Crisis Management Plan

PHX049

1. Contents

2. Introduction

2.1 Objectives of the Plan

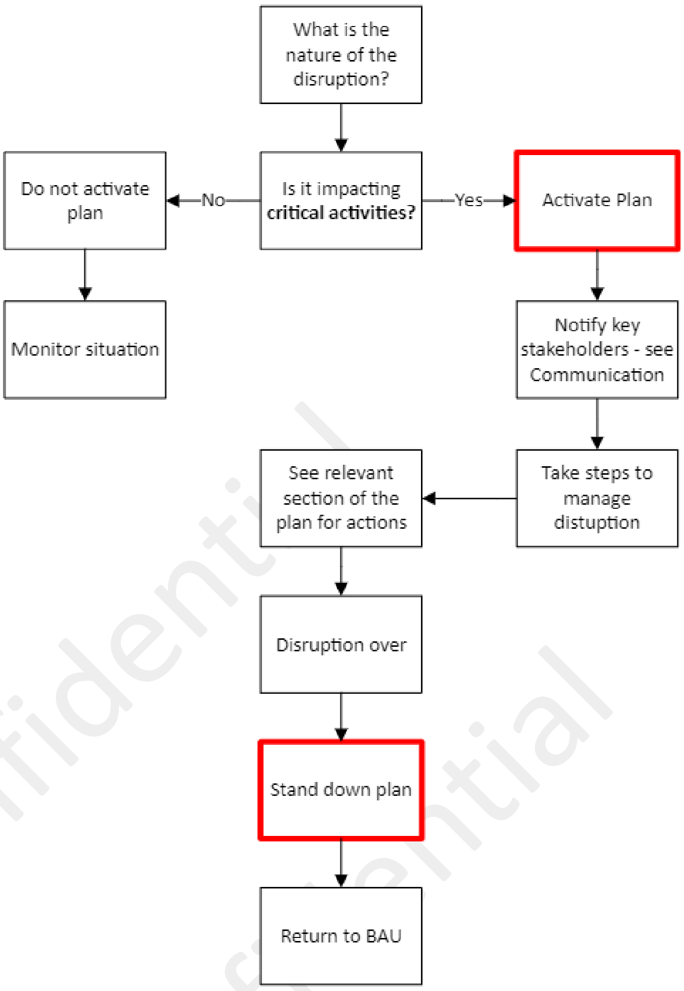
The Crisis Management Plan (CMP) has been designed to support management in providing the strategic response to any major event that does, or has the potential to, directly or indirectly threaten Phoenix's People; Property; Product; Profit; and Performance. The CMP provides the structure, direction, and resources, whilst providing flexibility to support responses to other incidents that may be experienced but not captured in detail. It aligns with Phoenix's Emergency, Operational and Tactical response and recovery plans.

2.2 What is a Crisis?

The CMP should be deployed only in the event of a Crisis. A Crisis is a situation that has the potential to:

- Threaten the ability to maintain business critical operations (or a significant part thereof), or supply to an acceptable level,
- Prevent the use of, or access to, business critical systems and data beyond an acceptable time,
- Threaten the lives or wellbeing of employees, visitors, and customers,
- Prevent a significant number of employees from working,
- Seriously damage the Phoenix brand and its reputation,
- Create major losses of critical business data, or
- Require a sudden unplanned legal process

The CMP must be flexible so that it can be used in any Crisis situation that occurs, without identifying specific causes.


What is the nature of the disruption?
Is it impacting critical activities?
No
Do not activate plan
Monitor situation
Yes
Activate Plan
Notify key stakeholders - see Communication
Take steps to manage distuption
See relevant section of the plan for actions
Disruption over
Stand down plan
Return to BAU

2.3 Principles

When managing a Crisis, the following principles should always be considered:

- Employee and visitor safety is paramount,
- Actions must be aligned to Phoenix's business objectives,
- Actions must protect the brand and reputation of Phoenix and its associated businesses, and that of Bytes Technology Group (BTG).

2.4 Operation of the Plan

The CMP is owned and operated by the Crisis Management Team (CMT). The plan assumes that those identified to have roles on the CMT have the authority to:

- Manage and co-ordinate Phoenix's response to a Crisis situation,
- Deploy necessary resources in order to support an efficient and effective resolution of the situation faced,
- Make financial commitments and authorise major spend in order to deliver solutions,
- Take strategic decisions in order to capture opportunities that emerge from the situation faced.

2.5 Deployment Guide

Once notified of the incident (see Escalation Process - Section 3), the CMT Lead / Deputy should use the Route Map below to guide them through this Plan in order to deploy an efficient and effective response should Phoenix be faced with a Crisis situation:

Step 1	Step 2	Step 3	Step 4	Step 5
Receive initial notification of the incident (Section 2.1)	Hold initial conference call / meeting using 'First Meeting Agenda' template (Section 4.5)	Allocate responsibilities	Review situation status and any new/evolving issues	Confirm resolutions of crisis situation
Record the incident and assess if it requires a crisis response (Section 2.2)	Activate the plan and allocate CMT Roles / Responsibilities	Deploy the Crisis Command Centre	Review impact assessment and revise priorities	Deactivate plan
Determine the appropriate CMT structure (Section 3.1)	Deploy Incident Logs as necessary	Activate Communications Plan	Update actions	Stand down team
Alert the CMT	Assess the potential impact of the situation	Notify BTG and provide initial situation report if appropriate	Review and maintain incident logs	Conduct post incident review (ISO Measurement Log)
Provide instruction for convening the team and confirm time/location of first conference call/ meeting (Section 3.2)	Agree immediate priorities and actions	Deploy 'Specific Event Guidance' (Section 6)	Maintain stakeholder communications	
			Continue to repeat all the above, as required	Restore business process into Business As Usual (BAU) or agree and communicate new BAU practices.

NOTE:

- All CMT members and their nominated deputies are expected to have access to this plan (stored on MS Teams) and keep their mobile devices active at all times,
- Copies of this plan and contact details of all CMT members and their deputies are accessible via company mobile phone on MS Teams,
- Contact details for CMT members and their deputies must be kept up to date and any changes must be notified to the plan author. All useful contact numbers must also be reviewed and updated on a regular basis in the same way,
- The CMT must be empowered to take ownership and assume responsibility for the strategic response to a crisis situation and have the authority to make decisions and deploy necessary resources. (The tactical response and resolution of the incident is the responsibility of the Incident Management Team (IMT) of the business area impacted), and
- The information contained within this plan is confidential. Copies of the plan must be held securely and must not be distributed beyond the CMT representatives and their deputies.

Relevant sections of the plan will be shared with key advisors.

2.6 Scope of the CMP

This document applies to Phoenix business units deemed critical for business function and contains response plans for time-critical incidents. Solutions have been developed based on risk identified through the business impact analysis.

2.6.1 Reselling of software and hardware

Software licensing is a major part of Phoenix Software followed by the supply of hardware and associated services. It fully depends on the availability of the core business applications and its databases. In a highly competitive market, a customer can quickly choose to switch their supplier. The impact of the inability to transact with our customers in the supply of licensing would have a catastrophic effect. The Board has determined the required Recovery Time Objective (RTO) and Recovery Point Objective (RPO) times and have detailed these in the Technology section below.

2.6.2 Software Asset Management

Software Asset Management is a service that maintains an inventory of license information for its customers. It relies on the provision of cloud services (Azure public cloud) to allow customer access to a SAAS platform. The impact of the service being unavailable is aligned with the service level agreement with each customer. The impact would be immediate and contractual terms determine that the customer's managed service should not beunavailable for 48 hours. The SAAS platform has a separate Service Level Agreement (SLA) which guarantees a 24-hour RTO.

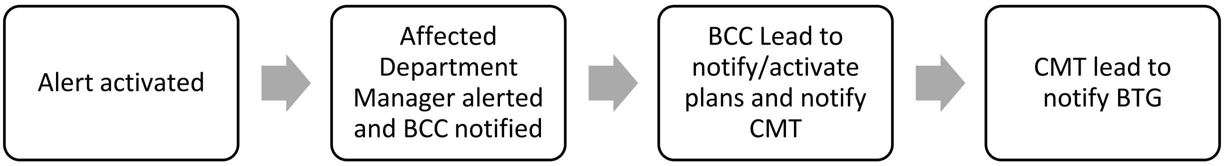
The SAM service is also a fully managed service whereby a customer's license inventory is stored and analysed onpremise at Blenheim House. The Board has determined the required RTO and RPO times and have detailed these in the Technology section below.

2.6.3 IT Managed Services

Phoenix Software manages a range of IT functions on behalf of its customer base. The impact of the service being unavailable is aligned with the service level agreement with each customer. The impact would be immediate and contractual terms determine that the customer's managed service should not beunavailable between 4 and 24 hours depending on their specific works order.

The Managed Service offerings require access to multiple portals to allow the monitoring of customer services. Phoenix utilises a third-party portal to assist with the monitoring.

The Board has agreed the required RTO and RPO times. These are available in PHX128 Phoenix Activity BIA.


Alert activated
Affected Department Manager alerted and BCC notified
BCC Lead to notify/activate plans and notify CMT
CMT lead to notify BTG

2.7 Assumptions of the plan

Detailed Planning Assumptions

The following assumptions have been taken into account when developing the plan:

- In the event of a major incident existing business premises would be out of use for more than 7 working days
- In the event of a less significant disruption some of the existing premises would remain in use
- Where a generator is not available loss of electricity supply across a region could last or up to 3 working days
- The mains water suppliers and sewerage services may be interrupted for 3 working days
- Availability of the IT network historically runs at over 98%. In the event of a partial failure of service the network could be unavailable for up to 8 working hours
- Access to the telephone network and mobile communications could be lost for up to 3 working days
- In a pandemic 25% - 30% of staff could be off work at any one time. This will include those who are sick, those caring for others and the "worried well" who are simply too scared to come to work. Working from home conditions will help mitigate impact, however on average people will be absent for less than 1 week, but some may not return
- In a fuel crisis only staff involved with delivering critical services are likely to have priority access to fuel. This will not cover Phoenix employees.

3. Escalation and Activation

3.1 Incident Escalation Process

The process detailed below should be followed by all areas of the business when a major incident is imminent, or has occurred, in order to escalate the situation and activate a Crisis response should it be necessary:

3.2 Crisis Response Activation Assessment

Following the escalation of the situation, only the Operations Director (CMT Lead) or their nominated deputy have the authority to activate the CMP. The CMT Lead should use the following for recording the incident and determining if the situation meets the definition of a Crisis (see Section 1.2). If so, the CMP and CMT should be activated immediately.

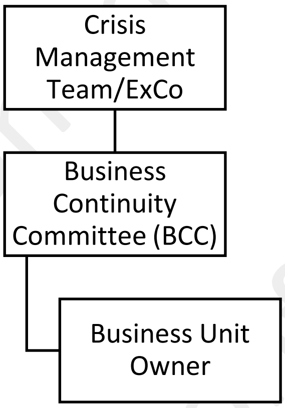
Depending on the situation faced, not all of the following questions will be relevant:

Date	**Time of notification**	**Notification received from**	**Activities affected**
What is the nature of the incident?			
When did it occur?			
Who is managing the situation?			
Is everyone accounted for?			
Has anyone been injured?			
Are Emergency Services in attendance?			
How will it affect the business and its customers?			
Have the media been alerted?			
Are any vendors/customers aware of the situation?			
Why did it happen?			
Does it require a Crisis response?			

4. Convening the Team

4.1 Team Structure

The following reporting structure is in place:


Crisis Management Team/ExCo
Business Continuity Committee (BCC)
Business Unit Owner

Crisis Management Team

The Crisis Management Team is comprised of the members of the Executive Committee:

Primary	**Deputy**
Sam Mudd – Managing Director	Clare Metcalfe – Operation Director Simon Rippon – Financial Director
Clare Metcalfe – Operations Director	Fay Mercer – Business Operations Manager
Simon Rippon – Finance Director	Matt Talbot – Management Accountant
Keith Martin – Sales Director	Sam Mudd – Managing Director Craig Taylor – Director of Cloud Solutions
Ben Rayner – Director of Managed Services and Solutions	Keith Martin – Sales Director Craig Taylor – Director of Cloud Solutions

Craig Taylor – Director of Cloud Solutions	Ben Rayner – Director of Managed Services and Solutions Keith Martin – Sales Director
Darren Goldsborough – Chief Technical Officer	Paul Chesworth – Head of IT Service Richard Barwick – Head of Service Delivery
Sean Robinson - Director of SAM & Cloud Optimisation Services	David Chamberlain – General Manager of SAM Services Clare Metcalfe – Operations Director
Trevor Hutchinson – Employee Welfare Manager	Jane Singleton – HR Manager

Business Continuity Committee

- Clare Metcalfe – Operations Director
- Fay Mercer – Business Operations Manager & deputising Governance Manager
- Shaun Tosler – Infrastructure Manager
- Rebecca Tosler – Governance Administrator

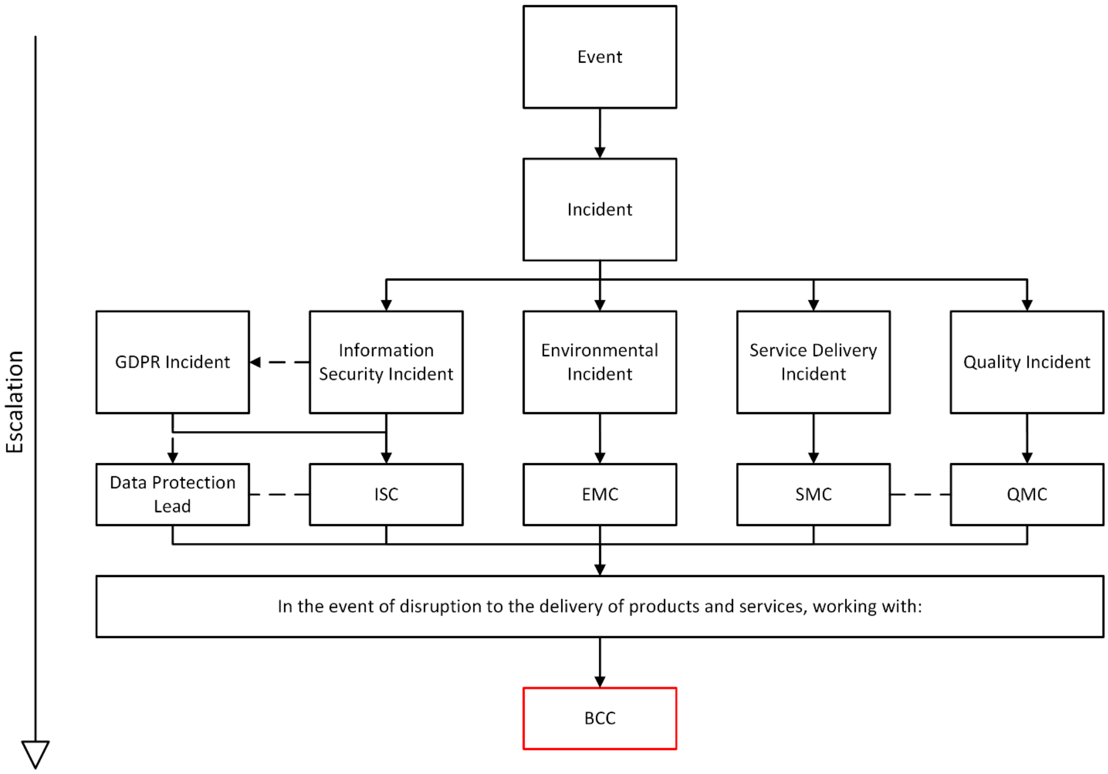
Business Unit Owners

- Department Managers

Incident Management Team – dependant on the incident.

- Business Continuity Committee
- Relevant Department/Business Unit Manager

Working with other response committees:


Event
Incident
GDPR Incident
Information Security Incident
Environmental Incident
Service Delivery Incident
Quality Incident
Data Protection Lead
ISC
EMC
SMC
QMC
In the event of disruption to the delivery of products and services, working with:
BCC
Escalation

4.2 Contact Details

Key internal contact details below – in the event of an assigned primary role, deputies are identified within Departmental Business Continuity Plans for critical activities.

Name	Position	Email Address
Sam Mudd	Managing Director	Sam-mudd@phoenixs.co.uk
Simon Rippon	Finance Director	Simon-rippon@phoenixs.co.uk
Clare Metcalfe	Operations Director	Clare-metcalfe@phoenixs.co.uk
Sean Robinson	Sales Director – License Dashboard	Sean-robinson@licensedashboard.com
Darren Goldsborough	Chief Technical Officer	gold@phoenixs.co.uk
Keith Martin	Sales Director	Keith-martin@phoenixs.co.uk
Debbie Dean	Sales Director – Education	Debbie-dean@phoenixs.co.uk
Greg Dean	Sales Director – Charities and Housing	Greg-dean@phoenixs.co.uk
Paul Scaling	Sector Sales Manager – Public Sector	Paul-scaling@phoenixs.co.uk
Lucie Collings	Sector Sales Manager – Public Sector	Lucie-collings@phoenixs.co.uk
Ben Lopez	Sector Sales Manager – Public Sector	Ben-lopez@phoenixs.co.uk
Dax Scutt	Sector Sales Manager – Education	Dax-scutt@phoenixs.co.uk
Jason Beaumont	Sector Sales Manager – Charities and Housing	Jason-beaumont@phoenixs.co.uk
Ben Rayner	Director of Managed Services and Solutions	Ben-rayner@phoenixs.co.uk
Craig Taylor	Director of Cloud Solutions	Craig-taylor@phoenixs.co.uk
Becky Wilson	Head of Microsoft Licensing & Strategic Development	Becky-wilson@phoenixs.co.uk
Jonny Scott	Alliance Manager	Jonathan-scott@phoenixs.co.uk
Ben Murden	Head of Marketing	Ben-murden@phoenixs.co.uk
Trevor Hutchinson	Employee Engagement & Staff Welfare Manager	Trevor-hutchinson@phoenixs.co.uk
Jane Singleton	HR, Payroll and Facilities Manager	Jane-singleton@phoenixs.co.uk
Natasha Jefferson	Finance Manager	Natasha-jefferson@phoenixs.co.uk
Jane Jack	Credit Control Manager	Jane-Jack@phoenixs.co.uk
Kevin Wootton	Chief Data Officer	Kevin-wootton@phoenixs.co.uk
Jayne Goddard	Operations Manager	Jayne-goddard@phoenixs.co.uk
Fay Mercer	Business Operations Manager & deputising Governance Manager	Fay-mercer@phoenixs.co.uk
Mark Pickersgill	Head of Bids Management	Mark-pickersgill@phoenixs.co.uk
David Chamberlain	General Manager of SAM	David-chamberlain@licensedashboard.com
Jason Davies	Service Delivery Manager	Jason-davies@licensedashboard.com
Steven Lamb	Managed Service Manager	Steven-lamb@licensedashboard.com
Will Booker	Data & Support Team Manager	William-booker@licensedashboard.com
Darren Moore	Head of Technology Asset Management Solutions	Darren-moore@licensedashboard.com
Andy Livesey	Development Manager	Andy-livesey@licensedashboard.com
Abbey Simpson	Service Desk Manager	Abbey-simpson@phoenixs.co.uk
Shaun Tosler	Infrastructure Manager	Shaun-tosler@phoenixs.co.uk
Richard Barwick	Head of Service Delivery	Richard-barwick@phoenixs.co.uk
Paul Chesworth	Head of IT Service	Paul-Chesworth@phoenixs.co.uk

Contact numbers are available from the Access HR system.

4.3 Initial Contact Procedure

Activation and initial communication to the CMT will be via phone, text, e-mail, or MS Teams. If the primary CMT member is not contactable, then their deputy must be contacted. The CMT Lead will provide basic information about the incident (as captured in the crisis Activation Assessment – see Section 3.2) and convene the CMT by requesting them to attend an initial meeting/conference call and confirm the time/location of this.

An MS Teams call will be activated by the CMT Lead

4.4 Team Responsibilities

- Respond to any 'Crisis' situation that may occur whether during or outside of normal working hours
- The CMT have the authority to sign off expenses required to implement response plans as per the Corporate Governance Policy.
- Manage the response to the Crisis at a strategic level
- Support the deployment and co-ordination of resources throughout the Crisis situation,
- Orchestrate and maintain effective communications with all key stakeholders both internally and externally, advising as appropriate on incident status, impact on business, and matters of governance and strategy, See: Communications Plan.
- Manage all PR communications (incl. Media) and respond to requests in order to mitigate the impact on the brand
- All staff email not to communicate with the media
- Provide financial authority and decision support to the relevant Incident Management Team and support the deployment of business recovery solutions
- Supporting and advising IMT Leads on key strategic matters
- Provide legal and compliance advice (obtain appropriate professional support -legal, financial, insurance etc. as necessary)
- Notifying business areas regarding developments and progress in managing the crisis,
- In a Supply Chain related event, agree the vendor /product/ customer priorities,
- Provide communications to the relevant business areas impacted e.g. Operations, Sales teams, IT, Human Resources etc.
- Where Supply Chain is affected, agree communication strategy to vendors and customers
- Oversee all brand and corporate stakeholder communications and ensure alignment with BTG requirements,
- Ensure recovery strategies are deployed effectively and any residual impact is notified to BTG

4.5 Crisis Management Team Meeting Templates

Templates have been created to guide the CMT through the crisis to:

- Crisis Management First Meeting Agenda

- Crisis Management Decision Log
- Crisis Management Final Meeting Agenda

All templates are attached to the printed Crisis Management Plan and distributed to all CMT members. They are also available for digital access via SharePoint, Hub, Crisis Management Tile Impact Profiling

The following matrix is designed to assist the CMT in assessing the likely impact on colleagues, the business, and its customers. It should be used to broaden the CMT's initial understanding of the situation and drive / prioritise actions by the CMT in responding to the situation faced. The CMT should make use of this matrix to describe the impact against the relevant categories.

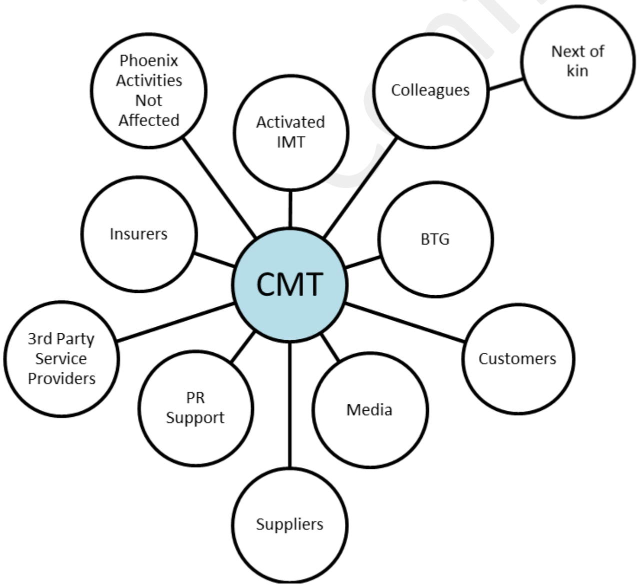
Nature of impact/Potential Impact						
People	**Building**	**Technology and Systems**	**Information and Data**	**Supply Chain**	**Services**	**PR**
Colleagues, visitors, public	Building, infrastructure, facilities	Technology, systems	Information accessibility and security	Delivery	Delivery	Brand and reputation

4.6 Crisis Command Centres

Crisis Management will take place within Blenheim House, or remotely through MS Teams as responders work from home. No command centre or alternative workspace set up is required.

5. Stakeholder Communications

The nature of the incident will determine whom the CMT will need to communicate with. The parties detailed below provide an example, but this is not intended as an exhaustive list. The CMT should refer to the Communications Plan and communication templates.



Staff must not communicate with external parties in the event of an incident unless there has been an approved statement provided by the Managing Director. All enquiries must be forwarded to bcc@phoenixs.co.uk.

To communicate with employees, Managers can utilise:

- Email/Teams
- Phone numbers available from Access HR
- In the event Access HR is unavailable, a data backup is available – see Internal IT Plan.

Where staff support is needed, contact Trevor Hutchinson as Employee Welfare Manager. For additional support, contact the Employee Accessibility Programme.

6. Specific Event Crisis Management Guidance

In a crisis, one or more of these plans may be relevant. Follow all relevant guidance to the event.

6.1 Threat to, or Loss of, Life

Event Category	**Threat of Loss of Life**	**Business Impact Assessment**	**Catastrophic**
Activities Impacted	**Impact on people**	**Stakeholder Engagement/Comms Plan**	
Localised to event	Emotional impact Family support absence	Internal: BTG Senior Management Relevant employees	External: Emergency Services Next of Kin Insurers Media
Impact Profile		**Resources Required from the Business**	
• Individual's family • Individual's business team members		• Additional resources may be needed from the following business areas: • Legal • Marketing • HR • H&S	
Recovery Constraints		**CMT's Key Tasks**	
• Operational capability of location affected if crime scene investigation or HSE investigation is required, resulting in restricted access to immediate area • Media attention		The CMT will be required to: • Inform next of kin • Deploy response taking advice from authorities • Establish employee support and assistance helpline • Take strategic/tactical decisions to manage the situation • Liaise and take direction from BTG • Liaise with relevant authorities and Emergency Services involved in any investigation as	

	required • Establish a communications strategy (contain communication – need to know basis) • Refer employees to Employee Assistance Programme for additional support. • Determine if other team members / family members require additional personal security measures and implement accordingly.

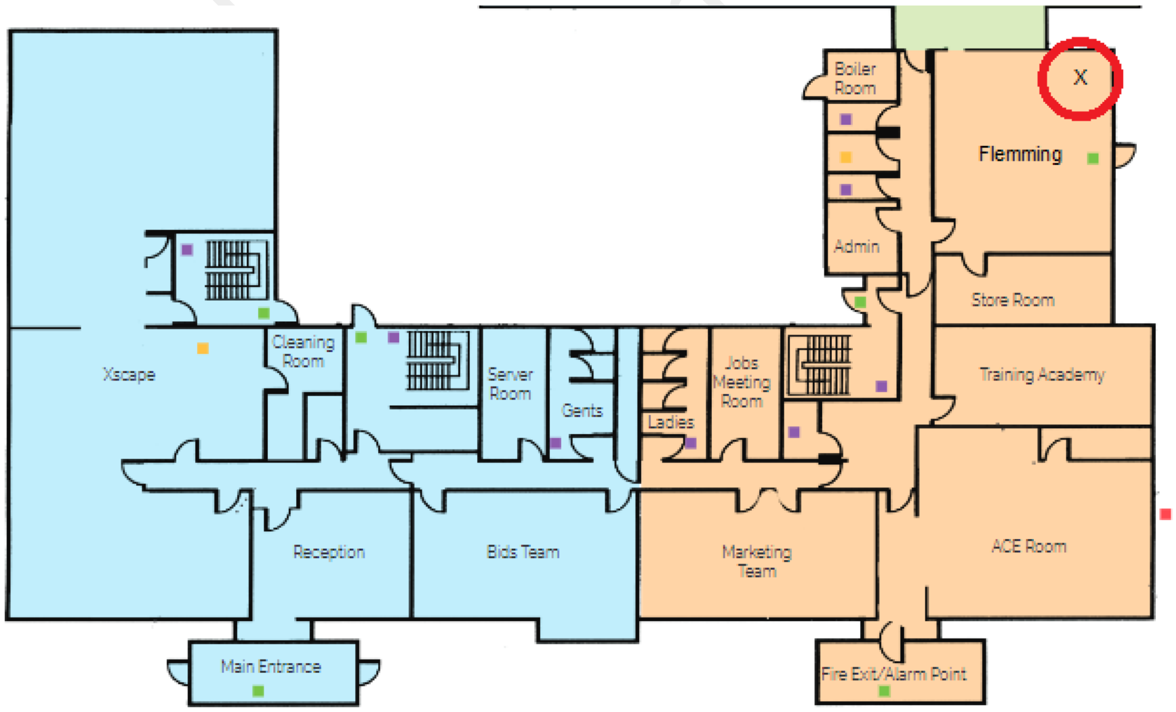
6.2 Flood/Gas Leak/Fire

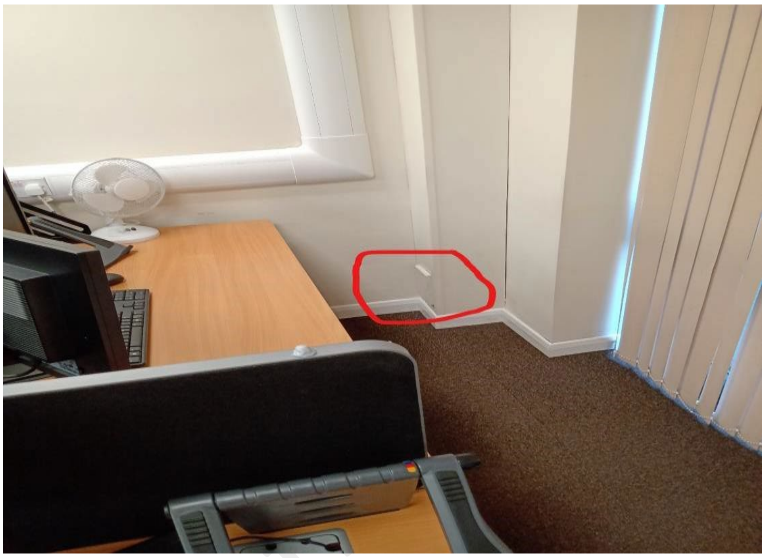
Event Category	**Flood/Gas Leak/Fire**	**Business Impact Assessment**	**Severe**
Activities Impacted	**Impact on people**	**Stakeholder Engagement/Comms Plan**	
Office activities depending on scope of event	HR/Admin/Technical additional workloads Employees unable to access office – mental health/well being	Internal: BTG Senior Management Relevant employees	External: Emergency Services Insurers Media
Impact Profile		**Resources Required from the Business**	
• Activities stopped across the business • Unplanned costs • Possible loss of employee confidence		• Additional resources may be needed from the following business areas: • Insurance/legal • Marketing • HR • H&S	
Recovery Constraints		**CMT's Key Tasks**	
• Operational capability of location affected if HSE investigation is required, resulting in restricted access to immediate area • Media attention		The CMT will be required to: • Establish and secure all relevant information and action investigation to establish source/cause of incident • Identify loss of equipment/damage to building • Notify staff of building unavailability – work from home • Establish when the building will become available • Establish legal / contractual position and appropriate action to take • Take strategic decisions that manage the situation • Liaise with relevant authorities involved in any investigation • Manage key stakeholder communications (including website) • Agree media and vendor/customer communications strategy	

For specific actions for each of the elements please see below:

Flood

- If outside of office hours, then a call will be made determining what course of action the magnitude of the flood merits. This call will be made by a combination of senior management and facilities management/admin whilst attending the site.
- If necessary, an all-staff e-mail and communication through teams will be issued to prevent staff coming onto site and staff will then work from home whilst the flood issues are resolved.
- If some areas are inaccessible and others accessible then a series of barriers will be put into place preventing access to staff to areas of danger, whilst professional help resolves the difficulties and makes safe and repairs any damaged electrics or other systems.
- If a flood occurs within office hours, then the building should be evacuated immediately, and the senior management team should decide on the best course of action in terms of working from home or what alternative course of action is safe.
- The main stop tap for the building is in the Fleming hot-desking office in the far-right corner (as shown on picture), past the full-length window blinds. It is near floor level behind a small discreet panel which is held in place magnetically and can be pulled off to access the main stop tap





Gas Leak

- Operate the nearest fire alarm point – pushing the "glass" activates the alarm and evacuate the building IMMEDIATELY.
- Everybody should evacuate the building immediately.
- People should stop using any electrical device immediately. Even a phone, light or small electrical device could ignite the gas leak.
- Leave open all doors and windows as you exit.
- Andy Baker, Trevor Hutchinson, or Jane Singleton will phone the fire brigade and the gas company once safely outside of the building.
- No-one should attempt to tackle the source or suspected source of the gas leak.

Key contacts:
Gas – Crown Gas & Power
Contract Document Q00172187-6-10
Agreement No: CG1736698
Telephone 0161 762 7744

The smell gas number: 0800 111 999

6.3 Fire

Fire procedures are available to all staff on notice boards throughout the building.

Emergency services: **999**

ON HEARING THE FIRE ALARM:

- Leave the building immediately and proceed to the signposted assembly point in the rear car park
- Report to your Team Leader/Manager or Fire Warden for the roll call
- Receptionists will collect visitor's signing in device and hand over to Andy Baker, Trevor Hutchinson, or Jane Singleton

MAKE YOURSELF FAMILIAR WITH:

- Your means of escape
- Your nearest alarm point
- The nearest fire appliance and how it should be used

IN THE EVENT OF A GAS LEAK / FIRE / FLOOD :

- Do not stop to collect your personal belongings
- Do not stop to answer the telephone
- Do not run or attempt to pass others
- Do not try to re-enter the building until you are told it is safe to do so

Facilities and CMT are responsible for contacting and liaising with emergency services

6.4 Fuel Spill

Spill kit available located at the rear of the property next to the generator. Spill procedure available within the spill kit.

Evacuated staff

In the event of inclement weather, staff can utilise local facilities including the 1079 gym. This has been pre-agreed verbally with the owner.

In the event of emergency building evacuation and staff unable to re-enter the building, staff may have left belongings behind. Transportation options for stranded staff:

Taxi:
Kumar - Brindle Gate, Pocklington - 07949574508
MNS Travel - Southfield Close, Pocklington - 07501348743
MR Travel - Brook Side Close, Barmby Moor - 07999550717
Willy's Travel - St Helens Close, Barmby Moor - 07703529099

Bus: Stop located outside of the premises.
East Yorkshire Bus Service, 01482 327142. Lines are open 8.30am-5pm, Monday-Friday.

The timetable has bus stop routes from Hull to York and York to Hull.

Internal communications: Notify all staff of the evacuation and for staff working from home to provide continuity while office staff relocate home.

Internal communications: Request out to local staff to support with any transport requirements if necessary.

6.5 Electricity Outage - Generator

The generator will be utilised in the event of a power cut. The tank holds 220L of fuel, which will keep Blenheim House running with all systems running and full complement of staff for 10 hours.

Should the electricity outage be anticipated to be longer than 7 hours. We reduce the load on the generator to critical systems only.

We hold fuel on site to enable refuelling on the generator. Generator maintenance contract with Enrogen includes refuelling should our on-site stocks be in use.

We need to provide 4 hours' notice to Enrogen (09:00 to 18:00) for fuel delivery

We aim to have 240L of fuel stored on site at any one time.

6.6 Full IT Systems Failure/Cyber Incident

Event Category	**IT Failure/Cyber Incident**	**Business Impact Assessment**	**Material**
Activities Impacted		**Impact on people**	
Office activities		Staff stood down, unable to work	
Impact Profile			
Activities stopped across the business Impact on customer fulfilment and directly impact on sales/turnover and rebates Sales, purchasing and commercial activities Phoenix brand and reputational impact			
Recovery Constraints			
Phoenix systems should be recoverable in 4 hours Recovery capabilities within Azure Disaster Recovery site Cyclical pressure points (Phoenix year-end, Public-sector year end, Microsoft yearend) Emails may not be functions – this could impact ability to manage the crisis communication Inbound and outbound phone lines may be unavailable Note: Business impact analysis (BIAs) have been completed across all departments and functions in the business. They capture and prioritise the critical resources required in order to maintain critical activities. It is the responsibility of the IMT to where practicable, deploy manual work around measures in order to maintain these critical activities to mitigate the impact to the business and its customers and, to align resources for recovering lost productivity once systems access is reinstated. **IT Critical Systems – Recovery Procedures are available within PHX230 Internal IT Department Business Continuity Plan. A physical copy of this plan is stored in the HR office and offsite with the Operations Director and Infrastructure Manager**			

6.7 Brand/Reputational Damage (including Scandal and Corporate Wrongdoing)

Event Category	**Brand / Reputational Damage (including**	**Business Impact Assessment**	**Severe**

	Scandal and Corporate Wrongdoing)		🟥
Activities Impacted	**Impact on people**	**Stakeholder Engagement/Comms Plan**	
Product/services supply Purchasing Sales	Board of Directors Colleague job concerns Scaremongering	Internal: BTG Senior Management Finance	External: Authorities (HMRC) Media Trade Press
Impact Profile		**Resources Required from the Business**	
• Possible significant reputational / brand impact • Loss of customer confidence • Possible significant financial penalties • Trading restrictions • Prosecution of Board Members • Unplanned costs (Legal / Fines / Loss of rebates / Loss of sales / Loss of profit)		Additional resource may be needed from the following business areas: • Legal • Marketing/PR (media, vendor, customer communications) • Finance • HR	
Recovery Constraints		**CMT's Key Tasks**	
• Media attention • Vendor/Customer reaction • BTG direction and requirements		The CMT will be required to: • Establish and secure all relevant information and action investigation to establish source/cause of incident • Establish legal / contractual position and appropriate action to take • Determine action to take in respect of any employees implicated (seek advice from HR) • Take strategic decisions that manage the situation • Liaise with relevant authorities involved in any investigation • Manage key stakeholder communications (including website) • Agree media and vendor/customer communications strategy • Provide direction to the purchasing, sales, and commercial teams as to what message is to be communicated to vendors and customers • Setup personal security measures for directors / family members as required • Provide situation updates to the wider business • Take all necessary action to mitigate the impact on the business and its customers	

7. Horizon Scanning

'Horizon scanning' is crucial if emergent business continuity risk scenarios are to be identified before they develop into significant threats to the business. Horizon scanning is carried out as a regular, systematic activity. Overall responsibility for horizon scanning rests with the Operations

Director who may delegate this role to other parties and/or convene appropriate risk workshops to highlight new risks.

New business continuity risks may be considered by reference to a PESTEL analysis, reviewing possible new risks within the following categories Political, Economic, Social, Technological, Environmental and Legal. When a new emergent Business Continuity risk has been identified by 'horizon scanning', an appropriate response plan should be defined, documented, and included as part of the BC Log within the Non-Conformity Log.

7.1 Departmental Continuity

Department continuity is the responsibility of each Business Unit Owner. Specific information for each department is contained within the Department Business Impact Assessments and Business Continuity Plans. All documentation can be accessed via SharePoint, Hub, Crisis Management tile, Departmental Continuity.

7.2 Key External Contacts

Function	Service	Primary Company	Contact Information	Info
IT Systems	Internet provider	Claro	01423 535 333	Account number: PH001
IT Systems	Telephone Systems	Claro Microsoft Teams	01423 535 333	Account number: PH001
IT Systems	Payroll	Sage	Datel Group	01925 849 000 – general Geoff.green@datelgroup.com – 07834 791 710
IT Systems	ITSM	ZenDesk	Eoin Brazier	Ebrazier@zendesk.com
IT Systems	Servers	Daisy	03448 632 863	Account Number: 5006350
Physical infrastructure	Security alarms	ADT	03448001999	Account Number: Intruder: 1000133929 Access: 1000619799 Fire: 1000133541 Gas Suppression: 1000139142 The Zone: 1000940864
Physical infrastructure	Gas	Crown Gas and Power	Telephone 0161 762 7744 **The smell gas no: 0800 111 999**	Contract Document Q00172187-6-10 Agreement No: CG1736698
Physical infrastructure	Water	Yorkshire Water	0333 4149040	Account number: 9091296201
Physical infrastructure	Electric	Brook Green	0207 870 4940	Account number: 200084301
Physical infrastructure	Fire	ADT	03448001999	Fire: 1000133541

Physical infrastructure	Pest control	VermEx	01904 798676	n/a
Physical infrastructure	Septic tank	Wansford	01482872666 Dom: 07802652286	n/a
Physical infrastructure	Waste removal	Forge Recycling	0345 5050905	n/a
Physical Infrastructure	Drainage Cleaning	Metro Rod York John Wrights	0800668800 01904 424114	n/a
Physical Instructure	Skip hire	RNH	01430634505	n/a
Physical Infrastructure	Electrical & Plumbing	John Wrights	01904 424114 Tony Smith (small works manager): 07747 846328 Emergency OOH: 07907038999 Mechanical (e.g boiler): 07805068692 Mechanical OOH: 07907038995	n/a
Physical infrastructure	Generator	Enrogen	01759307070 07921169797 Gavin Wilkinson 07763234113 James Brown 07703515274 Phil Barton	n/a
Physical infrastructure	Air Conditioning	AirKool	01482 371888	n/a
Physical Instructure	Building lock-up	Key Security Group	01924273050 Emergency contact: 07775 284340	n/a
Physical infrastructure	UPS	Riello	08:30 – 17:00: 01978 729 297 06:00 – 08:30, 17:00 – 23:00: 0843 853 9915	Contract Number: RMC24418
Physical Infrastructure	Insurance	Howard Collins - PIB Insurance Brokers	02038937404 OOH: 07775888933	n/a
Physical Infrastructure	Cleaning	Minster Cleaning	07970188873 – area manager	n/a

			01482 8872620 - office	
Finance	Payment	Bottomline Technologies	01189 258 250 option 2 then 1 **emea-support@bottomline.com**	*State Calling from Phoenix*

7.2.1 Other contact details:

Report an environmental incident including: damage or danger to the naturalenvironment pollution to water or land dead fish or fish gasping for air flooding from any river, stream, canal, natural spring, or the sea	Environment Agency: **0880 80 70 60**
Burst water main	Yorkshire Water: https://tell-us.yorkshirewater.com/ 0345 124 2424
Fly tipping	East Riding Council:**(01482) 393939**
Pest nuisances	East Riding Council:**(01482) 396301**
Dangerous buildings or structures	East Riding Council:**(01482) 393939**

Version Control

Author	Version	Date	Description
Richard Foster	1.0	26/04/2017	Document submitted
Richard Barwick	2.0	02/08/2018	Amendments
Clare Metcalfe	3.0	07/03/2019	Amendments
Clare Metcalfe	4.0	04/04/2019	Communication Section
Amy Trimble	5.0	08/11/2019	Disaster Recovery Data Centre added to Key Suppliers
Amy Trimble	6.0	15/11/2019	Added Service Continuity Management
Amy Trimble	7.0	20/01/2020	Environmental Incident update
Shaun Tosler	8.0	5/09/2021	IT Environment Update, Change of Job Titles and Update Document Distribution
Amy Trimble	9.0	17/03/2022	Restructure of plan to adhere to ISO 22301 best practices. Guidelines on invoking and revoking plans. Inclusion of ExCo, KW, FM into the distribution list
Amy Trimble	10.0	20/10/2022	Review in line with PwC audit response
Fay Mercer	11.0	27/04/2023	Change of personnel and job titles, amend key external contacts
Fay Mercer	11.1	10/08/2023	Change of personnel, removal of duplicate information from 7.1

Document Approval

Name	Version	Date	Position
Clare Metcalfe	1.0	26/04/2017	Operations Director
Clare Metcalfe	2.0	02/08/2018	Operations Director
Clare Metcalfe	3.0	07/03/2019	Operations Director
Clare Metcalfe	4.0	04/04/2019	Operations Director
Clare Metcalfe	5.0	08/11/2019	Operations Director
Clare Metcalfe	6.0	15/11/2019	Operations Director
Clare Metcalfe	7.0	20/01/2020	Operations Director
Clare Metcalfe	8.0	05/09/2021	Operations Director
Clare Metcalfe	9.0	17/03/2022	Operations Director
Clare Metcalfe	10.0	20/10/2022	Operations Director
Clare Metcalfe	11.0	27/04/2023	Operations Director
Clare Metcalfe	11.1	10/08/2023	Operations Director

Signed: Clare Metcalfe Clare Metcalfe, Operations Director

Dated: 10/08/2023