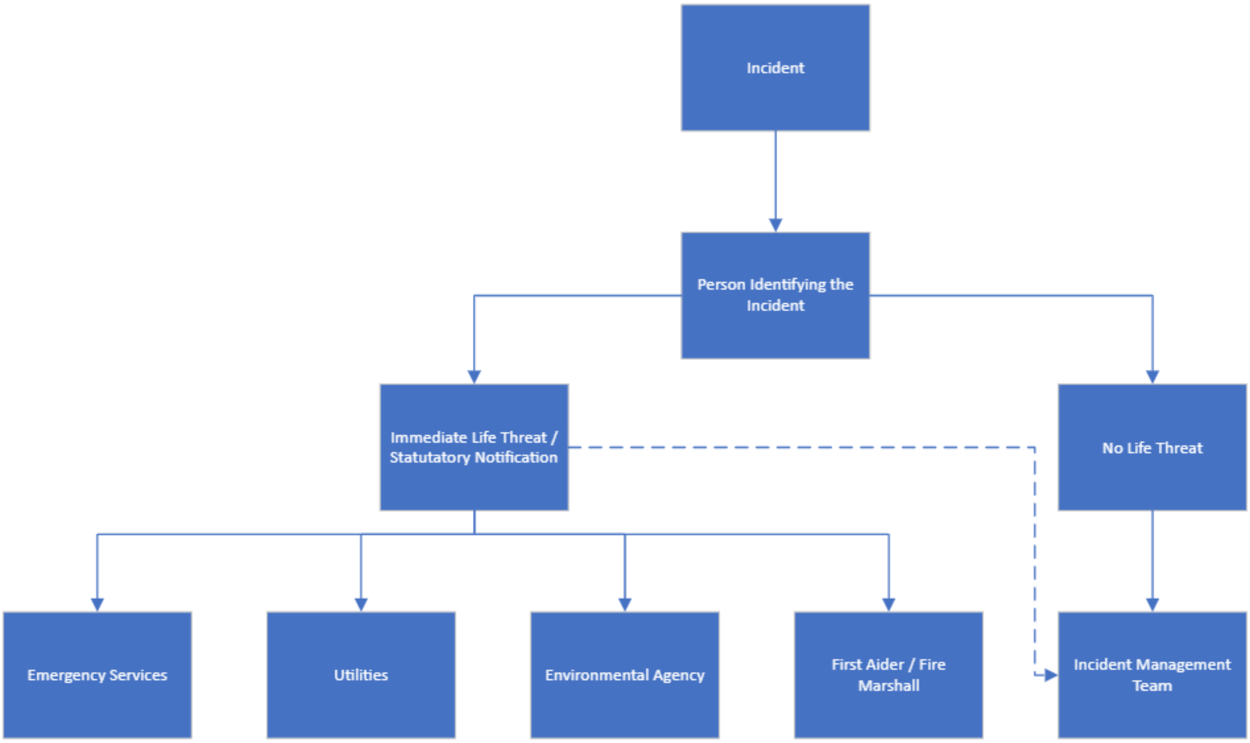
Please refer to the Integrated Management System for the Company Structure.

Rock Compliance Limited or “the Company” refers to the Rock Compliance Limited.

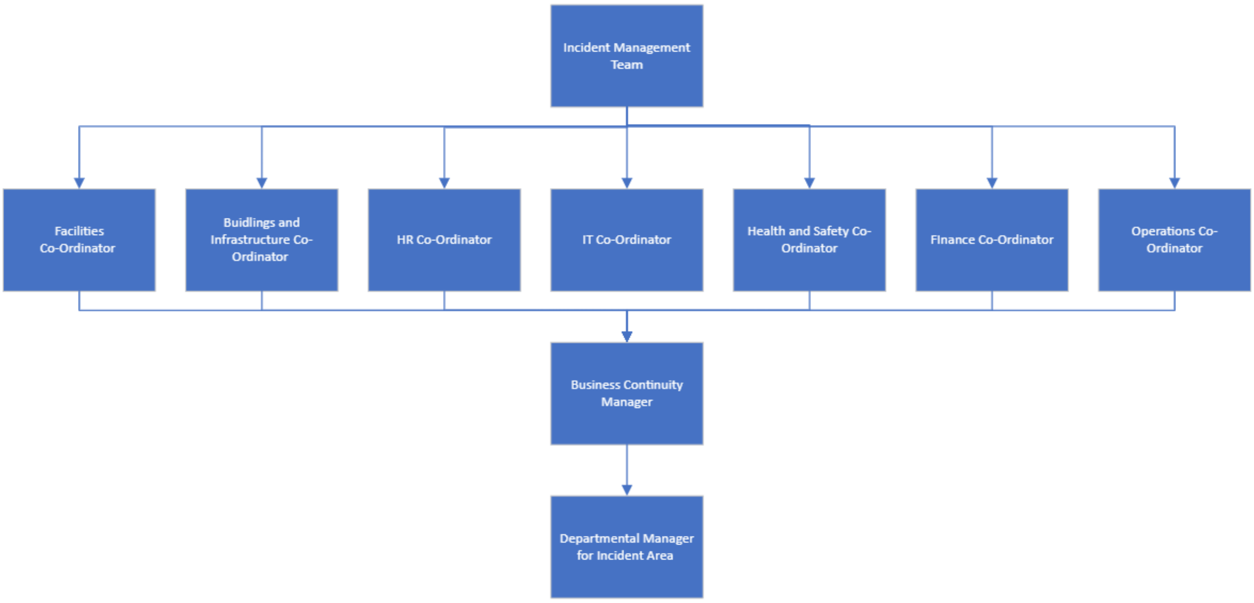
2.2 Business Continuity Reporting Structure



2.3a Emergency Response Structure


Incident
Person Identifying the Incident
Immediate Life Threat / Statutatory Notification
No Life Threat
Emergency Services
Utilities
Environmental Agency
First Aider / Fire Marshall
Incident Management Team

2.3b Incident Management Team


Incident Management Team
Facilities Co-Ordinator
Buidlings and Infrastructure Co-Ordinator
HR Co-Ordinator
IT Co-Ordinator
Health and Safety Co-Ordinator
FInance Co-Ordinator
Operations Co-Ordinator
Business Continuity Manager
Departmental Manager for Incident Area

2.4 Team – Roles and Responsibilities

2.4.1 Chief Executive

The Chief Executive shall ensure that Business Continuity Management System Reviews are held on at least an annual basis and that a competent internal staff member has been appointed to the role of Business Continuity Manager. The Chief Executive shall sign off this BCMS policy statement.

The Chief Executive has senior responsibility and shall perform the following items:

a) Direct appointment and management of the Business Continuity Manager
b) Ensure that the Business Continuity Manager has access to both internal and external resources for him or her to perform their task.
c) Ensure personal familiarity with significant Business Continuity Issues arising.
d) Attend annual Business Continuity annual Reviews.
e) Ensure that the Business Continuity Manager has reviewed all necessary documents within their respective timeframes and shall sign off the Business impact analysis and risk assessment as well as individual plans.

2.4.2 Business Continuity Manager (role undertaken by the Business Improvement Director)

The Business Continuity Manager shall perform the following items:

a) Direct management of or liaison with staff or external organisations appointed or expected to assist with QA training.
b) Ensure staff under his/her control are suitably competent, provided with all necessary training, aware of the actions expected of them and have the resources to implement them.
c) Check that delegated actions have been carried out.
d) Ensure personal familiarity with all legislation, approved codes of practice and guidance associated with Business Continuity Management. Ensure all documentation reflects required standards.

e) Maintain all documented systems including information and procedures within this manual and all technical documents / appendices.
f) Ensure their own on-going personal professional development.
g) Attend yearly reviews, ensuring action items are followed through and produce the ANNUAL BUSINESS CONTINUITY AUDIT & MANAGEMENT REVIEW.
h) Oversee the exercise of Business Continuity Management exercises on at least a quarterly basis.
i) Implement, review and update where necessary the following:
   - Business Continuity Management System
   - Business Continuity Incident Plans
   - Business Impact Analysis
   - Risk Assessment

   On at least an annual basis or where significant findings have been identified.
j) Shall request Business Continuity Plans from major suppliers and sub-contractors and shall review their contents for sufficiency and adequacy.
k) Maintain a continuing professional development training programme with regards to Business Continuity Management.
l) Shall ensure a deputy is appointed in the event of their non-availability in the event of a disaster and ensure that these deputies are regularly trained and informed of issues relating to Business Continuity Planning.

2.4.3 Business Continuity Incident Manager (role undertaken by the Compliance Manager)

a) Direct management or liaison of staff or external organisations appointed or expected to assist with an incident.
b) Take overall ownership of the BCMS in liaison with the BCM ensuring that delegated actions have been carried out in regard to incidents.
c) Ensuring their own on-going personal professional development
d) Co-ordinate the incident management team after invocation of the Business Continuity Plan.

2.4.4 The Incident Management Team

The Incident Management Team shall be formed of the following:

2.4.4.1 Facilities Co-ordinators (hub-based Team Leaders)

Shall perform the following items:

a) Shall ensure temporary facilities are available in alternative accommodation.
b) Shall photograph existing office assets and equipment and ensure photographs for major items of equipment and their receipts are regularly received and stored in a secure location off-site.
c) Shall liaise with Insurance Companies and appointed Loss Adjusters.
d) Shall liaise with any building contractor (Rock Compliance Limited Staff or other contractors) in any remedial works.
e) Shall ensure records of costs incurred are kept by responsible persons and safely documented (see appendices).
f) Shall liaise with Divisional Directors in ascertaining interim facility requirements.
g) Shall ensure a deputy is appointed in the event of their non-availability in the event of a disaster and ensure that these deputies are regularly trained and informed of current normal systems operation.

2.4.4.2 IT Coordinator

Shall perform the following items:

a) Shall ensure that an adequate Disaster Recovery Plan for all offices is available, up-to-date and tested on a regular basis.
b) Shall invoke the disaster recovery plan when required and as detailed within it.
c) Shall liaise with the Internet Service Provider and Equipment providers as necessary in the event of a disaster and provide interim levels of equipment and performance.
d) Shall liaise with Facilities Co-ordinators in allocation of interim resources in alternative office locations.
e) Shall ensure regular back-up of Rock Compliance Limited server information.
f) Shall ensure policy and procedures on information security are implemented within the organisation.

g) Maintain a continuing professional development training programme with regards to information security and disaster recovery.
h) Shall ensure a deputy is appointed in the event of their non-availability in the event of a disaster and ensure that these deputies are regularly trained and informed of current normal systems operation.

2.4.4.3 HR Co-ordinator

Shall perform the following items:

a) Shall liaise with the Business Continuity Manager, Business Continuity Incident Manager and Facilities Co-ordinators in the event of denial of access to any office and subsequently liaise with all Staff affected by a disaster.
b) Shall ensure that all staff are kept informed of dangerous weather conditions and shall liaise with them with regards to the ability to travel to the office.
c) Shall ensure that copies of personal details are not divulged without authorisation and in accordance with the data protection act.
d) Shall ensure lone-working policies are in operation within the group where necessary.
e) Shall ensure a written communications plan has been prepared to enable provision of information to and from all employees at any time.
f) Shall ensure that private mobile telephone numbers are recorded securely for all staff for use in an emergency and that these numbers are checked on at least a 6 monthly basis and updated where necessary.
g) Shall ensure that next of kin details are available for all staff.
h) Shall ensure that staff files are kept securely in digital and hard copy.
i) Shall liaise with the Public relations co-ordinator when required.

2.4.5.4 Public Relations Co-ordinator

Shall perform the following items:

a) Shall liaise with any departmental Director in relation to the death or serious injury of any Rock Compliance Limited employee or sub-contracted employee working on Rock Compliance Limited projects.
b) Shall liaise with any departmental Director in relation to any significant issue or accident that may negatively affect the image of Rock Compliance Limited.
c) Shall instruct all employees, in written form, to ensure they are aware of who can and who cannot liaise with the media.
d) Shall liaise with the media when required or liaise with any appointed P.R organisation and oversee media coverage of any event.
e) Shall ensure a deputy is appointed in the event of their non-availability in the event of a disaster.

2.4.4.5 Health and Safety Co-ordinator

Shall perform the following items:

a) Ensure Rock Compliance Limited comply with all relevant health and safety legislation, approved codes of practice and guidance.
b) Shall ensure Rock Compliance Limited activities have been risk assessed and suitable control measures implemented.
c) Shall ensure suitable training, industry certification and auditing regimes are in place. This shall include asbestos awareness training of operational staff.
d) Shall ensure office risk assessments have been completed.
e) Shall ensure fire risk assessments, asbestos surveys and legionella risk assessments have been conducted for each office and that significant findings are communicated to the competent person within appropriate timescales.
f) Shall ensure the provision of First Aid boxes and training of First Aiders within all offices.
g) Shall liaise with the Business Continuity Manager, Business Continuity Incident Manager and Departmental Directors in respect of health and safety incidents arising.
h) Maintain a continuing professional development training programme with regards to health and safety.

i) Shall ensure a deputy is appointed in the event of their non-availability in the event of a disaster and ensure that these deputies are regularly trained and informed of current normal systems operation.
j) Shall appoint First Aiders and Fire Marshals.

2.4.4.6 Infrastructure Co-ordinator

a) Shall ensure that new clients (private and including RSLs) are credit checked through a suitable external organisation. Credit checks shall be repeated on receipt of additional significant information relating to any individual organisation which might result in change to any credit score. The results of credit checks shall be discussed with the relevant account manager.
b) Shall ensure that payment mechanisms to staff or subcontractors are conducted in a regular and efficient manner.
c) Shall ensure adequate security provision in relation to access to pay-roll information and the issue of payslips.
d) Shall liaise with any other Director in relation to the prevention of fraudulent claims in relation to payment for works or services performed for Rock Compliance Limited or for expenses received.
e) Shall liaise with Fleet Managers in respect of fuel shortages or significant issues involving transportation to and from site or offices.
f) Shall ensure a deputy is appointed in the event of their non-availability in the event of a disaster.

2.4.5.7 Fire Marshal (Warden)

Shall perform the following items:

a) Take appropriate and effective action if a fire occurs.
b) Ensure that escape routes are available for use,
c) Identify hazards in the workplace,
d) Record and report their observations,
e) Ensure regular fire drills are undertaken and performed to a satisfactory standard.
If a fire is discovered, the fire warden should:
f) Ensure that the alarm has been raised / call the Fire Brigade when required and if not already performed.
g) Evacuate staff from the building or area involved,
h) Check that any staff or visitors with disabilities are assisted as planned,
call the reporting centre and give details of the location, severity
and cause of the fire, if known,
i) Ensure a roll call is carried out.
j) Fight any small fires if it is safe to do so.

2.4.4.8 First Aider

a) Call for ambulance(s) when required and attend hospital with the injured person.
b) Provide emergency first aid at work.
c) Administer first aid to a casualty with: injuries to bones, muscles and joints, including suspected spinal injuries; chest injuries; burns and scalds; eye injuries; sudden poisoning; anaphylactic shock.
d) Recognise the presence of major illness and provide appropriate first aid (including heart attack, stroke, epilepsy, asthma, diabetes).
e) Shall ensure they have received suitable training from an HSE approved First Aid Training Centre and undergone regular refresher training.
f) Shall ensure the correct stocking of First Aid Boxes and Kits provided.
g) Shall complete the accident book following any incident.
h) Shall liaise with the HR Co-ordinator if liaison with next of kin is required.
i) Shall complete RIDDOR forms if applicable.

2.4.4.9 Finance Co-Ordinator

a) Ensure adequate funds are made available for critical expenses.

b) Monitor and record expense flows for the incident.
c) Provide and communicate to the team a budget and financial modelling for incident handling and resolution.
d) Report to the CEO the financial impact to the CEO on an ongoing basis.

3 BCMS Needs and Strategy

3.1 The need for BCM.

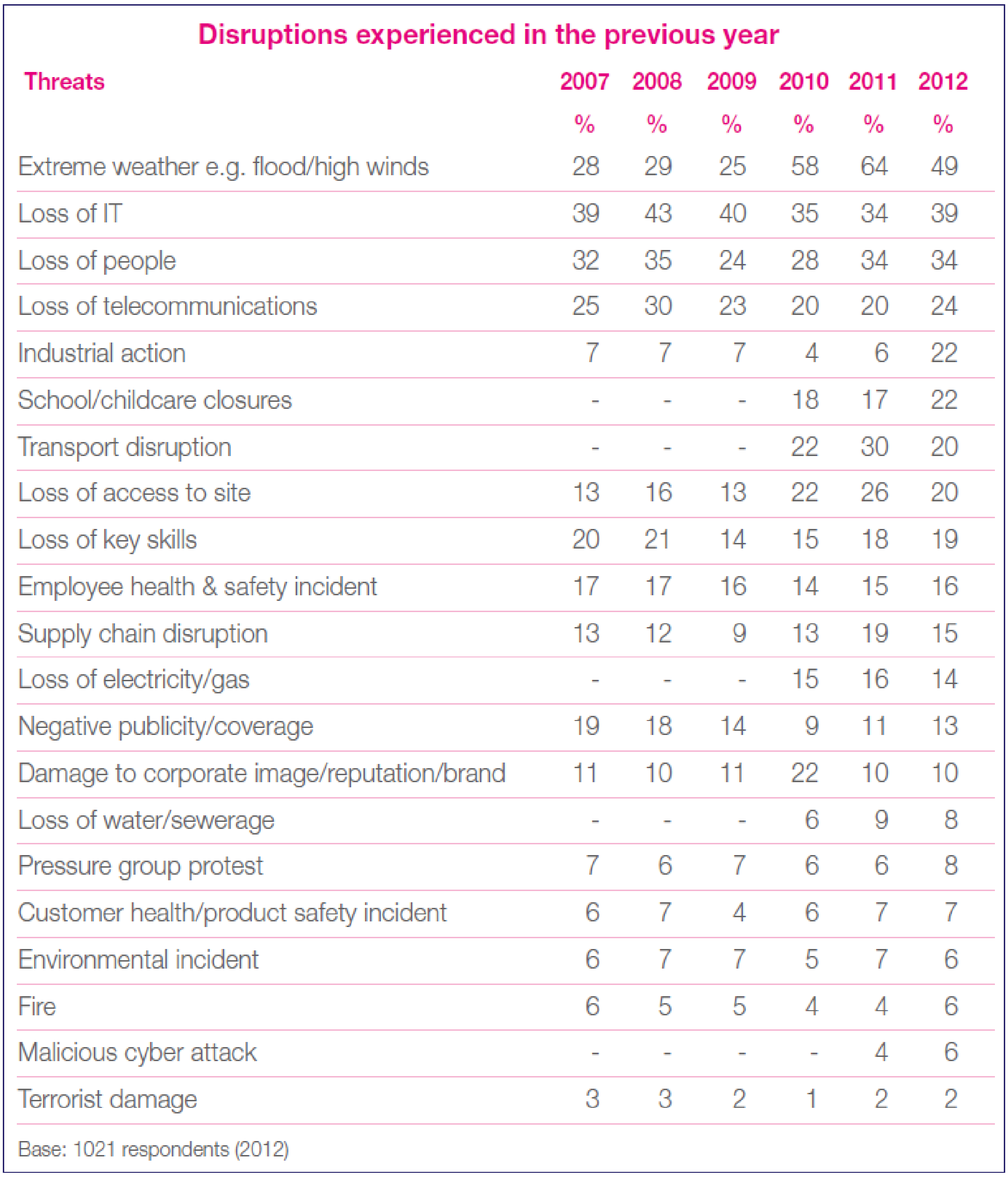
Business Continuity Management (BCM) is a holistic management process that identifies potential impacts that threaten an organisation and provides a framework for building resilience and the capability for an effective response that safeguards the interests of its key stakeholders, reputation, brand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

Organisations use BCM to protect their people, assets, reputation and ultimately the bottom line.

This BCM system has been designed in approximate concordance to the International Standard in business continuity (ISO 22301) which resulted in the development of the British Standard for BCM, BS25999.

BCM is not only important to individual organisations. It also forms an essential part of the UK's wider national security arrangements. The potentially significant contribution that small and medium sized enterprises (SMEs) may make to communities during large-scale disruptions has been increasingly recognised. As such, the Government pledged in the 2010 Strategic Defence and Security Review to support SMEs to improve BCM through a new corporate resilience programme. *(Source: The 2012 Business Continuity Management Survey, Chartered Management Institute).*

The following table identifies the types of disruptions experienced by organisations that enacted their Business Continuity Plan arrangements in recent years. This table demonstrates the broad range of the types of disruption and gives a good overall guide to what may reasonably be expected for organisations based on probability:



Disruptions experienced in the previous year

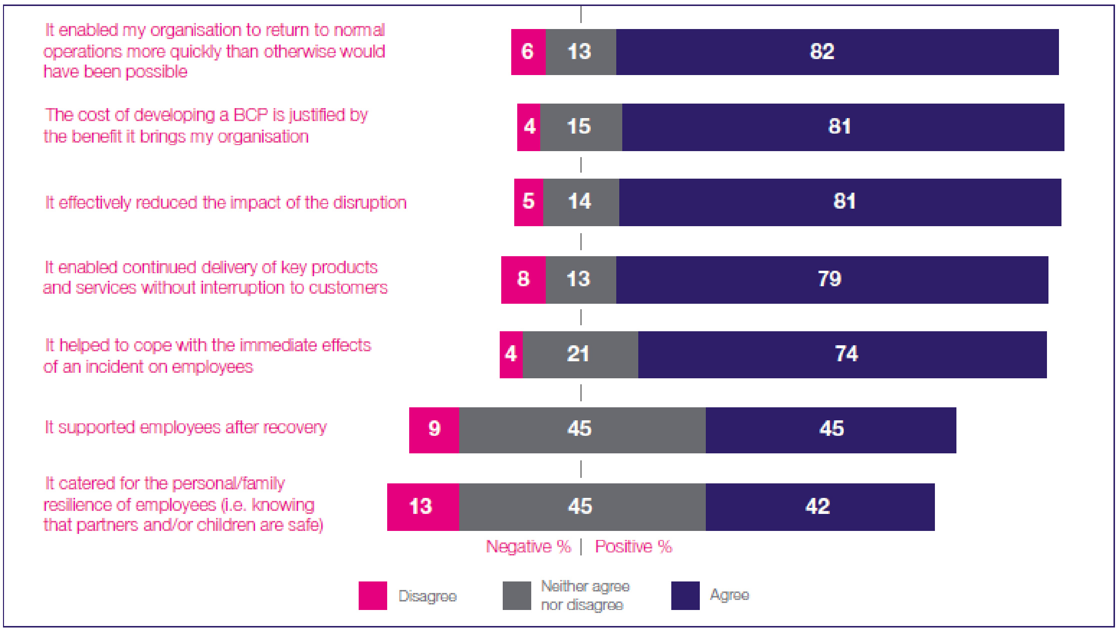
Threats	2007	2008	2009	2010	2011	2012
	%	%	%	%	%	%
Extreme weather e.g. flood/high winds	28	29	25	58	64	49
Loss of IT	39	43	40	35	34	39
Loss of people	32	35	24	28	34	34
Loss of telecommunications	25	30	23	20	20	24
Industrial action	7	7	7	4	6	22
School/childcare closures	-	-	-	18	17	22
Transport disruption	-	-	-	22	30	20
Loss of access to site	13	16	13	22	26	20
Loss of key skills	20	21	14	15	18	19
Employee health & safety incident	17	17	16	14	15	16
Supply chain disruption	13	12	9	13	19	15
Loss of electricity/gas	-	-	-	15	16	14
Negative publicity/coverage	19	18	14	9	11	13
Damage to corporate image/reputation/brand	11	10	11	22	10	10
Loss of water/sewerage	-	-	-	6	9	8
Pressure group protest	7	6	7	6	6	8
Customer health/product safety incident	6	7	4	6	7	7
Environmental incident	6	7	7	5	7	6
Fire	6	5	5	4	4	6
Malicious cyber attack	-	-	-	-	4	6
Terrorist damage	3	3	2	1	2	2

Base: 1021 respondents (2012)

(Source: The 2012 Business Continuity Management Survey, Chartered Management Institute)

Effectiveness

From those organisations that had experienced disruption, management cited the following statements on the importance of their BCIP process:



(Source: The 2012 Business Continuity Management Survey, Chartered Management Institute).

3.2 Client Requirements

The following represents general statements on expected client requirements. It should be supplemented with additional, specific statements from major clients within the Rock Compliance Limited Group of Companies and the Business Impact Analysis amended accordingly.

- Operatives (Rock Compliance Limited or sub-contracted employees) will work with regards to their own and others safety, reducing the possibility of site-incidents occurring.
- That all Rock Compliance Limited offices are safe places to work.
- That operatives are suitably trained experienced and qualified in relation to the works they are undertaking (e.g. CSCS, Gas-Safe).
- That suitable resources are available, so that in the event of either site or management staff absence, service provision is guaranteed.
- That the Rock Compliance Limited ICT systems are backed up and in the event of a disaster can be re-built with no loss of information.
- That alternative accommodation and equipment for Rock Compliance Limited staff, who normally operate from their offices or Client offices can be made available, at short notice,
- That Rock Compliance Limited remains solvent, able to pay supply-chain and staff on-time and have credit checked suppliers.
- That buildings or installations or services supplied are in accordance with the design and all necessary statutory and regulatory requirements.
- That Rock Compliance Limited have checked their sub-contractors in terms of operational competence, financial status, health and safety performance, capacity, experience, and their own business continuity.
- That weather related issues are predicted as far as possible and suitable systems set up to allow work and access to be maintained as far as reasonably practicable.
- That should an incident occur, suitable systems are in place to minimise the impact and that the Client’s reputation and image is always maintained.

3.2.1 Strategy

This management system reflects the ISO22301 ‘Plan, Do, Check, Act’ approach. The following is a graphic illustration of how this method works:

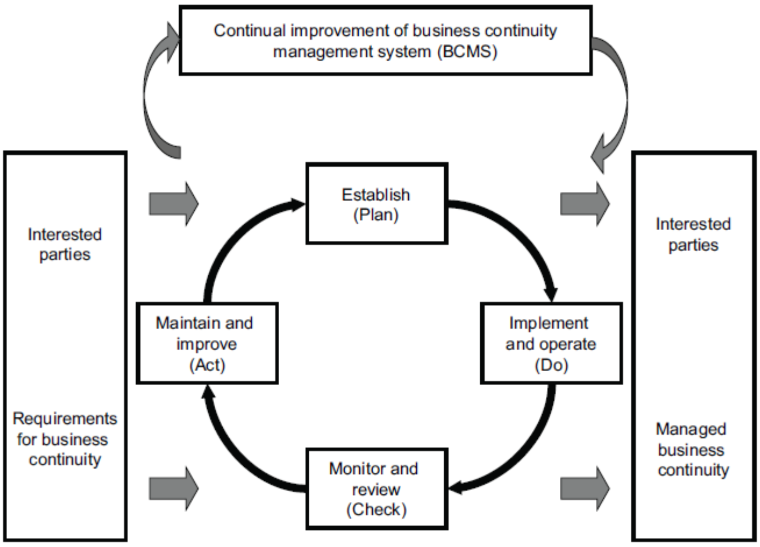
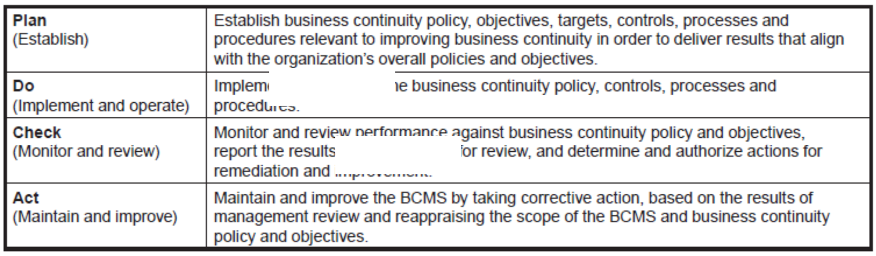

Continual improvement of business continuity management system (BCMS)
Interested parties
Requirements for business continuity
Establish (Plan)
Implement and operate (Do)
Monitor and review (Check)
Maintain and improve (Act)
Interested parties
Managed business continuity

Figure 1 — PDCA model applied to BCMS processes

Table 1 — Explanation of PDCA model



Plan (Establish)	Establish business continuity policy, objectives, targets, controls, processes and procedures relevant to improving business continuity in order to deliver results that align with the organization’s overall policies and objectives.
Do (Implement and operate)	Implem [illegible] ıe business continuity policy, controls, processes and procedures.
Check (Monitor and review)	Monitor and review performance against business continuity policy and objectives, report the results [illegible] for review, and determine and authorize actions for remediation and improvement.
Act (Maintain and improve)	Maintain and improve the BCMS by taking corrective action, based on the results of management review and reappraising the scope of the BCMS and business continuity policy and objectives.

(Source: International Standard ISO22301, Societal Security – Business continuity management systems – requirements, BSI).

Each section of the illustration is addressed within the various parts of this management system. It is important to note that this BCMS will only remain effective with consistent input from interested parties, continual review and updating of the Risk Assessment and Business Impact Analysis and commitment of senior management to drive through the BCM process.

4 Business Impact Analysis and Risk Assessment

4.1 Business Impact Analysis

Rock Compliance Limited shall assess the impacts of disrupting activities on the organisation's products and services.

The business impact analysis shall include the following:
a) Identifying products and services.
b) Identifying the impacts over time of not performing these activities.
c) Setting prioritised timescales for resuming these activities to a minimum acceptable level, taking into consideration the time within which the impacts of not resuming them would become unacceptable; and
d) Identifying dependencies and supporting resources for these activities, including suppliers, outsource partners and other relevant interested parties.

4.1.1 Key products and Services

The Key Products and Services, provided to customers by Rock Compliance Limited are:

- Water Hygiene
- Water Treatment
- Air Hygiene
- Mechanical & electrical compliance
- Pre-commissioning and commissioning
- Training services

The Business Impact Analysis will require regular review and amendment in order to remain valid.

The Critical Resources necessary to support these and allow them to function are defined within the denial of access business continuity plan.

Services provided by Rock Compliance Limited are essentially site based, driven or supported by office functions. As services provided by Rock Compliance Limited are commonly provided from similar offices, with similar support functions and from the same I.C.T system, maximum tolerable periods of disruption (M.T.P.D) and recovery time objectives (R.T.O.) have been set for the provision of accommodation (Denial of Access) and Loss of I.C.T. In addition, given the urgent, 24/7, nature of incoming calls received and the requirement to provide rapid on-site response, M.T.P.Ds and R.T.Os have been set for incoming calls for tenant lines.

Given the varied nature of site works, the use of sub-contractors and anticipated and regular delays in construction works from events which may possibly be outside the control of Rock Compliance Limited, MTPDs and RTOs have not been set for site-works.

4.1.2 Recovery Time Objectives and Maximum tolerable periods of disruption.

These are defined in ISO22301 as follows:

Maximum tolerable period of disruption (MTPD)

- time it would take for adverse impacts, which might arise as a result of not providing a product/service or performing an activity, to become unacceptable.

Recovery Time Objective (RTO)

Period of time following an incident within which:

- product or service must be resumed, or
- activity must be resumed, or
- resources must be recovered

NOTE: For products, services and activities, the recovery time objective must be less than the time it would take for the adverse impacts that would arise as a result of not providing a product/service or performing an activity to become unacceptable.

Please note that a full glossary of terms is available in section 3 (Terms and Conditions) of ISO 22301. This should be referred to in relation to the MTPD, RTO and other terms used within this document.

4.2 Risk Assessment

4.2.1 Requirement

Rock Compliance Limited shall:

a) Identify hazards and their risks of significant disruption or harm to the organisation's products, services, employees or those affected by Rock Compliance Limited works.
b) Analyse risk & evaluate which disruption related risks require control measures (treatment).
c) Identify control measures in accordance with business continuity objectives, statutory requirements and in accordance with the organization's risk appetite.

4.2.2 Summary

A number of hazards or scenarios exist which may impact on the Rock Compliance Limited business. These are recorded in the risk assessment.

The Risk Assessment will require regular review and amendment in order to remain valid.

Each potential incident or hazard shall include a Risk Assessment that considers the
Likelihood of Occurrence and Severity of Impact presented.

This assessment categorises the activities between Low, Medium and High Priority. These risks are not priorities for recovery as mostly the hazards are interdependent of each other, but overall ratings of potential impact on the business.

The risk assessment is provided twice, one risk assessment without control measures and the other with control measures.

4.2.3 Cost

This is a very approximate guidance on the likely financial implications of any incident occurring.

4.2.4 Affected departments and processes

This lists which departments are affected by the incident.

4.2.5 Acceptance of Risk / Risk Appetite

This provides a defining statement on risk appetite and whether actions will be put in place to mitigate the risk that any incident or hazard presents. The decision on whether to provide control measures to prevent the incident occurring in the first place or to minimise its harm should it occur may be based on the probability of it occurring and its potential harm. A number of options are presented. The risk can either be:

- Accepted: No measures are put in place to prevent the incident occurring and should it occur, then it is accepted that no measures are in place to control it.
- Reduce Risk: Control measures are put in place to reduce the possibility of the incident occurring in the first place. Should it occur, then it is accepted that no measures are in place to control it.
- Reduce Risk and Plan Continuity: Control measures are put in place to prevent the incident occurring in the first place and measures are in place to control it if it occurs.
- Eliminate Risk: This prevents the incident occurring in all possible circumstances.

Generally, costs associated with risk appetite increase with increased desire to reduce the possibility of the event occurring or the measures needed to control the risk should it occur. The decision may be based on what is desirable, reasonably practicable and within budget.

4.2.6 Control measures.

This details the sort of control measures that are already in place to prevent any incident occurring. It does not list the necessary steps if an incident occurs as this is contained within the business continuity incident plan.

4.2.7 Recommendations

These are the recommended next steps to improve business resilience for each noted hazard/ incident.

4.2.8 Assignment

This lists the individual people responsible for maintaining the control measures. It does not state who should carry out tasks in the event that an incident occurs – this is included within the Business Continuity Incident Plan.

4.2.9 Legal Status

Specific acts, regulations and guidance are listed here; however, it should be noted that this list may not exhaustive.

5 Business Continuity Incident Planning

5.1 General and Format

- A number of business continuity incident plans (BCIPs) have been produced on a maximum of 2 pages of A4, as separate, coloured, individual documents. Each BCIP is based on a single type of event occurring. They have been designed in this fashion to allow simple and easy access.
- Each incident has an overall co-ordinator, which is stated at the top of the plan. This nominated position is named within the General procedures section and their contact details are provided in the contacts section. This person will be responsible for overall co-ordination of individual Co-ordinators involved in resolving the issue who are detailed elsewhere within each individual BCIP. The overall co-ordinator will report to the Business Continuity Manager.
- Each incident has an alert status. This refers to the level of top-management response and structure of the incident handling (detailed later).
- Each incident has an assumption of what is and isn't included in the plan.
- BCIPs may distinguish between site and office-based incidents.
- BCIPs identify what steps should be taken, by who and by when.
- BCIPs identify in basic statements what initial outcomes and end outcomes should be.
- BCIPs may include basic guidance or further information on one page.
- BCIPs may refer to other documents (e.g. the Disaster Recovery Strategy).

5.2 Location / Storage of business continuity incident plan

The Business Continuity Incident Plans shall be kept separate from this Business Continuity Management System (BCMS) Document. This BCMS should not be needed in the event of any incident occurring; only the BCIP and associated (and specifically referenced) documents are needed.

Hard copies of the individual Business Continuity Incident Plans (not the full BCMS) shall be distributed as follows:

For site employees:

- To be stored within every site office within a White folder with the BC logo

For named Incident Management Team Co-ordinators and Senior Management Staff

- Personal issue within White folder

Documents are also available on-line via the SHEQ drop down menu on Rock Compliance Limited World.

5.3 Incident Management Team Coordinators / Senior Management

Individual members of staff have been nominated with specific Business Continuity duties. Their titles will not always be their formal Rock Compliance Limited job titles, but instead refer to the type of work they will perform in the event of the invocation of any Business Continuity Incident Plan.

5.4 Invocation of the business continuity incident plans

Any single 'Incident Management Team Co-ordinator' can invoke the BCIP. Any employee can contact the Business Continuity Incident phone number (**0800 8620458**) or any Senior Management Staff. The contact details section of the BCIP will be provided to all employees.

5.5 Structure and reporting of incident management (alert status).

Not all ‘Incidents’ need to have specific ‘control-centres’ set up, nor involve all layers of management or all incident management team co-ordinators. The Management Arrangements part of the BCIP details how staff should liaise and report in the event of an incident and the lines of reporting required.

The Management arrangements also details basic requirements for reporting under RIDDOR, completion of diaries and review arrangements during and after any event.

6 Resources

6.1 General Statement on Resources

Suitable internal resources shall be provided for the maintenance, development and review of this business continuity management system and for the operation of the Business Continuity Incident Plan, when required. External Service Support Providers, Facilities and ICT shall also be provided and maintained to assist in any control measures needed.

Specific Roles and Responsibilities to be followed, in the result of an incident are defined within each Business Continuity Incident Plan.

Individual Incident Management Team Co-ordinators are named within the Contacts section of the BCIP, and this will need to be amended should any job roles change or if any staff are no longer employed by Rock Compliance Limited.

The general organisational structure is outlined within section 2 of this BCMS.

The role of Business Continuity Manager has overall responsibility for overseeing the implementation, development and review of the BCMS and the Business Continuity Plans and processes. Senior Management shall allow sufficient time for all nominated individuals to administer the BCMS and development and testing of the BCIPS.

The BC Incident Manager shall ensure that any nominated deputy shall have the necessary skills to manage any BC plan invocation in their absence.

6.2 Competency and training of BCM personnel

It is assumed that individuals named as Incident Management Team Co-ordinators have the necessary basic technical skills (e.g. ICT) to perform their function in the event of invocation of any BCIP and that they have been selected for this reason.

The H.R Manager maintains Training Plans and copies of relevant qualification certificates of nominated ‘Incident Management Team Co-ordinators’ and shall make these records available to the BC Manager on request. If physical evidence of training, such as a certificate, is not available, then the H.R Manager shall make a subjective judgement to evaluate this, which may be based upon experience, testing or questionnaire completion. Training needs analysis shall be undertaken where appropriate and if required additional internal or external training provided.

6.3 Training

A process of Business Continuity Awareness Activities shall be established in order to embed BCMS values and processes within Rock Compliance Limited. There are four distinct classes of training required for the successful operation of this BCMS:

a) General training:

This is provided to all employees, so that they know what to do in the event of an incident and who to contact. The training can consist of basic provision of information such as a letter/email along with the provision of any material required (e.g. basic BC planning information / contact details etc.).

b) Senior Management training:

This shall be conducted in a group workshop and provided by the Business Continuity Manager.

- A brief overview of the purpose of this BCMS and ISO22301 in general.

- Brief Discussion on each individual Business Continuity Incident Plan, the role of senior management in each case and how business continuity incident plans are located/ distributed.
- Discussion on general and management arrangements.
- Discussion on exercising and testing possibilities and arrangements.

Refresher training shall be provided on at least an annual basis (possibly through simplified means e.g. provision of summary information by email), or on a specific one to one basis where roles/positions have changed at any time.

c) Incident Management Team Co-ordinator training:

- This shall be similar to training for senior management, but with increased detail on each specific business continuity plan and the role of the Co-ordinator in each case.

d) Business Continuity Manager Training

The BC Manager and BCI Manager shall be provided with specific training for preparing, developing, maintaining and administering a BCMS with the intention of achieving formal qualifications /certification. Possible courses are administered by the BSI, however other providers are available.

The result of the training should enable the BC/BCI Manager to:

- Develop, maintain and administer this BCMS.
- Oversee the implementation of Business Continuity Incident Plans
- Structure and carry out specific exercises.
- Review control measures required.
- Provide internal BCM training to staff.

Following any training, a feedback questionnaire shall be completed by the trainee, in order that senior management may evaluate the effectiveness of training and establish whether and when further training is needed.

7 Documentation

7.1 Control of BCMS Records

BCMS documentation shall be maintained both electronically and in hard copy. All records shall be held in suitably named/identified folders in a legible manner. Rock Compliance Limiteds' ISO9001 Quality Management System procedures detail general management of records.

Each BCMS document shall show suitable identifying details, such as a title and/or reference number, plus a revision status and/or date.

A Master 'Document Control List' shall be maintained which shall list all BCMS documents and their revision numbers.

The Business Continuity Manager shall record amendments to this document, and all appendices including the Business Impact Assessment and Business Continuity Incident Plans, and any subsequent appendices on an **amendment sheet in the Disaster Recovery Log**, which will contain all pertinent details of the changes made.

The Business Continuity Manager has overall responsibility for amendments and shall review and approve each BCMS document before it is released into use and add their initials to the document control list.

The Chief Executive shall sign the Policy Statement within section 1 of this BCMS.

Individual plans shall be distributed as detailed within section 5.2 of this BCMS. It is not necessary to distribute the whole contents of this BCMS to all employees, but it should be made available to them, should they request to have access to it.

7.2 Supply Chain

Copies of Business Continuity Plans of key suppliers shall be obtained by the Business Continuity Manager. These shall be reviewed in a prioritised manner for compatibility with Rock Compliance Limited's services and expectations.

The decision, by the Business Continuity Manager, to obtain the BCMP of any single supplier, shall be based on a number of factors including financial value of goods or services provided and the possibility of being able to identify other providers at short notice. Those suppliers that can be seen as 'single points of failure' shall have their BCMP examined in closer detail for potential issues arising which may ultimately affect Rock Compliance Limited's service delivery.

7.3 Clients

Copies of Business Continuity Plans of key clients shall be requested by the Business Continuity Manager. These shall be reviewed in a prioritised manner for compatibility with Rock Compliance Limited's service delivery, this BCMS, the Business Impact Analysis and Risk Assessment as well as the individual Business Continuity Plans.

The decision, by the Business Continuity Manager, to obtain the BCMP of any client shall be based on the financial value of goods or services provided to that client. As a minimum it shall include those Clients where Rock Compliance Limited have shared office arrangements.

8 Communication

The Management arrangements section contains further details of communication and reporting requirements during and after any incident arising which invokes any individual Business Continuity Plan.

A Business Continuity Management Annual meeting shall be held.

The meeting shall include The Business Continuity Manager, The Business Continuity Incident Manager, Incident Management Team Co-ordinators, Senior Management as appropriate and the CEO.

A basic agenda shall include the following:

- Minutes of the previous meeting.
- A summary of the results of BC Incidents, outcome and lessons learned.
- A summary of the results of BCM Exercises, outcome and lessons learned.
- Details of any newly introduced or amended BCMS documentation.
- Changes which have affected the BCMS, Business Impact Analysis, Risk Assessment or BC Incident Plans in the year.
- Feedback from senior management, department heads and other employees on changes in perceived risks.
- External input received and updates on alternative accommodation plans.
- Changes in nominated personnel.
- Training requirements in relation to Business Continuity.
- Summary of any other reviews carried out.
- Improvement actions and non-conforming works identified.
- Emerging Good Practice and Guidance.
- Any other business.

Copies of the minutes shall be recorded and distributed to all attendees via email. The output of this annual review is documented in section 9.

Release of basic BCMS information and contact details to general Rock Compliance Limited Employees shall be through written means (post).

9 Exercising and Testing

The adequacy of any BCIP remains unknown until it is tested. Often this may only be when it is required, at which time it may not have the desired outcomes and/or be out of date.

A very effective way of ensuring an effective BCMS is through testing scenarios with outcomes for improvement being re-incorporated into any individual BCIP.

Testing different scenarios helps increase staff awareness of the BCIP, can help identify gaps between the BCIP and staff's interpretation of the BCIP, and can improve staff confidence in implementing the BCIP.

It can also highlight resource and logistical gaps (for example, how to relocate essential staff). The overall adequacy of the BCIP during the testing scenario may also be a good indicator of the adequacy of the testing cycle.

Exercises should aim to test all parts of the BCMS, however it should be noted that these tests can be performed over long time periods and should be designed in a way that should not generally disrupt normal business operations to any significant extent.

Testing should be based on appropriate scenarios that are well planned with clearly defined aims and objectives with formal post-exercise reports that contain outcomes, recommendations and actions to implement improvements.

There are several ways of testing the BCIP, with relative advantages and disadvantages in terms of cost and disruption to an organisation. The following represents a general guide to the type of exercises that could potentially be carried out.

a) Desktop review - low cost and low, if any, disruption.
Staff with key responsibilities attend a guided presentation with discussion on the BCIP and its implementation.

b) Desktop scenario - low cost and low disruption.
Similar to desktop review except that hypothetical disruption scenarios are used to examine assumptions made during the development of the BCIP.

c) Recovery exercise - medium cost and medium disruption.
Closing down or removing access to systems, resources or infrastructure. The recovery or establishment of alternatives is examined to determine adequacy.

d) Live scenario - high cost and high disruption (but dependant on the extent).
Activation of BCIP(s) based on a hypothetical scenario that provides a robust test of a BCIP.

To optimise the effectiveness of BCIP testing, the Business Continuity Manager should:

- determine participants - participation will promote increased familiarity of the BCIP for responsible staff.
- decide on resources to be tested.
- develop a sequence of events.
- observe responsible staff to ensure they understand their responsibilities during a disruption.
- consider the response of key stakeholders (media, suppliers, clients, employees etc.).
- review the exercise to confirm that resource requirements and key contacts are appropriate.
- review the exercise to verify that the BCIP is current, practical and feasible; and
- understand that outputs will drive continuing improvement in the BCIP.

It should be understood that 'live scenario' testing does not need to involve whole departments or always involve 'denial of access' and the requirement to identify alternative accommodation. Selected employees can be specifically targeted as representative of any Rock Compliance Limited department or office and with some limited warning to their Senior Management to ensure a suitable time is chosen. This will ensure disruption is minimal.

The Business Continuity Manager shall be responsible for the planning and overview of the testing regime. The plan shall be produced on an annual basis and suitably documented and signed off by the Chief Executive Officer. Exercises shall be carried out on at least a quarterly basis; however, the exercise programme should be considered for updating in response to significant changes in business operations and clients, significant changes in personnel, accommodation arrangements, ICT systems, funding and specific contractual requirements.

The Business Continuity Manager will retain responsibility for ensuring that the exercise is suitably documented (using diary sheets) and that areas for potential improvement are suitably recorded and actioned.

10 Review, Performance Evaluation, Audit and Improvement

The annual review shall be carried out and suitably documented as outlined within section 8 – communication.

A Formal Review of the BCMS and all associated documentation will be carried out on at least an annual basis and prior to the annual meeting.

The results of this review, the annual meeting, regular exercises conducted and any incidents arising may require:

- An update to the Business Impact Analysis.
- A modification of the risk assessment and acceptance (or otherwise) of any individual risk identified.
- A change to control measures required.
- A change to resource needs.
- A change in Funding and budget requirements.
- Modification of BCM strategy and procedures as well as individual Business Continuity Incident Plans as necessary.

As part of this review process, where issues are identified which show that the BCMS or BCIPs are not working as planned, the item shall be detailed as a non-conformity and recorded in writing, with a recommended action (corrective or preventative). It shall ascertain the appropriate action to address the cause of the problem, with the aim of eliminating the cause & preventing its recurrence.

All improvement actions shall be recorded on an ‘Improvement action plan’ and appended to this BCMS. The plan shall specifically itemise each requirement, together with a realistic timescale for implementation. This shall be managed through the existing Rock Compliance Limited Audit Management system via Rock Compliance Limited World.

Through the implementation of this BCMS and its constant testing and reviewing as well as acting on recommended actions for improvement, Rock Compliance Limited shall aim to continually improve the effectiveness of the BCMS and their overall business resilience in the event of incidents arising.

11 APPENDICES

Appendix 1

Refer to DRP Log containing:

- Risk Assessment
- Incident Plans
- Exercise and Testing Programme
- Improvement Action Plan

Appendix 2

Sample Plan

	Risk Type	Potential Problem/s and Cause	Potential Impact	Action taken to mitigate risks
1.	**Workplace**	Fire or flood damaging a regional office or preventing access.	Loss of working office space. Damage to equipment paper records and equipment.	11 Regional offices enables business functions and storage to be transferred to other regions and members of staff to work from home where applicable. High stocks of essential equipment and materials are held in all offices and can be transferred to local employees and new local storage facility immediately. A fully electronic Operations Model which is continuously backed up minimises disruption caused by loss of paper records which are scanned on receipt where necessary. Office staff work from laptops which can be utilised from home.
2	**Information Technology**	Loss of data due to failure of systems.	Inability to maintain service visits and disruption to all operations managed by EPIC.	Disaster recovery and emergency planning issues are encompassed within management systems. All systems and firewalls are maintained to the highest standards. All computer data is backed up to the cloud daily with critical functions backed up every 4 hours. Alerts are raised in the event of back-up failures. Back up restores are undertaken in accordance with the requirement of the data type. 24/7 EPIC testing environment can be deployed as fail-over from the latest back-ups in the event of severe production outage. Systems can be restored from back up within 4 hours. All processes are reviewed at least annually.
3	**Information Technology**	Ancillary Equipment Failure – firewall, router, switches	Disruption of service	All ancillary equipment is covered by a support agreement, provided by MFM-IT, according to incident severity - down to instant call-back for the most critical issues.

	Risk Type	**Potential Problem/s and Cause**	**Potential Impact**	**Action taken to mitigate risks**
4	**Information Technology**	Virus infection on servers	Downtime and loss of data, equipment failure	All PCs/Laptops throughout the group run centrally monitored anti-virus software and monitoring agents with mobile device management software on roll-out. Primarily cloud-based system architecture ensures continuously updated security patches. Support company e-mail warnings when received from AV software companies allowing emergency AV patches to be loaded if needed. User cyber security awareness programme in effect to minimise risk from malicious actors. Service Packs and Updates applied to all servers during course of preventative maintenance visits. Computer Use Policy prohibits the use of unauthorised disks/ programs to reduce probability of virus infection and also to avoid breach of copyright law.
5	**Information Technology**	Disaffected user	Some loss of data	Rock operates a principle of least privilege, with granular permission structure in place. Automated offboarding process revokes access across all devices. Back-ups in place for key business data.
6	**Information Technology**	Breach of Security. Passwords being compromised, failure of firewall	Data loss or corruption,	Company wide mandated Multi-factor Authentication. User cyber security awareness programme in effect to minimise risk of credential compromise. Use of Cloud-based storage for shared documents ensures any local compromise is isolated.
7	**Information Technology**	Support company fails	In short term, minimal impact unless there is a problem with the system	Rock Compliance operates a hybrid support model with internal and external IT support persons. Issues are escalated by internal support, so context and knowledge can be passed on to another provider if need be.
8	**Exposure to Legionella hazard**	Risk of developing legionellosis to employees, customers and damage to business reputation	Illness and potential fatalities to employees and customers, loss of business due to damaged reputation.	Adequate qualified and competent persons employed to carry out the tasks of the company. The implementation of safe systems of work and risk assessments carried out. All procedures for all tasks documented and made known and available to all employees. Operating to highest industry standards and Risk Management incorporated within bespoke Legionella Control Management software (EPIC).

	Risk Type	Potential Problem/s and Cause	Potential Impact	Action taken to mitigate risks
9	**Staff Shortages**	Staff leaving or increase in work demand. Staff absenteeism.	Inability to maintain contractual commitments or take on new works. Damage to reputation through failure to meet with site visit arrangements and reduced profitability due to re scheduling process of planned visits.	Constantly assess labour requirements covering all aspects of the business and plan ahead through recruitment when required. Ensure skill levels are monitored and undertake training where required. Ensure high levels of employee engagement are maintained - Hold regular staff meetings. Have performance appraisals. Provide positive and constructive feedback to staff. Praise in public, reprimand in private. Avoid key person dependency by multi-skilling staff. Regularly assess remuneration of staff to ensure that marketplace packages are provided. Staff turnover rates are closely monitored. Processes in place to effectively manage absenteeism. It is the responsibility of all staff to telephone their line manager on the first day of absence by the normal starting time of their shift and give a specific reason for their absence and their anticipated date of return to work. It is the responsibility of Supervisors to manage the work pattern to avoid missed visits, to plan in advance and to reduce the impact of absenteeism. The use of EPIC enables the transfer of planned site visit information and reports to another member of staff seamlessly and the use of vehicle tracking equipment enables location of employees to determine best means of re allocation of time critical works.
10	**Immediate loss of Key contract personnel**	Loss of key operational and account management staff.	Negative impact on effective management of key contracts	We are reliant upon the competence and relationships that exist both internally and externally. Robust management structures and processes are in place across the business to ensure engagement of staff.
11	**Working with Vulnerable People**	Lack of training or poor working practices endanger vulnerable people and lead to contractual conflicts.	Legal disputes, emotional distress and potential loss of business through contractual failures.	Rock Compliance Engineers are trained to give consideration and respect to property, possessions and cultural differences practiced within properties. Working with Vulnerable People Policy document provided to employees and tool box talks provided to employees entering sites/properties with Vulnerable People present. All Rock site operatives are DBS checked.

	Risk Type	Potential Problem/s and Cause	Potential Impact	Action taken to mitigate risks
12	**Suppliers**	Ineffective management of supply chain impacts the quality of Rock Compliance service delivery and conflicts with the company ethos	Damage to business reputation and impact on productivity and subsequent profitability.	All suppliers to Rock Compliance undergo a supplier approval process which includes a questionnaire and is overseen by the Rock Compliance Quality Manager. Approved status depends upon a variety of factors including the systems in place to ensure a safe working environment, a robust continuity plan, accredited quality and environmental systems implemented to ensure that the product has minimal or no impact on the environment and that the products sustainability has been accounted for throughout the supply chain. The evaluation of competence will be augmented by site inspections, audits, and spot checks to ensure that suppliers of goods and services comply with all legislative requirements. During the supplier selection process, all relevant trade associations and accreditations are requested to ensure that the company has the required level of expertise and procedures for carrying out the works. We are committed to working across our supply chain, with customers and business partners to promote and share best practice on ethical behaviour, sustainability procurement, health and safety.
13	**Fleet – Van & Car**	Vehicle breakdown or damage through collisions	Inability to maintain workload	Regular assessment of vehicle fleet requirements. Vehicles are well maintained and have breakdown cover. We replace vehicles over 4 or 5 years, from new, dependant on mileage. Maintain spare van capacity to cover routine maintenance within fleet. If ever required short term hire is utilised.
15	**Epidemic**	Illness to employees and clients impacts our ability to deliver services and remain profitable.	Impact on service delivery and profit as well as employee welfare.	Events are somewhat outside of our control, but steps are taken to minimise risk by undertaking a 'risk assessment' and taking all reasonable steps to prevent harm to our staff and customers.