Business Continuity Manual

PHX120

Contents

Context of the Organisation

Understanding the organisation and its context

Established in 1990, Phoenix Software Ltd provides IT solutions to markets including Public Sector, Voluntary and Charities, Housing, Education and Corporate sectors.

In December 2020 Phoenix became part of the Bytes Technology Group PLC, with over 350 employees working out of the Yorkshire based office, remotely or to a hybrid pattern.

The IT Solutions offered to our customers include the resell of industry standard software licensing and hardware, consultancy (Professional) and managed IT services across leading edge technologies including software asset management tooling and services.

Phoenix has considered the factors and issues that can affect the Information Security Management System, these comprise of the following:

Political Factors

Change of Government political parties and policies affect the spending patterns and decision making within Central and Local Government Authorities along with the NHS and other government bodies.   These decisions may affect the timing and budgets of these organisations which may in turn influence the performance of Phoenix and associated supply chains.

Economic Factors

The economic climate can influence the timing of purchasing new IT solutions or may reduce the budgets available for investment. Our sales and marketing strategies must allow us to adapt and adjust to these conditions by offering alternative cost-effective solutions.

Social Factors

Phoenix is one of the largest employers in the local area and our ethos is to employ locally where practicable and to support local businesses. The prevailing culture at Phoenix plays a crucial role in enabling policy awareness and Phoenix recognises that business continuity awareness encourages employees to be proactive in safeguarding our assets. By considering human behaviour, communication dynamics, and culture, we can enhance the effectiveness of our business continuity efforts and ensure a more successful recovery from a crisis.

Technology Factors

The rate of technology change demands that Phoenix must continually upskill and ensure the latest technological solutions are offered to our customers. We must be diligent in retaining our current supplier and vendor products and services to remain a forerunner in the industry as well as monitoring emerging technology offerings from new sources. Phoenix also has a software development team, developing applications for internal and external use, these applications must be designed and developed securely, made fit for purpose, be resilient, maintained and business continuity friendly.

Environmental Factors

Environmental factors, such as climate change can influence the operability and availability of our assets. The cost of energy and other resources can be impacted, affecting Phoenix's ability to maintain continuity. Our geographical location may influence our environmental risks. Economic conditions can be impacted by environmental events, affecting market demand and supplier behaviour. A pandemic could severely impact workforce availability and disrupt operations.

Legislative Factors

Phoenix is affected by government policies and legislation that determine the purchasing processes that are imparted onto our government authority customers. Legislative factors shape the legal requirements and obligations that Phoenix must adhere to during a disruptive event. Compliance with relevant laws and regulations is critical for protecting the interests of Phoenix, for managing risks, and ensuring continuity of operations.

Understanding the needs and expectations of Interested Parties

Interested parties are persons or organisations that can influence the business continuity of Phoenix or can be affected by our business continuity activities;

Phoenix has determined the below interested parties and their requirements:

- **Employees** – Require guidance, training, policy awareness and contractual information to help protect the assets of Phoenix and an understanding of what is required of them during a crisis. Employees need confidence that their safety and wellbeing is also being considered.
- **Dependents** – Need their expectations to be managed and require an understanding of the communication channels during a crisis. They require assurance that that the wellbeing of their loved ones is being considered.
- **Shareholders and investors** – Confidence in the resilience of Phoenix, in its risk management framework to address all threats to business continuity, such as cyber-attacks, IT system failures, natural disasters, or supply chain disruptions. Succinct communication in a crisis.
- **Executive Committee/Board of Directors** – Need assurance that the Business Continuity Management Systems (BCMS) identifies and addresses risks that could disrupt business operations. They require business impact analysis that identifies critical business processes and the potential financial, operational, and reputational impacts of disruptions to those processes. Evidence of testing and exercising business continuity plans, and assurance of regulatory compliance.
- **Neighbours** – Require confidence that risks that could affect their property are appropriately managed and mitigated, i.e. a fire at Phoenix would be managed and contained as to not impact the businesses nearby on the industrial estate or the fields which surround Blenheim House.

- **Government agencies/regulators** – Expect Phoenix to comply with applicable laws and regulations related to business continuity and disaster recovery. They may require Phoenix to conduct exceptional risk assessment under certain conditions.
- **Customers** – Confidence and compliance with continuity and assurance clauses in contracts and general business activities. A significant number of Phoenix customers operate in the Public Sector where supplier continuity is paramount. Some customers are also subject to the Civil Contingencies Act.
- **Media** – The media requires timely, succinct, and transparent responses to major business continuity incidents to negate opportunities for competitors to take advantage of and to keep the public informed. The appointed spokespeople of Phoenix must be accessible by the media to receive statements and press releases.
- **Suppliers (including Sub Contractors)** – Suppliers need to understand the criticality of supplies to Phoenix's operations to ensure their preparedness in a business continuity situation. Both Phoenix and suppliers need to be confident that business continuity arrangements and disaster recovery plans are robust and fit for purpose in the event of a crisis to either party, or both. Suppliers need to be compliant and need assurance from Phoenix on their compliance with Data Security and Privacy regulations such as GDPR.
- **Auditors and certifying bodies** - External auditors and certifying bodies will assess the effectiveness of our BCMS for compliance with relevant standards.
- **Insurers** – Our insurers need a good understanding of Phoenix's risk profile, our risk assessment and mitigation strategies. They want to know that we have identified potential risks and have taken appropriate measures to reduce their impact.

Procedures are in place to ensure legal and regulatory requirements are identified and adhered to through legal horizon scanning (see PHX079 Horizon Scanning Procedure).

Applicable legislation, regulations and other requirements are taken into account through the maintenance of the BCMS.

New or variations of requirements are communicated to affected employees and other interested parties.

Interested party feedback, needs and expectations are considered at committee meetings and management reviews.

Determining the scope of the Business Continuity Management System

The scope of the BCMS for Phoenix is as follows:

The Business Continuity Management System Policy applies to all our offerings which include reselling of software licensing and hardware, Managed and Professional services and supply of Software Asset Management services. The sectors serviced are Public Sector, Charities & Housing Associations , Education and Corporate. Sales and services are delivered by the employees, systems and business processes within Blenheim House, York Road, Pocklington, York YO42 1NS

Departmental Application

All business departments at Phoenix have been subject to a thorough business impact analysis with the following categories of adverse circumstances being considered:

- People
- Building
- Suppliers
- Finance
- Technology and Systems
- Information and Data

The following impacts have been identified:

Department / Impact area	People	Building	Suppliers / Subcontractors	Finance / cashflow	Technology and Systems	Information and Data
Bids	X	-	X	X	X	X
Building Facilities	X	X	X	X	X	-
Business Processes	X	-	-	X	X	X
Cloud Solutions	X	-	X	X	X	X
Consultancy	X	-	X	X	X	X
System Development and Testing	X	-	X	X	X	X
Finance*	**X**	**-**	**X**	**X**	**X**	**X**
Governance	X	-	-	X	X	X
Human Resources & Administration	X	-	X	X	X	X
Internal IT*	**X**	**X**	**X**	**X**	**X**	**X**
LDL Development	X	-	X	X	X	X
Marketing	X	-	X	X	X	X
Microsoft Licensing	X	-	X	X	X	X
Operations*	**X**	**-**	**X**	**X**	**X**	**X**
Project Management	X	-	X	X	X	X
Sales*	**X**	**-**	**X**	**X**	**X**	**X**
Managed Service Delivery*	**X**	**-**	**X**	**X**	**X**	**X**
Solutions	X	-	X	X	X	X
Training and Development	X	-	X	X	X	X
Vendor Alliances	X	-	X	X	X	X

*Identified as critical departments

Prioritisation

The prioritisation of activities has considered the activities of the business; health and safety; legal and regulatory requirements; contractual obligations and cashflow.

Legal and regulatory requirements include those listed in the Legal Register.

Contractual requirements are broken down into:

- Reselling software – point in time transaction reliant on the supplier to fulfil.
    - If software reselling stopped, cashflow would be impacted.

- Reselling hardware – point in time transaction reliant on a distributor to provide and ship goods.
    - If hardware reselling stopped, cashflow would be impacted. If the goods were not provided a potential breach of contract would occur.

- Professional services – one-off project work defined by a statement of work.
    - If we could not provide professional service, contract breach may take place. Alternatively, the work could be postponed or outsourced.

- Managed services – ongoing support contracts defined within service descriptions spanning over 3 years.
    - If we could not provide managed services, we would be in breach of contracts and Service Level Agreements. This may lead to a breach of contract and potential legal action.

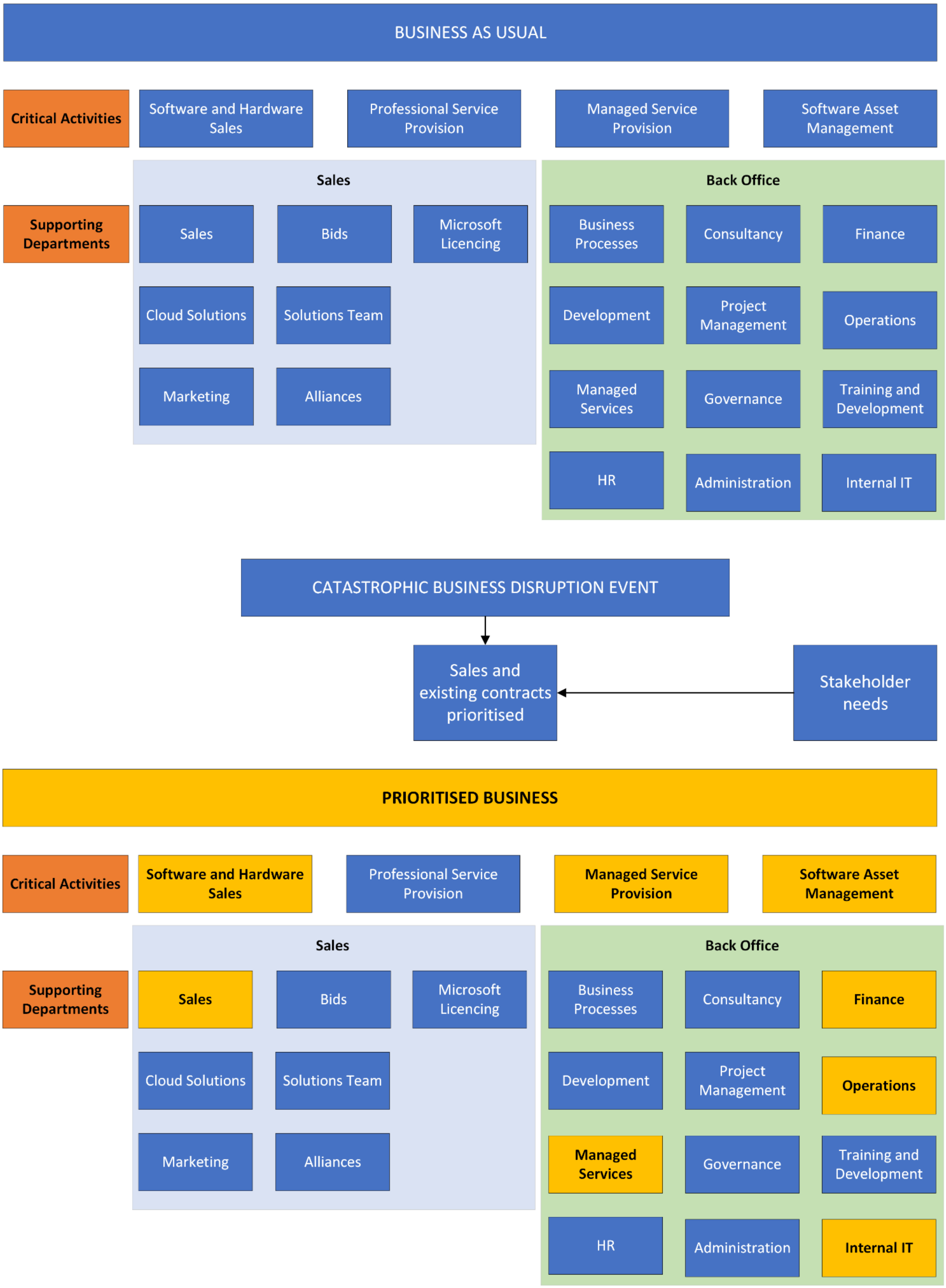
The business departments are split into Sales and Back Office departments. Each department performance business activities, however in the event of adverse circumstances impacting business as usual, the following activities have been deemed critical for business continuity:

- **Software and Hardware Sales**: this activity prioritised cash flow into the business.
- **Managed Service and Professional Services Provision**: failure to continue service delivery will result in breaches of contractual obligation and potential legal action from customers.
- **Software Asset Management**: failure to continue software asset management contracts will result in breaches of contractual obligation and potential legal action from customers.

The following departments perform a key role in performing the identified critical activities:

- Sales
- Finance
- Operations
- Managed Services
- Internal IT

All department have priorities and plans in place in the event of adverse circumstances impacting business as usual. Critical activities are prioritised in a crisis event.



BUSINESS AS USUAL

Critical Activities

Software and Hardware Sales

Professional Service Provision

Managed Service Provision

Software Asset Management

Supporting Departments

Sales

Sales

Bids

Microsoft Licencing

Cloud Solutions

Solutions Team

Marketing

Alliances

Back Office

Business Processes

Consultancy

Finance

Development

Project Management

Operations

Managed Services

Governance

Training and Development

HR

Administration

Internal IT

CATASTROPHIC BUSINESS DISRUPTION EVENT

Sales and existing contracts prioritised

Stakeholder needs

PRIORITISED BUSINESS

Critical Activities

Software and Hardware Sales

Professional Service Provision

Managed Service Provision

Software Asset Management

Supporting Departments

Sales

Sales

Bids

Microsoft Licencing

Cloud Solutions

Solutions Team

Marketing

Alliances

Back Office

Business Processes

Consultancy

Finance

Development

Project Management

Operations

Managed Services

Governance

Training and Development

HR

Administration

Internal IT

Scope Exclusions and Assumptions

Exclusions to the business continuity planning include:

People - N/A

Building - N/A

Suppliers / Subcontractors - N/A

Finance - N/A

Technology and Systems

- Microsoft applications: the business accepts the impact of a Microsoft application outage. Communication methods are in place via social media; however we accept Microsoft business continuity plans and provisions. The data remains in scope.
- Critical systems have contingency and restoration procedures in place. The contingency procedures do not have restoration in place. e.g. no contingency is in place for the backup solution.

Information and Data - N/A

Business Continuity Management System

Our BCMS is in place due to senior management sponsorship, approval, and leadership in accordance with ISO22301.

As part of the management system, regular reviews are undertaken to ensure the effectiveness and identify improvements required by the Standard, changes to the business and interested parties.

Leadership

Operations Director

The OD is responsible for:

- Determining the business continuity objectives and provide adequate resources to ensure the effectiveness of the objectives
- Assigning the responsibilities for business continuity
- Sponsorship of the business continuity management system
- Providing resources needed to implement business continuity
- Performing business continuity management reviews.
- Providing final sign-off for policies and procedures

Business Continuity Committee

Roles and responsibilities for the maintenance and management of the Business Continuity framework:

The BCC holds primary responsibilities for business continuity at Phoenix and ensures the business continuity policies and procedures are established, communicated, and complied with throughout the organisation. The BCC is responsible for:

- Publishing the business continuity policy
- Interpreting the continuity needs of the business and implementing appropriate contingency plans
- Ensuring that the business continuity management system is aligned with the strategic goals of the organisation.
- Developing policies and procedures to ensure continuity
- Contact with authorities
- Defining, implementing, and testing continuity procedures
- Assessing business continuity risk

The business continuity committee consists of the following members:

Name:	Clare Metcalfe
Job Title:	Operations Director
Competence:	Head of the BCC and member of the board, brings strong commercial knowledge and understanding of prioritisation.
Deputy:	Sam Mudd – Managing Director

Name:	Fay Mercer
Job Title:	Business Operations Manager
Competence:	Brings strong business knowledge, understanding of prioritisation.
Deputy:	Clare Metcalfe – Operations Director

Name:	Shaun Tosler
Job Title:	Infrastructure Manager
Competence:	Brings technical understanding for systems maintenance and recovery
Deputy:	Will Ford – Senior Infrastructure Analyst & Richard Barwick – Head of Service Delivery

Name:	TBC – Fay Mercer currently deputising
Job Title:	Governance Manager
Competence:	Internal Audit, BSI liaison, documentation, Standard conformance, reporting and system maintenance
Deputy:	Fay Mercer – Business Operations Manager

Name:	Rebecca Tosler
Job Title:	Governance Administrator
Competence:	Internal Audit, BSI liaison, documentation, and system maintenance
Deputy:	Vikki Smith – HR/Administration Officer

Response roles and responsibilities are documented within each department business continuity plan and within the Crisis Management Plan.

Managers

Managers are responsible for:

- Ensuring staff and contractors follow business continuity procedures when required
- Provide guidance, communication, and liaison to their teams in the event of Business Continuity event
- Maintenance of their departmental business continuity plan

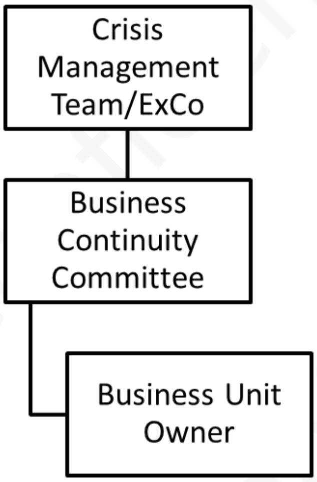
All Staff

All employees, third parties and contractors are responsible for:

- Reporting incidents
- Following guidance when issued

Response Structure

The following response structure is in place:



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

Primary	Deputy
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
- TBC – Governance Manager
- Shaun Tosler – Infrastructure Manager
- Rebecca Tosler – Governance Administrator

In the event of absence, the team will continue without the use of deputies.

Business Unit Owners

- Department Managers

Incident Management Team – dependant on the incident

- Business Continuity Committee
- Relevant Department/Business Unit Manager

Response roles and responsibilities are available within PHX049 Crisis Management Plan.

Policy

The Management of Phoenix has established and business continuity policy that:

- is appropriate to the purpose of the company
- includes business continuity objectives
- includes a commitment to satisfy the requirements related to the Standard
- includes an assurance of continual improvement of the BCMS

The business continuity policy is:

- available as documented information on SharePoint
- communicated within the company
- available to interested parties, as deemed appropriate by the Business Continuity Committee

Planning

Actions to address risks and opportunities

When planning for the BCMS, the company has considered the context of the organisation and determined the risks and opportunities that need to be addressed to:

a) ensure the business continuity management system can achieve its intended outcomes
b) prevent or reduce undesired effects
c) achieve continual improvement

Key events have been risk assessed to prioritize response plans and efforts to prevent occurrence or mitigate the impact.

The company plans actions to address risks and opportunities utilising the BCMS processes. This includes measurement and evaluation for effectiveness.

The Business Continuity Committee meet at least annually to assess and evaluate the system through the Management Review requirement.

The Business Continuity Management process for Risk Management and Risk Assessments is documented in the Enterprise Risk Management Framework.

The Enterprise Risk Management results then identify priority operational processes to inform response plans and response efforts.

Business Continuity Objectives and planning to achieve them

Phoenix has established the business continuity objectives for relevant functions and levels within the Business Continuity Policy located on SharePoint.

The achievement of objectives is reported through the Business Continuity Management Reviews to ensure they remain on track and appropriately monitored.

Support

Resources

Phoenix has allocated the resources required for the establishment, implementation, maintenance, and continual improvement of the BCMS.

Additional resource needs are covered as part of the Business Continuity Management Review.

Competence

The company has determined the necessary competence of person(s) doing work under its control that affects its business continuity performance by utilising in-house Governance Risk Compliance consultants to perform assurance and consultancy regarding business continuity throughout the implementation, management, and maturity of the Standard. These individuals are certified through BSI accreditations and therefore deemed appropriate to guide the implementation and evidence of competency certification is obtained.

Throughout business continuity strategies and solutions, business unit managers have been identified as primary action owners. The business deems these individuals to have the appropriate skills, experience and business understanding to be tasked with the assigned responsibilities. Secondary members of staff identified are also considered competent to undertake the role if required.

Individuals with roles and responsibilities within the BCMS have been approved by the Board and Human Resources.

The competencies and key behaviours of the Crisis Management Team that are deemed to be the most critical in a Crisis response situation are:

COMMUNICATION **Competency Statement:** Communicates during times of crisis in a timely, clear, accurate, and truthful manner. **KEY BEHAVIORS:** • Communicates effectively and concisely with internal and external audiences in the face of limited, unknown, stressful, and negative situations • Expresses the crisis, mission, expectations for response team members and decisions in clear and compelling terms appropriate for the target audience • Initiates communication using vertical and horizontal channels of communication to keep stakeholders informed	**CONNECTIVITY** **Competency Statement:** Activates a network of interested parties and meets the immediate (and changing) needs of the response. **KEY BEHAVIORS:** • Interacts effectively with interested parties and facilitates collaboration • Uses influence and diplomacy skills to reach a goal, to build consensus, or to resolve a conflict • Links knowledge of networks to successfully accomplish mission objectives
COURAGE AND PERSEVERANCE **Competency Statement:** Displays strength, confidence and persistence when faced with danger, uncertainty, or intimidation. **KEY BEHAVIORS:** • Takes appropriate risks and accepts responsibility for the outcome • Addresses resistance quickly, rationally, and fairly with due consideration. • Perseveres under difficult circumstances.	**CREDIBILITY** **Competency Statement:** Demonstrates expertise and trustworthiness during crisis; earns the confidence and respect of interested parties **KEY BEHAVIORS:** • Demonstrates knowledge and experience in their area of expertise • Exhibits humility; recognises personal strengths and weaknesses; looks to others for guidance on topics outside of personal expertise; admits to mistakes and takes corrective action.

• Displays steadfast adherence to public health priorities despite hardship or obstruction.	• Determines the appropriate information to share, and when to engage others in conversations, decisions, and actions. • Acts in accordance with legal compliance, ethics, and organisational values for the common good of those responding to and impacted by the crisis.
DECISIVENESS **Competency Statement:** Makes critical, timely decisions when faced with ambiguous information about the disaster and response efforts. **KEY BEHAVIORS:** • Gathers facts, solicits input, makes reasonable and appropriate assumptions, consults with critical stakeholders, and weighs the benefits and risks in order to make and execute decisions quickly with incomplete or limited information. • Makes decisions rapidly; based on prior experience, intuition, and knowledge of established protocols. • Applies appropriate decision-making processes – systematic problem-solving verses experience / intuitively derived — based on the conditions and context of the emergency response situation. • Perceives and anticipates the impact and implications of decisions. • Assesses and adjusts decisions and actions in response to changing information.	**EMOTIONAL EFFECTIVENESS** **Competency Statement:** Recognizes the impact crisis has on one's self and others and promotes positive interactions under emergency response conditions. **KEY BEHAVIORS:** • Demonstrates self-awareness and responds constructively to problems and difficult interactions. • Recognizes survival instincts and signs of stress, demonstrates mental discipline, and maintains control. • Considers and responds to the needs, feelings, and capabilities of team members, stakeholders and individuals impacted by the crisis. • Promotes an environment of safety, connectedness, and hope.
INTEGRATIVE THINKING **Competency Statement:** Identifies what is critically important during an emergency and uses the information to strategically lead, balance priorities, and anticipate consequences. **KEY BEHAVIORS:** • Synthesizes information into a coherent plan with a clear, yet flexible, strategy and priorities demonstrated through operations, tactics, and logistics • Re-adjusts objectives based on changing priorities to align capacity and create desired results • Proactively assesses and addresses both day-to-day and long-term problems and opportunities • Anticipates probable and possible events; develops innovative and adaptive solutions to current and potential crisis situations	**SITUATIONAL AWARENESS** **Competency Statement:** Identifies, processes, and comprehends the critical elements of an emergency with public health consequences. **KEY BEHAVIORS:** • Compiles a plausible picture of the situation that is compatible with the known facts and potential outcomes • Acquires, represents, interprets, and utilizes relevant information in order to make sense of current events, to anticipate future developments, and to make intelligent decisions • Demonstrates awareness of environment and activities; stays abreast of the mission status; continually assesses and reassesses the situation

TEAM LEADERSHIP

Competency Statement:
Leads, inspires, motivates, and guides emergency response team members in a safe and effective manner.

KEY BEHAVIORS:

- Models' actions and behaviours that inspire and motivate positive responses from team members during a crisis
- Takes initiative to identify key cross-functional team personnel needed; obtains required resources and information so team members may effectively respond to the crisis
- Recognises, acknowledges, and addresses the impact of stress on their team during a crisis and makes themselves available and visible to the team when responding to the event
- Delegates roles, responsibilities, and decisions appropriately; shares responsibility, accountability, and recognition; gives guidance, and promotes autonomy for others to make decisions within guidelines during the crisis
- Manages and resolves disputes and disagreements among team members in a positive and constructive manner
- Demonstrates flexibility when confronted with deviations from standard procedures, monitors changes in the performance of other team members.
- Develops, communicates, and monitors expectations for team performance.

Measurement criteria for assessing competency attainment is via:

Skills Assessment: This involves an examination of a personal ability to complete certain tasks. This will be tested through simulated Crisis scenarios such as a ransomware tabletop exercise and demonstration of role requirements through real life scenarios.

Knowledge: This involves testing the person's understanding of certain concepts important for the job or task. This will be shaped by prior learning and knowledge through training and life/work experiences.

Performance Evaluation: This is an assessment of how well a person has performed assigned tasks over a certain period. This will be captured by regular 1:1 meeting with their Line Manager

Behavioural Analysis: This involves evaluating how a person reacts or behaves in certain circumstances. This will be tested through simulated Crisis scenarios such as a ransomware tabletop exercise and demonstration of role requirements through real life scenarios.

Self-assessment: An individual's self-evaluation of their own skills, behaviour, and performance. This will be assessed via Alva Labs and The Emotional Intelligence Profile (EIP3) through Talogy

Skills matrix of the CMT competencies:

	Managing Director	Operations Director	Finance Director	Sales Director	Director of Managed Services and Solutions	Director of Cloud Solutions	Chief Technology Officer	Director of SAM & Cloud Optimisation Services
	CMT	**CMT & BCC**	**CMT**	**CMT**	**CMT**	**CMT**	**CMT**	**CMT**
Communication	Expert	Expert	Expert	Proficient	Proficient	Proficient	Proficient	Proficient
Connectivity	Expert	Expert	Expert	Proficient	Proficient	Proficient	Proficient	Proficient
Courage and Perseverance	Expert	Expert	Expert	Proficient	Proficient	Proficient	Proficient	Proficient
Credibility	Expert	Expert	Expert	Proficient	Proficient	Proficient	Proficient	Proficient
Decisiveness	Expert	Expert	Expert	Proficient	Proficient	Proficient	Proficient	Proficient
Emotional Effectiveness	Expert	Expert	Expert	Proficient	Proficient	Proficient	Proficient	Proficient
Integrative Thinking	Expert	Expert	Expert	Proficient	Proficient	Proficient	Proficient	Proficient
Situational Awareness	Expert	Expert	Expert	Proficient	Proficient	Proficient	Proficient	Proficient
Team Leadership	Expert	Expert	Expert	Proficient	Proficient	Proficient	Proficient	Proficient

Novice:	A novice is a beginner who lacks experience in a skill, subject, or activity. They often require close supervision or instruction to perform a task or role. They usually rely on rules and guidelines to perform tasks and may struggle when those rules do not directly apply.
Advanced Beginner:	An advanced beginner has surpassed the novice stage and has gained experience on real tasks that show sufficient recurring components. They start to understand the situation contextually and can generally deal with increasingly complex tasks, but their exposure is still limited, and they may need guidance.
Competent:	A competent person has the necessary ability, knowledge, or skill to do something successfully. They can fulfil the role or task requirements, but may still need some assistance or supervision, particularly in complex scenarios.
Proficient:	Proficiency refers to a high degree of competence or skill. A proficient individual is capable of performing a job or task without requiring supervision and with high quality, efficiency, and effectiveness.
Expert:	An expert is a person who has comprehensive and authoritative knowledge or skill in a particular area. They are highly experienced and can solve problems based on their instinct and deep understanding.

Awareness

Persons doing work under the company’s control are aware of (when appropriate):

a) the business continuity policy
b) their contribution to the effectiveness of the BCMS, including the benefits of improved business continuity performance
c) the implications of not conforming with the BCMS requirements
d) their own role during disruptive incidents.

Communication

Phoenix has determined business continuity communications required as part of the BCMS within response plans, including internal and external communications to interested parties.

Department activities and required communications and those responsible are documented within the Departmental Business Continuity Plan, the Crisis Management Plan has an associated Communications Plan, supported by the Marketing Team.

Documented Information

The BCMS includes the documented information required by the ISO22301 standard as determined by Phoenix as being necessary for the effectiveness of the system.

This is managed and maintained in line with the Document Control Process and stored within the Document Control Register.

Operation

Operational planning and control

The BCC has planned, implemented, and controlled the processes needed to meet business continuity requirements through the development of business continuity plans and test procedures.

The company has ensured that outsourced processes are determined and controlled through supplier management practices

Business Impact Analysis and Risk Assessment

The company has established, implemented, and maintains a documented process for business impact analysis and risk assessment through the Enterprise Risk Management Framework that established the context of the assessment, defines criteria, and evaluates the potential impact of a disruptive incident.

The following definitions and criteria have been developed and are applied throughout the BCMS application:

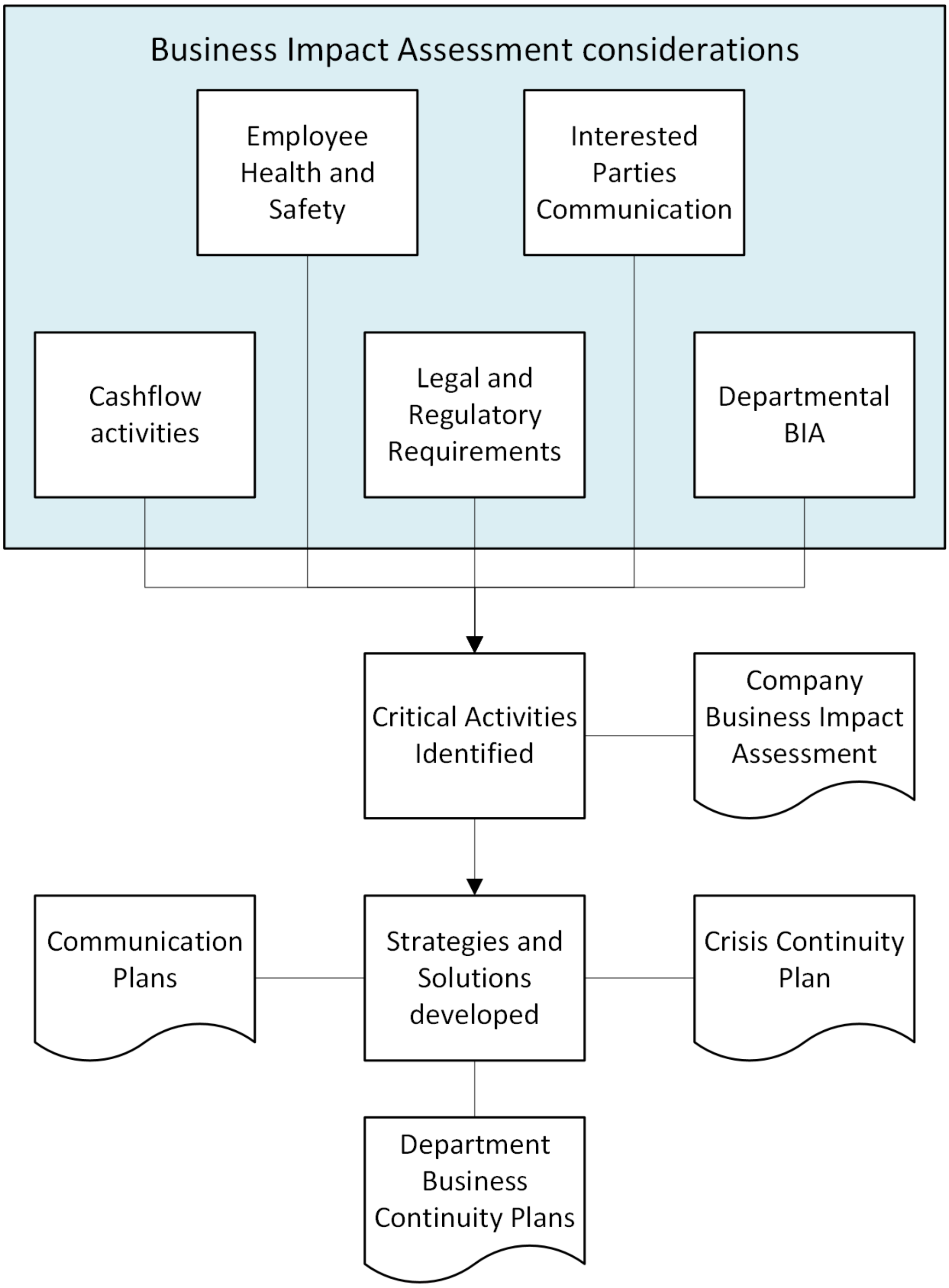
Impact Category	Category Definition	Business Examples
Catastrophic	A disaster with a potential to lead to the collapse of the company and is fundamental to the achievement of objectives.	• Major disruption to business continuity resulting in failure to meet SLA and contractual obligations which would trigger an immediate cessation of the contract • Breach of regulatory or legal requirement • Loss of critical/primary business funding source • Business brand damaged • Disruption to entire system or infrastructure which cannot be accommodated by altered operational routines or stand-by infrastructure (i.e., no backup site exists) • Human death suffered.
Severe	An event which can be endured but which may have a prolonged negative impact and extensive consequences to the company.	• Serious disruption to business continuity resulting in failure to meet SLA and contractual obligations • Loss of major source of business funding • Disruption to entire system or infrastructure device which can be accommodated by altered operational routines or stand-by infrastructure (i.e. loss of primary processing site where a backup site exists) • Serious or multiple human injuries suffered • Adverse publicity nationally/internationally
Material	Major events, which can be managed but that require additional resources and management effort.	• Disruption to business continuity yet still within SLA • Loss of minor source of business funding • Disruption to single critical device which cannot be accommodated by altered operational routines or stand-by component • Significant human injuries suffered • Adverse publicity locally • Some lost time as a result (i.e., less than 1 day).
Moderate	Consequences can be absorbed under normal operating conditions.	• Minor disruption to business continuity • Disruption to single critical device which can be accommodated by altered operational routines or stand-by component • Minor human injuries suffered • No lost time as a result.
Minor	The impact is minor and can easily be contained.	• Breach of policy but no disruption to business continuity • Disruption to single (non-critical) device which can be accommodated by altered operational routines or stand-by component • No lost time as a result

The BIA and risk assessments take into account legal and internally defined requirements; systemic analysis, risk prioritization or risk treatment and costs; defined outputs of the BIA and risk assessment; and specifies the requirements to keep the information up-to-date and confidential through access rights.

Each department has a Business Continuity Assessment where critical activities are identified by the business unit owner. These activities are considered alongside the legal and regulatory requirements of the business to form the Company Business Impact Assessment. Here, the priorities of activity recovery are identified. This informs the Crisis Continuity Plan and the requirements for strategies and solutions through the business.

Strategies and Solutions are developed within the Departmental Business Continuity Plan.

Any time-critical responses are documented within the Crisis Management Plan, for example fire or gas leak which pose a risk to life.

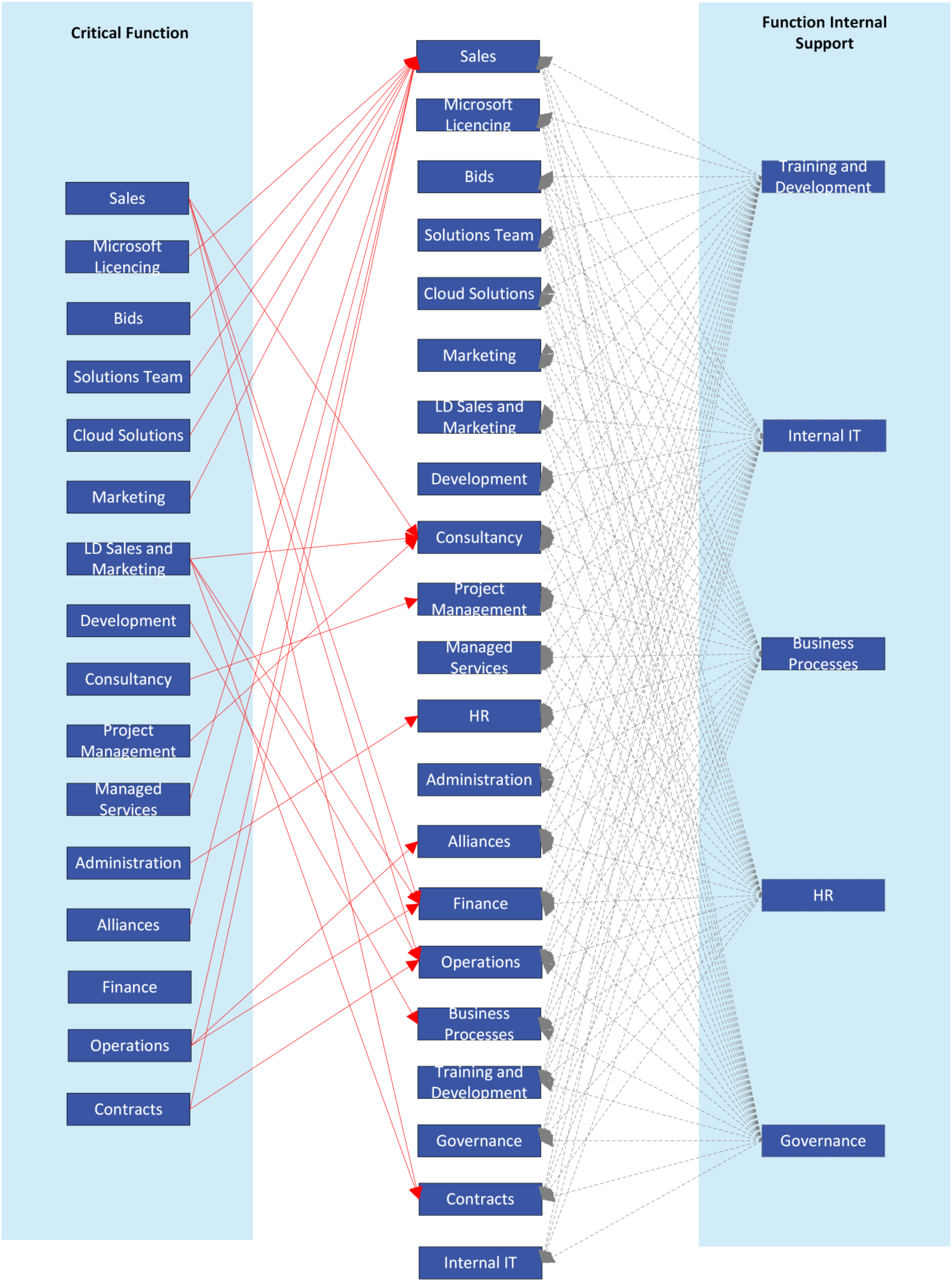

Business Impact Assessment considerations
Employee Health and Safety
Interested Parties Communication
Cashflow activities
Legal and Regulatory Requirements
Departmental BIA
Critical Activities Identified
Company Business Impact Assessment
Communication Plans
Strategies and Solutions developed
Crisis Continuity Plan
Department Business Continuity Plans

Phoenix has established, implemented, and maintains documented evaluation process for determining continuity and recovery priorities, objectives, and targets.

This includes assessing the impacts of disruptive activities that support our products and services. This analysis includes:

- Identified activities and systems that support the provision of products and services
- Assessing of impacts over a time of not performing these activities
- Setting prioritized time frames for resuming these activities at a specified minimum acceptable level, taking into consideration the time within which the impacts of not resuming them would become unacceptable; and
- Identifying dependencies and supporting resources for these activities, including suppliers, outsource partners and other relevant interested parties.
- These are documented within the Departmental Business Impact Assessments.

Process Dependency Map



The organisation retains documented information of the results of the business continuity risk assessments.

Reviews of risk assessments are performed by the Business Continuity Committee on an annual basis and as required due to changes in the company, systems, processes, information, people, assets, outsourced partners, and other supporting resources.

This is documented in the Enterprise Risk Management Framework documentation.

Business Continuity Strategy

The business continuity strategy is based on outputs from the business impact analysis and risk assessment. The strategy is appropriate for:

a) Protecting prioritised activities
b) Stabilizing, continuing, resuming, and recovering prioritised activities and their dependencies and supporting resources, and
c) Mitigating, responding to, and managing impacts.

The strategy includes approving prioritised time frames for the resumption of activities.

Resource considerations for the development of the strategy include:

- People
- Building
- Suppliers
- Finance
- Technology and Systems
- Information and Data

These considerations have been applied where appropriate to critical activities as department level within the Departmental Business Continuity Plans.

The business continuity capabilities of suppliers are evaluated when appropriate to critical activities.

Strategies and Solutions

Before:

- Horizon scanning
- Notification assessment
- Business Impact Assessment Reviews
- Tabletop Exercises
- Management Review

During:

- Crisis Management Plan
- Department Business Continuity Plans
- PHX022 Crisis Management First Meeting Agenda
- PHX033 Crisis Management Decision Log
- PHX082 Crisis Management Final Meeting Agenda

After:

- Communications out to interested parties as appropriate
- Event Log
- Lessons Learnt
- Management Reviews
- Review Business Impact Assessment

Strategies and solutions have been implemented based on the activity downtime and remain proportionate to predefined risk impact definitions. These have been identified through Business Impact Analysis and identified the prioritised activities required to keep the business operational.

These strategies and solutions are in place to mitigate the impact and length of downtime and are based on people, building, technology and systems, information and data, finance and suppliers and identify resource allocation as appropriate.

Establish and implement business continuity procedures

The company has established, implemented, and maintains procedures including the PHX049 Crisis Management Plan, the PHX022 Crisis Management First Meeting Agenda, the PHX033 Crisis Decisions Log, the PHX082 Crisis Management Final Meeting Agenda and the Departmental Business Continuity Plans designed to manage disruptive incidents and continue business activities based on recovery objectives informed by the business impact assessments.

The incident response structure within the Crisis Management Plan utilises individuals with the necessary responsibility, authority, and competence to manage an incident.

The BCC will liaise with senior management and the board to communicate externally about the significant risks and impacts identified and document the decision taken. If the decision is made to communicate externally, established procedures are implemented to ensure appropriate communication with warnings and alerts where appropriate. These are available in the Crisis Management Plan and supported by the Communication Plan and templates. Department level outages have identified communication requirements within Department Business Continuity Plans.

A media strategy will be developed as appropriate with the Managing Director (or deputy), or Marketing Manager and team. This will vary depending on the nature of the incident, however, must contain:

Do we need a media strategy?

- Are media at the scene / aware of situation?
- If so, will we need a media spokesperson, where and who?
    - The individuals responsible for speaking to the media are limited to the Crisis Management Team and their deputies.
- Is there a need to hold a press conference? If so, who, when and, where?

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.

The Business Continuity Committee will forward enquiries to the subject matter experts.

To communicate with employees, Managers can utilise:

– Email/Teams/SMS
– Phone numbers available from Access HR
– In the event Access HR is unavailable, data is backed up – see Internal IT Plan.

This would be initiated by the Managing Director and then flow through the Management Hierarchy to ensure speed of messaging.

Procedures are implemented and maintained for:

- detecting and monitoring an incident
- internal communication and receiving, documenting, and responding to communication from interested parties
- receiving, documenting, and responding to any national or regional risk advisory system or equivalent through horizon scanning procedures
- assuring availability of communication systems with contingency systems identified
- facilitating structured communication with emergency responders
- recording of vital information about the incident, actions taken, and decisions made - including alerting interested parties of the disruptive incident
- assuring the interoperability of multiple responding organizations and personnel
- and operation of a communications facility.

These procedures are regularly tested at least annually or upon significant change.

Each plan defines purpose and scope; objectives; activation criteria and procedures; implementation procedures; roles, responsibilities, and authorities; communication requirements and procedures; internal and external interdependencies and interactions; resource requirements; and information flow and documentation process.

Documented procedures are in place to restore and return business activities from the temporary measures adopted to return to business-as-usual.

Exercise and testing

The Business Continuity Committee liaise with the Crisis Management Team to create an exercise and testing schedule appropriate to the business and its objectives.

Business continuity testing takes place through the implementation of an exercising and testing schedule that ensures tests:

a) are consistent with our business continuity objectives
b) are based on appropriate scenarios that are well planned with clearly defined aims and objectives
c) develop teamwork; competence, confidence, and knowledge for those who have roles to perform in relation to disruptions
d) taken together over time validate business continuity strategies and solutions
e) produce formalised post-exercise reports that contain outcomes, recommendations, and actions to implement improvements
f) are reviewed within the context of promoting continual improvement
g) are conducted at planned intervals and when there are significant changes within the organisation or to the environment in which it operates.

Test schedules and requirements are documented with a clear scope, objective and aims, alongside recommendations and identified areas of improvement to strategize and solutions. These reports are shared with the Business Continuity Committee and, where appropriate, the Crisis Management Team. The schedule is maintained within the Internal Audit Schedule, under Business Continuity Tabletop.

Exercise and testing take place in 2 ways:

- Physical tests
  - End to end strategy and solution test carried out and results documented
- Tabletop exercises
  - Discussion based session with key stakeholders of a strategy or solution to discuss roles and responsibilities of a predefined scenario. The format is dependent on the scenario and the impact of a physical test to the business.

Performance Evaluation

Monitoring, measurement, analysis, and evaluation

Phoenix evaluates the business continuity performance and the effectiveness of the BCMS through the Business Continuity Management Reviews.

The company determines:

a) what needs to be monitored and measured, including business continuity processes and controls within management reviews
b) the methods for monitoring, measurement, analysis, and evaluation, as applicable, to ensure valid results
c) when and by whom the monitoring and measuring shall be performed,
d) when and by whom the monitoring and measuring shall be analysed and evaluated.

Phoenix retains appropriate documented information as evidence of the results, as well as evaluation of the BCMS performance and the effectiveness of the BCMS through management reviews, the reporting of internal audit and exercising and testing reports.

Additionally, Phoenix will take action when necessary to address adverse trends or results before a nonconformity occurs and retain relevant documented information as evidence of the results. This will be documented and tracked through the ISO Measurement Log.

The procedures for monitoring performance shall provide for:

a) the setting of performance metrics appropriate to the needs of the organization,
b) monitoring the extent to which the organization's business continuity policy, objectives and targets are met,
c) performance of the processes, procedures and functions that protect its prioritized activities,
d) monitoring compliance with this International Standard and the business continuity objectives,
e) monitoring historical evidence of deficient BCMS' performance, and
f) recording data and results of monitoring and measurement to facilitate subsequent corrective actions

The organisation conducts evaluations of its business continuity procedures to ensure suitability and effectiveness through internal audit, lessons learnt reviews, exercise and testing reports and management reviews.

Significant changes arising shall be reflected in the procedure(s) in a timely manner.

Periodic evaluations of compliance with applicable legal and regulatory requirements, industry best practices, and conformance with the business continuity policy and objectives takes place annually and upon significant changes.

When a disruptive incident occurs and results in the activation of its business continuity procedures, the organization undertakes a post-incident review and records the results within the ISO Measurement Log.

Internal Audit

Phoenix conducts internal audits at planned intervals within the Internal Audit Schedule to provide information on whether the BCMS conforms to the company's own requirements for its BCMS and the requirements of the Standard; and is effectively implemented and maintained. These reports are communicated back to the Business Continuity Committee and to the Crisis Management Team as appropriate.

Phoenix:

a) plans, establishes, implements, and maintains an audit programme, including the frequency, methods, responsibilities, planning requirements and reporting which takes into consideration the importance of the processes concerned and the results of previous audits
b) defines the audit criteria and scope for each audit
c) selects auditors and conducts audits that ensure objectivity and the impartiality of the audit process
d) ensures that the results of the audits are reported to the relevant management
e) retains documented information as evidence of the audit programme and the audit results

This is documented in the Internal Audit Policy.

Management Review

The Business Continuity Committee and the Board reviews the company's BCMS at least annually to ensure its continuing suitability, adequacy, and effectiveness. Business Continuity Committee reviews take place alongside Board performance reviews.

This forms the basis of the Business Continuity Management Review and includes consideration of:

a) the status of actions from previous management reviews
b) changes in external and internal issues that are relevant to the BCMS
c) Information on the BCMS performance, including trends in:
    1) nonconformities and corrective actions
    2) monitoring and measurement results
    3) audit results
d) Feedback from interested parties
e) The need for changes in the BCMS, including policy and objectives
f) Procedures and resources that could be used in the organisation to improve the BCMS' performance and effectiveness
g) Information from the business impact analysis and risk assessment
h) Output from the evaluation of business continuity documentation and capabilities
i) Risks or issues not adequately addressed in any previous risk assessment
j) Lessons learned and actions arising from near-misses and disruptions
k) Opportunities for improvement

The outputs of the management review include decisions related to scope variations; continual improvement opportunities and effectiveness; risk, business impact analysis, plans and procedure updates; updates to legal and contractual obligations; business and operational requirements; resource needs; funding requirements and any need for changes to the BCMS.

The company retains documented information as evidence of the results of management reviews.

The agenda and documentation are put together by The Business Continuity Committee prior to the review.

Results from the Business Continuity Management Review are stored on SharePoint.

Improvement

Non-conformity and corrective action

When a non-conformity occurs, Phoenix:

a) reacts to the nonconformity and as applicable:
    1) take action to control and correct it
    2) deal with the consequences
b) evaluate the need for action to eliminate the cause(s) of nonconformity, in order that it does not reoccur or occur elsewhere, by:
    1) reviewing the nonconformity
    2) determining the causes of the nonconformity
    3) determining if similar nonconformities exist or could potentially occur
c) implement any action needed
d) review the effectiveness of any corrective action taken
e) make changes to the BCMS, if necessary

Corrective actions shall be appropriate to the effects of the non-conformities encountered.

This is documented within PHX004 Corrective Preventative Action Process.

Phoenix retains documented information as evidence of:

a) the nature of the nonconformities and any subsequent actions taken
b) the results of any corrective action

Continual Improvement

The company continually improves the suitability, adequacy, and effectiveness of the BCMS.

Continual Improvement is reviewed as part of the Business Continuity Management Review. Phoenix strives for continual improvement through the maturity of the Business Continuity management system.

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
Amy Trimble	6.0	15/11/2019	Suppliers
Amy Trimble	7.0	20/01/2020	Added Service Continuity Management
Shaun Tosler	8.0	05/09/2021	Environmental Incident update
Amy Trimble	9.0	17/03/2022	IT Environment Update, Change of Job Titles, and Update Document Distribution
BCC	10.0	11/10/2022	Restructure of plan to adhere to ISO 22301 best practices
BCC	10.1	19/12/2022	Added policy sign-off to OD role responsibilities
BCC	10.2	25/04/2023	Amended Governance Manager and added competencies matrix
BCC	10.3	27/06/2023	Amended Roles/Responsibilities, Business Operations Manager job title
Geoff McGann	10.4	20/07/2023	Reviewed Interested Parties
Clare Metcalfe	10.5	09/08/2023	Updated Governance Manager details

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	11/10/2022	Operations Director
Clare Metcalfe	10.1	19/12/2022	Operations Director
Clare Metcalfe	10.2	25/04/2023	Operations Director
Clare Metcalfe	10.3	28/06/2023	Operations Director
Clare Metcalfe	10.4	20/07/2023	Operations Director
Clare Metcalfe	10.5	09/08/2023	Operations Director

Signed: Clare Metcalfe Clare Metcalfe, Operations Director

Dated: 09/08/2023