University Hospitals of Leicester NHS
NHS Trust

Business Continuity Management Policy

Approved By:	Policy and Guideline Committee
Date of Original Approval:	18 January 2012
Trust Reference:	**B1/2013**
Version:	6.0
Supersedes:	5.0 May 2022
Trust Lead:	Mo Patel, EPRR Manager
Board Director Lead:	Jon Melbourne, Chief Operating Officer
Date of Latest Approval	19 September 2024 – Non-Clinical Policy and Guideline Committee
Next Review Date:	September 2029

CONTENTS

Table of Amendments

Version	Date	Amendment Details
6.0	July 2024	Review of document in conjunction with updated NHSE Business Continuity Guidance and Documentation. New Elements: Appendix D and E. Updates to the general format, document grammar, additional detail to Supplier and Contractor Business Continuity Plans and combining of Training sections.
5.0	Apr 2022	Added new elements: • Roles & Responsibilities of the EIM&T Board (to support the development of IT System Application Business Continuity Plans) – EIM&T Board subsequently has been updated to the Digital Governance Board. • Roles & Responsibilities of Clinical IT Facilitators (to help embed Business Continuity across the Trust) • How the Trust will develop its IT System Application Business Continuity Plans (how the Trust will work towards developing contingency arrangements in the event of IT system failures) • How the Trust will develop procedure sheets to support response procedures impacting critical infrastructure Updates to: • Roles & Responsibilities of the EPRR Board

		• Detail behind the elements captured within the Business Continuity Toolkit (i.e. Business Impact Analysis, Risk Assessment & Localised Action Cards) • The frequency and method of updating the localised Business Continuity Toolkits (i.e. Toolkits to be reviewed annually by Business Continuity Leads. This is supported by off the shelf table-top exercises developed by the EPRR Team).
4.0	July 2019	Tweaks to Section 5.0, Policy Implementation & Associated Documents
3.0	Apr 2019	Full policy rewrite
2.0	Jan 2013	New policy
1.0	Dec 2012	New policy (Draft)

Key Words

Business Continuity, Business Impact Analysis, Risk, Risk Assessment, Disaster Recovery

DEFINITIONS & ABBREVIATIONS

Acronym	Description
AEO	Accountable Emergency Officer
BC	Business Continuity
BCM	Business Continuity Management
BCMS	Business Continuity Management System
BCP	Business Continuity Plan
BIA	Business Impact Analysis
CCA	Civil Contingencies Act (2004)
CEO	Chief Executive Officer
CMG	Clinical Management Group
COO	Chief Operating Officer
CPD	Continuous Professional Development
CRR	Community Risk Register
DR	Disaster Recovery
EPRR	Emergency Preparedness, Resilience and Response
ICC	Incident Coordination Centre
IM&T	Information Management and Technology
ITDR	Information Technology Disaster Recovery
KPI	Key Performance Indicators
LLR	Leicester, Leicestershire and Rutland
LRF	Local Resilience Forum
MI	Major Incident
MTPAS	Mobile Telecommunications Privileged Access Scheme
MTPD	Maximum Tolerable Period of Disruption
NHS	National Health Service
NHSE	National Health Service England
NRA	National Risk Assessment
NRR	National Risk Register
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SCG	Strategic Coordinating Group
Sitrep	Situation Report
TCG	Tactical Coordinating Group
TNA	Training Needs Analysis
UHL	University Hospitals of Leicester
AEO	Accountable Emergency Officer
BC	Business Continuity
BCM	Business Continuity Management
BCMS	Business Continuity Management System
BCP	Business Continuity Plan
BIA	Business Impact Analysis
CCA	Civil Contingencies Act (2004)
CEO	Chief Executive Officer
CMG	Clinical Management Group
COO	Chief Operating Officer
CPD	Continuous Professional Development
CRR	Community Risk Register
DR	Disaster Recovery
EIM&T	Executive Information Management & Technology Board
EPRR	Emergency Preparedness, Resilience and Response
ICC	Incident Coordination Centre
IM&T	Information Management and Technology
ITDR	Information Technology Disaster Recovery

KPI	Key Performance Indicators
LLR	Leicester, Leicestershire and Rutland
LRF	Local Resilience Forum
MI	Major Incident
MTPAS	Mobile Telecommunications Privileged Access Scheme
MTPD	Maximum Tolerable Period of Disruption
NHS	National Health Service
NHSE	National Health Service England
NRA	National Risk Assessment
NRR	National Risk Register
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SCG	Strategic Coordinating Group
Sitrep	Situation Report
TCG	Tactical Coordinating Group
TNA	Training Needs Analysis
UHL	University Hospitals of Leicester

Primary Term	Definition
Activity	Process or set of processes undertaken by an organisation (or on its behalf) that produces or supports one or more products and services
Business Continuity	Capability of the organisation to continue delivery of products or services at acceptable predefined levels following disruptive incident
Business Continuity Incident	A business continuity incident is an event or occurrence that disrupts, or might disrupt, an organisation’s normal service delivery, below acceptable predefined levels, where special arrangements are required to be implemented until services can return to an acceptable level. (This could be a surge in demand requiring resources to be temporarily redeployed).
Business Continuity Management System	Part of the overall management system that establishes, implements, operates, monitors, reviews, maintains and improves business continuity
Business Continuity Plan	Documented procedures that guide organisations to respond, recover, resume, and restore to a pre-defined level of operation following disruption
Business Continuity Programme	On-going management and governance process supported by top management and appropriately resourced to implement and maintain business continuity management
Business Impact Analysis	The process of analysing functional areas and the effect that a disruption might have upon them
Civil Contingencies Act (2004)	Act of 2004 which established a single framework for Civil Protection in the United Kingdom. Part 1 of the Act establishes a clear set of roles and responsibilities for Local Responders; Part 2 of the Act establishes emergency powers
Community Risk Register	A register communicating the assessment of risks within a Local Resilience Area which is developed and published as a basis for informing local communities and directing civil protection work streams.
Critical Function	A service or operation the continuity of which a Category 1 responder needs to ensure, in order to meet its business objectives and/or deliver essential services.
Critical Incident	A critical incident is any localised incident where the level of disruption results in the organisation temporarily or permanently losing its ability to deliver critical services, patients may have been harmed or the environment is not safe requiring special measures and support from other agencies, to restore normal operating functions.

Disaster	Emergency (usually but not exclusively of natural causes) causing, or threatening to cause, widespread and serious disruption to community life through death, injury, and/or damage to property and/or the environment.
Disaster Recovery	An organisations ability to restore access and functionality to IT infrastructure after a disaster event.
Emergency	An event or situation which threatens serious damage to human welfare in a place in the UK, the environment of a place in the UK, or the security of the UK or of a place in the UK.
Emergency Plan	A document or collection of documents that sets out the overall framework for the initiation, management, co-ordination and control of personnel and assets to reduce, control or mitigate the effects of an emergency.
Emergency Planning	Aspect of Integrated Emergency Management concerned with developing and maintaining procedures to prevent emergencies and to mitigate the impact when they occur.
Emergency Preparedness	The extent to which emergency planning enables the effective and efficient prevention, reduction, control and mitigation of, and response to emergencies.
Exercise	A simulation designed to validate organisations' capability to manage incidents and emergencies. Specifically exercises seek to validate training undertaken and the procedures and systems within emergency or business continuity plans.
Exercise Programme	Planned series of exercises developed by an organisation or group of organisations to validate training and plans.
Harm	Nature and extent of physical injury (including loss of life) or psychological or economic damage to an individual, community, or organisation.
Hazard	Accidental or naturally occurring (i.e., non-malicious) event or situation with the potential to cause death or physical or psychological harm, damage or losses to property, and/or disruption to the environment and/or to economic, social and political structures.
Incident	Event or situation that requires a response from the emergency services or other responders
Incident Coordination Centre	Operations centre from which the management and co-ordination of the response by each emergency service to an emergency are carried out.
Likelihood	Chance of something happening, whether defined, measured or estimated objectively or subjectively, or in terms of general descriptors (such as rare, unlikely, and almost certain), frequencies or mathematical probabilities.
Local Resilience Forum	Process for bringing together all the category 1 and 2 responders within a police force area for the purpose of facilitating co-operation in fulfilment of their duties under the Civil Contingencies Act
Major Incident	A major incident is any occurrence that presents serious threat to the health of the community or causes such numbers or types of casualties, as to require special arrangements to be implemented.
Maximum Tolerable Period of Disruption	The time it would take for adverse impacts, which might arise as a result of not providing a service or performing an activity, to become unacceptable. The recovery time objective (RTO) has to be less than the maximum tolerable period of disruption.
Mobile Telecommunications Privileged Access Scheme	Scheme that provides call preference for key emergency management organisations if public network access is restricted
Multi-Agency	Involving the participation of several agencies

Mutual Aid	An agreement between Category 1 and 2 responders and other organisations not covered by the Act, within the same sector or across sectors and across boundaries, to provide assistance with additional resource during an emergency.
National Risk Assessment	The full and classified assessment of the likelihood and potential impact of a range of different risks that might directly affect the UK.
National Risk Register	A publically available statement of the assessment of the likelihood and potential impact of a range of different risks that might directly affect the UK.
Operational	The level (below tactical level) at which the management of 'hands-on' work is undertaken at the incident site(s) or associated areas, equating for single agencies to operational level.
Preparedness	Process of preparing to deal with known risks and unforeseen events or situations that have the potential to result in an emergency.
Recovery	The process of rebuilding, restoring and rehabilitating the community following an emergency.
Recovery Phase	Phase focussed on recovery, commencing at the earliest opportunity following the onset of an emergency, and running in tandem with the response phase.
Recovery Point Objective	The point to which information used by an activity must be restored to enable the activity to operate on resumption. Can also be referred to as "maximum data loss." The RTO is expressed in a unit of time.
Recovery Time Objective	The period of time following an incident within which an activity must be resumed or resources must be recovered in order to avoid unacceptable consequences. The RTO is expressed in a unit of time and must be less than the identified Maximum Tolerable Period of Disruption.
Resilience	Ability of the community, services, area or infrastructure to detect, prevents, and, if necessary to withstand, handle and recover from disruptive challenges.
Response	Decisions and actions taken in accordance with the strategic, tactical and operational objectives defined by emergency responders. At a high level these are to protect life, contain and mitigate the impacts of the emergency and create the conditions for a return to normality.
Response Phase	Phase in which decision making and actions are focused on response to an actual emergency or disaster.
Risk	Measure of the significance of a potential emergency in terms of its assessed likelihood and impact.
Risk Assessment	A structured and auditable process of identifying potentially significant events, assessing their likelihood and impacts, and then combining these to provide an overall assessment of risk, as a basis for further decisions and action.
Risk Management	All activities and structures directed towards the effective assessment and management of risks and their potential adverse impacts.
Risk Treatment	Process of determining those risks that should be controlled (by reducing their likelihood and/or putting impact mitigation measures in place) and those that can be tolerated at their currently assessed level.
Service Interruption	Any disruptive challenge that threatens personnel, buildings or the operational procedures of an organisation and which requires special measures to be taken to restore normal operating functions which could be short, medium or long term.
Situation Report	Report produced by an officer or body, outlining the current state and potential development of an incident and the response to it.
Situational Awareness	The state of individual and/or collective knowledge relating to past and current events, their implications and potential future developments.
Statutory	Prescribed in legislation.

Statutory Guidance	Advice provided by or to an authority under statutory powers concerning the implementation of or compliance with a specific law.
Strategic	The level (above tactical level and operational level) at which policy, strategy and the overall response framework are established and managed.
Strategic Coordinating Group	Multi-agency body responsible for co-ordinating the joint response to an emergency at the local strategic level.
Tactical Coordinating Group	A multi-agency group of tactical commanders that meets to determine, co-ordinate and deliver the tactical response to an emergency.
Tactical	Level (below strategic level and above operational level) at which the response to an emergency is managed.

1. Introduction And Overview

1.1.1 University Hospitals of Leicester (UHL) (hereby referred to as the ‘Trust’) is a Category 1 responder outlined in the Civil Contingencies Act (CCA, 2004), and subsequently upholds the responsibility and requirement to deliver an effective Business Continuity Management System (BCMS) in order to continue service provision for patients. The Trust achieves this through aligning its practices with ISO 22301 ‘Societal Security – Business Continuity Management Systems – Requirements’.

1.1.2 This policy provides an overview of how the Trust embeds BCMS specifically in reference to establishing, implementing, operating, monitoring, reviewing, maintaining and continuously improving its business continuity.

1.2 Business Continuity Policy Statement

1.2.1 ISO 22301 makes clear that a “key component of establishing a BCMS is the creation of a suitable policy statement, indicating the intention and commitment of the organisation in embedding business continuity”. The Trust’s business continuity policy statement is:

“University Hospitals of Leicester NHS Trust is fully committed to creating, maintaining and improving a robust business continuity management system, so to ensure the continuation of its critical and essential functions at all times”.

2. Policy Scope

2.1.1 ISO 22301 states that a BCMS has five key components:

- A policy;
- People with defined responsibilities;
- Management processes relating to:
    - policy,
    - planning,
    - implementation and operation,
    - performance assessment,
    - management review, and
    - improvement;
- Documentation providing auditable evidence; and
- Any business continuity management processes relevant to the Trust.

2.1.2 This policy describes each of the above five key components in the context of the “Plan-Do-Check-Act” model which ISO 22301 applies to establishing, implementing, operating, monitoring, reviewing, maintaining and improving the effectiveness of an organisation’s BCMS:

UHL Business Continuity Management System (BCMS)	
Establish (Plan)	Context for the BCMS Scope of the BCMS BCMS Leadership BCMS Roles and Responsibilities

	BCMS Resources Business Continuity Policy Statement Business Continuity Objectives Risk Assessment Business Impact Analysis Business Continuity Plans BCMS Documented Information
Implement and Operate (Do)	Training Workshops Business Continuity Toolkit
Monitor and Review (Check)	Exercising Internal Audit
Maintain and Improve (Act)	Learning from Incidents Review

2.1.3 The aim of this policy is to ensure the Trust has in place a robust business continuity management system, so to ensure any disruption to the Trust's activities are kept to within predefined tolerable levels.

2.1.4 The objectives of this policy are to:

- Establish the key terms and definitions relating to business continuity management;
- Identify the key roles and responsibilities that supports the Trust in embedding its business continuity management system;
- Set out how the Trust embeds its business continuity management system;
- Align the Trust's business continuity management system with:
    - ISO:22301 Societal Security – Business Continuity Management Systems – Requirements;
    - ISO 22313 Societal Security – Business Continuity Management Systems – Guidance on the use of ISO 22301;
    - ISO 27001 - International Standard for information security management systems (ISMS);
    - NHS England Business Continuity Management Toolkit (2023); and
    - Business Continuity Institute's Good Practice Guidelines (2023).

2.1.5 This policy is supported by and should be read in conjunction with the Trust's Emergency Preparedness, Resilience and Response (EPRR) Policy (B25/2018).

2.1.6 While this policy references disaster recovery planning, it is not included within the scope of this policy. Details of how the Trust manages disaster recovery can be found in the IM&T Business Continuity and Disaster Recovery Plan (Appendix C: BCMS Supporting Documentation).

2.1.7 This policy is applicable to all Trust staff, inclusive of temporary and agency staff, those with honorary contracts, students, and staff of contractors or other service providers whom are contracted to work by the Trust.

3. Definitions and Abbreviations

3.1.1 All definitions and abbreviations used in this policy, and all EPRR documentation, are based on the UK Civil Protection Lexicon which can be accessed online at https://www.gov.uk/government/publications/emergency-responder-interoperability-lexicon.

4. Roles and Responsibilities

4.1 Chief Executive Officer (CEO)

4.1.1 The CEO is responsible for ensuring the Trust meets its legal and statutory obligations to have in place business continuity plans and arrangements, and appoints an Executive Board Director as the Accountable Emergency Officer.

4.2 Accountable Emergency Officer (AEO)

4.2.1 The role of the AEO is assigned to the Chief Operating Officer (COO) who is a member of the Trust's Executive Board of Directors and is responsible for:

a) Ensuring the Trust develops and maintains a robust BCMS, while promoting the culture of business continuity within the Trust;
b) Appointing a nominated lead for the implementation of business continuity plans;
c) Ensuring that the Trust is properly prepared and resourced for managing a disruptive incident or an emergency;
d) Ensuring that the Trust, and any sub-contractors, are compliant with the EPRR requirements as set out in the CCA (2004), the NHS Act (2006 and as amended) and the NHS Standard Contract, including the NHS England EPRR Framework and the NHS England Core Standards for EPRR; and
e) Ensuring that the Trust, any of its commissioned providers and any subcontractors all have robust business continuity planning arrangements in place which are aligned to ISO 22301 or subsequent guidance which may supersede this.

4.3 Executive Directors

4.3.1 All Executive Directors demonstrate clear leadership with respect to establishing, implementing, operating, monitoring, reviewing, maintaining and improving the Trust's business continuity management system. In accordance with ISO 22301, strong leadership with respect to the Trust's BCMS can be provided by:

- Ensuring that policies and objectives are established for the BCMS and are compatible with the Trust's strategic direction and this is being integrated into the Trust's business processes;
- Ensuring resources needed for the BCMS are made available;
- Communicating to staff the importance of effective business continuity management and conforming to the BCMS requirements;
- Directing and supporting staff to contribute to the effectiveness of the BCMS;
- Promoting continual improvement; and

- Supporting other relevant management roles to demonstrate their leadership and commitment as it applies to their areas of responsibility.

4.4 Emergency Preparedness, Resilience and Response (EPRR) Board

4.4.1 The EPRR Board, whom meet quarterly, receive compliance reports against the Trust's BCMS at each meeting. This includes updates for each Clinical Management Group (CMG) / Corporate Directorate regarding:

- The number of Business Continuity Toolkit meetings completed;
- The number of booked Business Continuity Toolkit meetings that are planned to be completed over the next quarter; and

4.4.2 Where non-compliance is identified, the Chair of the EPRR Board tasks its relevant members to ensure a plan is in place to achieve compliance within an agreed timeframe.

4.5 Digital Governance Board

4.5.1 The Digital Governance Board receives compliance reports against the Trust's 'IM&T System Applications' spreadsheet at each meeting. This includes:

- An update on the criticality, functionality, scale of use and contingencies currently in place for IT systems listed within the Business Continuity Toolkits; and
- An update on the number of Trust IT System Application Business Continuity Plans completed.

4.5.2 The Digital Governance Board utilises the IM&T System Applications spreadsheet to prioritise the development of IT system applications.

4.5.3 Where non-compliance are identified, the Chair of the Digital Governance Board tasks its relevant members to ensure a plan is implemented to achieve compliance within an agreed timeframe, and these are recorded on the Trust's risk register until resolved.

4.6 EPRR Team

4.6.1 The EPRR Team leads the implementation of the Business Continuity Policy, by:

- reviewing and updating the policy no less frequently than three yearly to ensure it remains fit for purpose;
- reviewing and updating the Trust's Business Continuity Plan on an annual basis;
- developing and rolling out the Trust's Business Continuity Toolkits to all services and departments so service-level business impact analyses, risks assessments and business continuity plans can be developed.
- collating information captured through local services Business Continuity Toolkits to create business impact analyses specific for each respective Clinical Management Group (CMG), directorate specialities and for the Trust as a whole;

- collating information around the use of IM&T System Applications, to help guide the development of IM&T System Application Business Continuity plans;
- supporting services and departments to test and exercise their local Business Continuity Toolkits by proving at least one exercise scenario annually;
- monitoring compliance against this policy and the BCMS through providing reports to the EPRR Board; and
- monitoring compliance against this policy and the IM&T System Applications spreadsheet through providing reports to the Digital Governance Board.

4.7 CMG Heads of Operations and Corporate Directors

4.7.1 CMG Heads of Operations and Corporate Directors are the Strategic Business Continuity Lead for their respective CMG / Corporate Directorate. They are responsible for scoping out the rollout of Business Continuity Toolkits within their respective remit, and nominating a Business Continuity Lead for every identified service and department.

4.8 Business Continuity Leads

4.8.1 Business Continuity Leads establish, implement, operate, monitor, review, maintain and improve a business continuity toolkit for each service/department that they are the assigned Lead for, through:

- Meeting with the EPRR Team to complete a localised Business Continuity Toolkit. Inclusive of the development of a Business Impact Analysis (BIA) and Risk Assessment;
- Developing action cards as part of the Business Continuity Toolkit to provide local service specific actions in response to disruptive events with high localised risk scorings;
- Familiarising and informing staff members of the relevant Business Continuity Toolkit, and ensuring it is readily available;
- Reviewing and updating the Toolkit annually;
- Ensuring any relevant completed IT System Application Business Continuity Plans are made available to the service/department; and
- Coordinating and delivering tests and exercises of their business continuity plans.

4.9 IT System Application Owners

4.9.1 IT System Application Owners coordinate the development of their respective IT system applications' business continuity plan in line with Section 5.10.8 – 5.10.12 of this policy.

4.10 Clinical IT Facilitators

4.10.1 The Clinical IT Facilitators complete a monthly audit to check IT business continuity documentation is present. They ensure these are readily available within the department, and ask a randomly selected staff member if they are aware of the location and functionality of these plans.

4.10.2 These staff members also test the functionality of any computing devices which have been allocated to support business continuity (major incident devices). This ensures these devices have been set up correctly and staff members in the area are aware of how and when to utilise them.

4.11 Information Management & Technology (IM&T)

4.11.1 IM&T have in place Disaster Recovery (DR) plans to ensure any disruption is kept within pre-defined tolerable limits. The DR plans are reviewed every three years, alongside the latest 'Trust IM&T System Applications' sheet see Section 5.10.8 for further details).

4.11.2 To inform the Trust's IM&T System Applications sheet, IM&T provide the most up-to-date list of the Trust's IT System Applications, their priority order according to their Disaster Recovery run-book and the relevant service owner.

4.11.3 To further support the Trust, in the event of a high severity incident priority 1 / 2 alerts for unplanned IT system downtime and are issued out by IM&T for those registered to the alerting service. Alerts provide information about the affected systems, the impact to the Trust, when updates are received and when the issue has been resolved. It is the responsibility of Services / Departments and Staff to ensure relevant personnel are registered to the IT System Alerts. *(For further information regarding IT priority incidents please refer to the IM&T Disaster Recovery Plan).*

4.12 All Staff

4.12.1 All staff must ensure they are aware of what is expected of them in the event of a business continuity incident. This includes escalating any Business Continuity events to their local Business Continuity Lead (typically a General or Service Manager for their department). Staff, who may be assigned a role-specific action card, must also ensure they have read and are familiar with the Trust's Incident Response Plan, Business Continuity Plan and relevant localised business continuity toolkit(s).

4.12.2 The Trust-wide Business Continuity Plan can be found on UHL Connect, via: https://uhlconnect.uhl-tr.nhs.uk/site/565de1a1-092a-434d-a809-33dd514ecbb0/page/00f6f131-e0cf-4345-9c2f-bdc1ed6fe472

4.12.3 Localised Business Continuity Toolkits can be found electronically on the UHL Business Continuity Sharepoint, via: https://uhltrnhsuk.sharepoint.com/sites/BusinessContinuity/Shared%20Documents/Forms/AllItems.aspx

5. POLICY IMPLEMENTATION AND ASSOCIATED DOCUMENTS

5.1 Context for the BCMS

5.1.1 The Trust is one of the biggest in the country, serving the one million residents of Leicester, Leicestershire and Rutland (LLR) and increasingly specialist services over a much wider area. Patients (and their friends, family, neighbours and colleagues) rely on the Trust to provide them with care and treatment when they require a range of different services, irrespective of any disruptive challenges. Hence, the Trust has in place plans to deliver critical and essential functions during any disruptive event.

5.1.2 The Trust's BCMS is aligned to the following standards, legislation and best practice:

- Civil Contingencies Act (2004);
- Health & Social Care Act (2012);
- NHS England's Emergency Preparedness, Resilience & Response (EPRR) Framework;
- Business Continuity Institute's Good Practice Guidelines (2023);
- NHS England's Business Continuity Management Toolkit (2023);
- NHS England Core Standards for Emergency Preparedness, Resilience and Response (EPRR); and
- ISO 22301 Societal Security – Business Continuity Management Systems (BCMS) Requirements.

5.2 Scope of the BCMS

5.2.1 The scope of the Trust's BCMS applies to the entirety of the Trust, for all services and departments in each of the Trust's CMGs and Corporate Directorates and any externally contracted providers.

5.3 BCMS Leadership

5.3.1 The Trust's AEO (assumed by the COO), provide the overall Trust leadership to ensure BCMS is embedded in alignment with the standards prescribed in Section 5.1.2, with wider support from the Trust's Board Executive and Non-Executive Directors.

5.4 BCMS Roles and Responsibilities

5.4.1 Embedding BCMS effectively into the Trust requires input from a wide range of staff at UHL. Clear roles and responsibilities have been established in Section 4.0 of this policy.

5.5 BCMS Resources

5.5.1 To effectively deliver the Trust's BCMS, the following resources are allocated:

- People Services: The time of identified Business Continuity Leads (General or Service Managers) to support establishing and implementing the Business Continuity Toolkits;

- Finance: Considering financial requirements to support the resolution of risks identified to key processes. If deemed appropriate, this may require funding from pre-existing budgets or capital funding; and

- Estates & Facilities, IM&T and Procurement & Supplies: Reviewing equipment and infrastructure required in association with key activities or processes.

5.6 Business Continuity Objectives

5.6.1 The Trust's business continuity objectives are to:

- Comply with the CCA (2004)) and NHS England's core standards for EPRR and other relevant legislation / standards;
- Identify, assess and manage risks which may lead to a disruption to the Trust's activities and undertake a Corporate BIA;
- Exercise and test Business Continuity Plans in place to ensure disruption can be kept within pre-defined tolerable limits;
- Identify the location of critical data and assets; and
- Inform IM&T's disaster recovery planning.

5.7 Risk Assessment

5.7.1 As part of the Business Continuity Toolkit, all services and departments complete a risk assessment, which are completed in line with the Trust's risk management policy (see Appendix C 'BCMS Supporting Documentation').

5.7.2 In assessing risks, Business Continuity Leads should consider and refer to the following sources of information:

- Existing Trust risk registers;
- Incident history (for the service/department, the CMG, the Trust and the local area);
- LLR community risk register.

5.7.3 Based on the outcomes of the business disruption risk assessment, strategies need to be devised for all risks identified from very high to low scores, based on the following framework:

- **Mitigation:** identifying strategies, activities, modifications or controls aimed at reducing the risk likelihood and/or consequence;
- **Acceptance**: ensuring the risk is owned at the appropriate level (normally director level) within the organisation;
- **Transferring**: changing an activity, ceasing an activity, outsourcing the activity or transferring the risk (if financial, by means of insurance);
- **Eliminating**: if possible by removing the cause, avoiding the risk or introducing preventative measures;
- **Recovery:** developing and testing recovery plans to deal with any threats and hazards identified.

5.7.4 As part of the business disruption risk assessment process, all services and departments should give consideration to the risks listed in Appendix B 'List of Business Disruption Risks for Consideration by Services and Departments'.

5.8 Business Impact Analysis (BIA)

5.8.1 ISO 22313 defines a BIA as the "process of analysing activities and the effect that business disruptions might have upon them." The BIA identifies, quantifies and qualifies the impacts and their effects of a loss, interruption or disruption and measures the impact of disruptions to its processes on the organisation. It provides information that underpins later decisions about business continuity strategies.

5.8.2 All services and departments complete a BIA for their own activities, which form part of their Business Continuity Toolkit. This process is completed by the service's/department's nominated Business Continuity Lead and involves the following:

- Identifying the key activities being undertaken;
- Understanding the impact if those activities were to be ceased;
- Understanding how long the organisation can cope with a disruption to those activities, through clarifying the maximum tolerable period of disruption (MTPD), as illustrated below:

Activity Criticality	
Tier	**MTPD**
Tier 1	Less than 4 hours
Tier 2	Between 4 – 12 hours
Tier 3	Between 12 – 24 hours
Tier 4	Between 24 – 72 hours
Tier 5	Between 72 hours – 1 week
Tier 6	Greater than 1 week

- Determining the minimum resources required to perform the activities at a minimum; and
- Identifying all internal and external dependencies relevant to each activity.

5.8.3 Through the BIA the Trust:

- Informs services and departments of the potential impacts from a disruptive incident;
- Informs services and departments what needs to be prioritised during a disruption, and what resources they require to restore / maintain it;
- Quantifies the maximum tolerable period of disruption for each process – the timeframe during which a recovery must become effective before an outage compromises the ability of the Trust to achieve its business objectives in light of contractual, regulatory and statutory requirements;
- Obtains information which can be collated at a CMG / Directorate / Trust-wide level to provide Tactical and Strategic commanders focus and strategy in the response to a disruption;
- Obtains information that can inform the Trust's wider resilience strategies on IM&T and Procurement & Supplies.

5.9 Business Continuity Plans

Introduction

5.9.1 Business Continuity Plans are documented procedures that guide organisations to respond, recover, , and restore activities to a pre-defined level of operation following a disruption. To achieve its Business Continuity objectives, the Trust embeds the following plans:

- Corporate Business Continuity Plan;
- Local-level Business Continuity Toolkits;
- IM&T Disaster Recovery Plans; and
- IT System Application Business Continuity Plans;
- Estates & Facilities Procedure Sheets;
- Supplier and Contractor Business Continuity Plans.

Corporate Business Continuity Plan

5.9.2 A single Corporate Business Continuity Plan describes the generic business continuity response arrangements for key business disruption risks identified as part of the business disruption risk assessment. This is maintained by the EPRR Team in conjunction with key stakeholders.

Business Continuity Toolkits

5.9.3 Business Continuity Toolkits are for every service and department across the CMG and Directorate Specialities. They are specific to each service and department and are completed by the nominated Business Continuity Lead, with support from the EPRR Team.

5.9.4 Toolkits describe detailed business continuity response arrangements for key business disruption risks identified as part of local business disruption risk assessments.

5.9.5 Toolkits may take direction from the Corporate Business Continuity Plan to ensure local arrangements are commensurate with the Trust's wider business continuity plan. This is achieved through the development of:

- BIA (see further detail in Section 5.9);
    - This supports services in identifying the importance of each of their activities, and the minimum resources required to maintain or recover them during / following disruptive incidents.
- Risk Assessment (see further detail in Section 5.8);
    - This supports services and departments in identifying the likelihood and the consequence of a number of pre-identified business continuity risks from occurring;
    - This is implemented following the same methodology as the Trust's Risk Management Policy (A12/2002);
    - Risks scored at 15 or higher are placed on the corporate risk register.
- Localised Business Continuity Action Cards.
    - The services utilise the Risk Assessment to develop localised business continuity action cards (above the generic actions included within the Business Continuity Plan), where risks with higher scorings pose a greater threat to their activities.

IM&T Disaster Recovery Plans

5.9.6 The IM&T DR Plan focuses on restoring systems within pre-defined tolerable limits. The plan is updated no less frequently than annually, and provides reliable planning assumptions on how long it may take to recover each IT System Application following a period of downtime.

5.9.7 IM&T use the information submitted by Business Continuity Leads on the "Trust's IM&T System Applications" spread sheet to inform their disaster recovery planning objectives. IM&T also support in populating this spreadsheet by providing application owners.

IT System Application Business Continuity Plans

5.9.8 The IT System Application Business Continuity Plans look at how the Trust can continue its critical activities during an IT outage while awaiting the restoration of those systems, through the delivery of IM&T's Disaster Recovery Plan.

5.9.9 To quantify the importance of each IT System which needs to be utilised during potential down-times, the 'Trust's IM&T System Applications' spread sheet is developed to provide the following information for each system:

- Criticality (based on the reported maximum tolerable period of disruption);
- Functionality;
- Scale of use;
- Contingency plan in case of downtime.

5.9.10 The Trust's IM&T System Applications spread sheet are shared with the Digital Governance Board to help identify IT systems that need to be utilised during disruptive periods and therefore require the development of plans.

5.9.11 Where information available from system applications still needs to be accessed during down-times, the following approach is undertaken to develop business continuity plans:

- Systems utilised by an individual CMG or service/department have the responsibility to develop their IT System Business Continuity Plan;
- Systems utilised Trust-wide or by multiple services across different CMG
- Where an application is utilised Trust-wide or by multiple services across different CMGs, the development of these plans need to be overseen by an identified committee or group who are responsible for supporting the IM&T System Application Owner in developing, implementing and approving any IT System Business Continuity Plans.

5.9.12 The development of IT System Application Business Continuity Plans is overseen by the Digital Governance Board. Once the plans have been created and uploaded onto SharePoint, the Business Continuity Leads are responsible for making relevant plans available for their respective service/department as part of the annual review of the Business Continuity Toolkits.

Estates & Facilities Procedure Sheets

5.9.13 Where appropriate, the Trust has developed procedural sheets for the loss of utilities including power, water, fuel, heating, cooling, gas and medical gases. This provides the technical detail on how Estates and Facilities can prepare for, respond to and recover from Estates and Facilities related disruptions.

5.9.14 The procedure sheets also provide guidance to services and departments on the use of the emergency generators, including the identification of which elements are on the emergency generator and the process to be followed to remove / add elements onto the generator.

Supplier and Contractor Business Continuity Plans

5.9.15 Where appropriate, the Trust reviews existing contracts, develop service level agreements and/or memoranda of understanding which help in monitoring the business continuity arrangements of relevant external service providers and/or contractors.

5.9.16 Business Continuity is paramount in the Trust's mission to provide continued, quality healthcare services. Ensuring that all of the Trust's suppliers are prepared for any potential disruptions is a critical component of the Trust's risk management strategy.

5.9.17 Upon tender of contract the Trust request that Non-NHS Supply Chain providers have in place business continuity arrangements and make available to the Trust, a copy of the Provider's Business Continuity Plan. In the event that a Provider does not have business continuity arrangements or business continuity plans available, the Trust does not progress with the awarding of contract(s) to the Provider.

5.9.18 On an annual basis, the Trust circulates a UHL Business Continuity Audit Survey request to Non-NHS Supply Chain providers to complete, to support the Trust in identifying and mitigating risks, thereby enhancing the collective ability to respond to unforeseen events effectively within the supply chain. The UHL Supplier Business Continuity Audit is available to view in Appendix E.

5.9.19 The Trust's EPRR Team select a random sample group of 10-15 Non-NHS Supply Chain Providers as part of the Survey request to analyse further, working in collaboration with the Procurement and Supplies Department and thereafter, providing findings, advice and recommendations.

5.9.20 NHS Supply Chain providers all agree to the NHS Standard Contract Service Conditions in particular, Service Condition 30 'Emergency Preparedness, Resilience and Response'; outlining definitive conditions the Provider must comply with. Written particulars for The NHS Standard Contract Service Conditions can be viewed via NHS England.

5.9.21 Any Trust NHS Standard Contract Sub Contract Providers are also required to comply with Service Condition 30. The NHS Standard Sub Contract templates are available to view via NHS England.

5.9.22 NHS Standard Contract Providers and NHS Standard Sub Contract Providers are managed by NHS England and therefore are out of scope of the Trust's audit process.

5.10 BCMS Documented Information

5.10.1 The Trust's BCMS incorporate the following documented information:

- EPRR Policy (B25/2018);
- Risk Management Policy (A12/2002);
- Business Continuity Management Policy (B1/2013);
- Corporate Business Continuity Plan;
- Business Continuity Toolkits for each service/department;
- Business Continuity Toolkit Compliance Sheet;
- IM&T System Applications Spreadsheet;
- IM&T Disaster Recovery Plan;
- IT System Application Business Continuity Plans; and
- Estates & Facilities Procedure Sheets.

5.10.2 Full details on the above listed documentation are listed under Appendix C 'BCMS Supporting Documentation'.

5.11 Education and Training

5.11.1 To support the Trust in achieving the aims and objectives of this policy, and effectively embedding the BCMS, the Trust must ensure recognised staff groups are adequately trained. The recognised staff groups with defined education and training needs are stated below. Further details of the training requirements are captured within the EPRR Training and Education Strategy, overseen by the Trust's EPRR Board.

Staff Group	Education and Training Need(s)
EPRR Team Staff Members	Must have relevant knowledge and skills to effectively coordinate the development of the Trust's BCMS, through either possessing a relevant qualification or being able to attend courses as part of their continuing professional development (CPD).
IM&T	The IM&T staff members must have relevant knowledge and skills to effectively coordinate the development and implementation of the Trust's ITDR plan, through either possessing a relevant qualification or being able to attend courses as part of their CPD.
Business Continuity Leads	Following the initial two-hour appointment to develop the Business Continuity Toolkit, the EPRR Team provides a number of documents to support Business Continuity Leads in reviewing, updating and maintaining their localised Business Continuity Toolkit. Further support can be requested from the EPRR Team to: • Update and maintain their Business Continuity Toolkit; • Develop appropriate business continuity related action cards for their service and department; • Deliver local tests and exercises of their local-level business continuity plans.
All Staff	All staff are to be made aware and familiarise themselves with the Trust's Business Continuity Plan and their relevant local Business Continuity Toolkit (which provides service specific procedures), where these plans are available and that they may be used to inform the response strategy to a disruptive incident. This is provided by their respective Business Continuity Lead, and is supplemented by further email communications, tests and exercising of the plans by the EPRR Team. Local Business Continuity Toolkits will be available on Sharepoint via: https://uhltrnhsuk.sharepoint.com/sites/BusinessContinuity/Shared%20Documents/Forms/AllItems.aspx

5.12 Exercising

5.12.1 The full details of exercising requirements are set out within Section 5.12 of the EPRR Policy.

5.12.2 To support embedding BCMS into the Trust, the EPRR Team has developed scenarios to support Business Continuity Leads test and exercise service and departments localised Business Continuity Toolkits annually.

5.12.3 This supports the longer term implementation of the Business Continuity Toolkits within each respective service and department, as the exercises provide opportunities for:

- Business Continuity Leads to test their relevant plans and ensure they are fit for purpose;
- Staff to gain familiarity with the Business Continuity Toolkit and their localised Business Continuity Action Cards;
- Continual learning and development of the Business Continuity Toolkit through reviews and updates.

5.12.4 To further support the Trust in ensuring the continuous improvement of the BCMS, the development of table-top exercises based on loss of utilities and / or other pre-determined business continuity risks to the Trust, enables Business Continuity Leads to review and update (where relevant) local toolkits and business continuity arrangements. Upon completion of table-top exercises, update toolkits are shared with relevant service / department staff to ensure familiarity.

5.13 Internal Audit and Monitoring Compliance

5.13.1 The Trust employs internal auditors to review its BCMS on a regular basis and no less frequently than triennially. Audit outcomes are reported to the EPRR Board and the Audit Committee, with any actions being overseen by the EPRR Board and subsequently incorporated into the EPRR Work Programme.

5.13.2 The IT System Application Business Continuity Plans are audited monthly by the Trust's Clinical IT Facilitators. The Facilitators ensure services and departments have their relevant IT System Application Business Continuity Plans available, and ensure the functionality of the IT Major Incident devices.

5.13.3 The EPRR Team conduct a continual audit process on the Business Continuity Toolkit development and progression, reporting on the Business Continuity Programme Overview (see Appendix D: Business Continuity Programme Overview), on a quarterly basis to the EPRR Board with specific reference to key performance indicators (KPIs)).

5.13.4 Upon the conduction and completion of a Business Continuity Toolkit, in particular a service activity risk assessment; in the event that any risks identified score 15 or more, these risks are escalated and added to the Trust Risk Register for monitoring and mitigation.

5.13.5 The Trust monitors compliance of its BCMS through the maintenance of a structured Business Continuity Programme. This tool is designed to support the establishment, implementation and operation, monitoring and reviewing, and maintenance and continued improvement of the BCMS, in alignment with the "Plan-Do-Check-Act" Model (ISO: 22301).

5.13.6 The Programme provides overview of the Business Continuity Toolkits in detail inclusive of the below key information, an example of the Business Continuity Programme Overview can be seen in Appendix D.

5.13.7 The Business Continuity Programme Overview Tool, through the understanding of Business Continuity Toolkit compliance, also enables the provision of KPIs to be reported to the EPRR Board, thus ensuring an appropriate level of accountability.

5.13.8 KPI's reported on include the number of toolkits completed, the number of toolkits scheduled for completion in the upcoming quarter, and the identification of any areas of non-compliance within any specific CMG / Corporate Directorate.

5.13.9 In the event that any non-compliances and risks identified are reported to the EPRR Board, discussed and appropriate agreed plans implemented to ensure the efficient and effective correction of non-compliances.

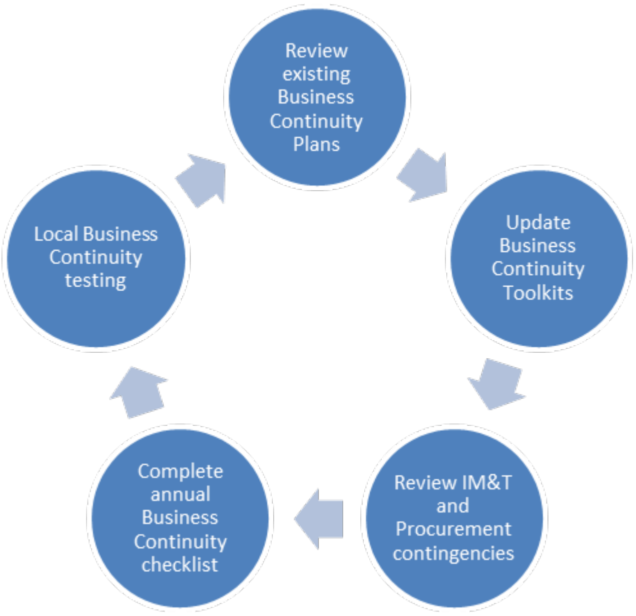
5.14 Learning from Incidents

5.14.1 Identifying and learning lessons from business continuity incidents adhere to the pre-established processes outlined in Section 5.10 of the EPRR Policy.

5.15 Review

5.15.1 As described in ISO 22301, a BCMS emphasises the importance of continual improvement based on objective measurement. To achieve this, the Trust's BCMS documentation is reviewed and updated periodically and in line with the timescales outlined in Appendix C 'BCMS Supporting Documentation'.

5.15.2


Review existing Business Continuity Plans
Update Business Continuity Toolkits
Review IM&T and Procurement contingencies
Complete annual Business Continuity checklist
Local Business Continuity testing

6. Equality Impact Assessment

6.1.1 The Trust is fully committed to being an inclusive employer and opposes all forms of unlawful or unfair discrimination, bullying, harassment and victimisation.

6.1.2 It is the Trust's legal and moral duty to provide equity in employment and service delivery to all and to prevent and act upon any forms of discrimination to all people of protected characteristic: Age, Disability (physical, mental and long-term health conditions), Sex, Gender reassignment, Marriage and Civil Partnership, Sexual orientation, Pregnancy and Maternity, Race (including nationality, ethnicity and colour), Religion or Belief, and beyond.

6.1.3 The Trust is also committed to the principles in respect to improving social deprivation and health inequalities. The Trust's aim is to create an environment where all staff are able to contribute, develop and progress based on their ability, competence and performance. The Trust recognises that some staff may require specific initiatives and/or assistance to progress and develop within the organisation.

6.1.4 The Trust is also committed to delivering services that ensure the Trust's patients are cared for, comfortable and so far as reasonably practicable, meet their individual needs.

7. Supporting References, Evidence Base and Related Policies

7.1.1 This policy was developed in line with the following:

- Civil Contingencies Act (2004);
- Health and Care Act (2022);
- Health & Social Care Act (2012);
- NHS Contract;
- ISO:22301 Societal Security – Business Continuity Management Systems – Requirements;
- ISO 22313 Societal Security – Business Continuity Management Systems – Guidance;
- ISO 27001 - Information Security Management Systems (ISMS);
- Business Continuity Institute's Good Practice Guidelines (2023);
- NHS England's Emergency Preparedness, Resilience and Response (EPRR) Framework;
- NHS England Business Continuity Management Toolkit (2023); and
- NHS England's Core Standards for EPRR.

8. Process for Version Control, Document Archiving and Review

8.1.1 This policy is reviewed every 5 years or more frequently if new or revised national guidance is released. Any review is to be led by the Trust's EPRR Team.

Element to be monitored	Lead	Tool	Frequency	Reporting arrangements
Relevant policies	EPRR Team	EPRR Policy, Business Continuity Policy and Risk Management Policy	Every 5 years	To be reported to the EPRR Board, via the EPRR Annual Report to Trust Board
Corporate Business Continuity Plan	EPRR Team	Corporate Business Continuity Plan up to date and available via UHL Connect	Annually	To be reported to the EPRR Board, via the EPRR Annual Report to Trust Board
Services/departments with a completed and up-to-date Business Continuity Toolkit	Business Continuity Leads	Business Continuity Toolkit Compliance Sheet	Quarterly	Compliance status to be reported to the EPRR Board. This includes: • Number of Business Continuity Toolkits completed • Number of Toolkits scheduled over the next quarter • Any non-conformity identified within any specific CMG / Corporate Directorate.
IT System Applications with a completed and up-to-date Business Continuity Plan	IT System Application Owners	IT System Applications Spreadsheet	Quarterly	Compliance status to be reported to the EPRR Board. This includes: • Critically of IT System Applications utilised • Number of Trust IT System Application Business Continuity Plans completed.
IM&T Disaster Recovery Plan	IM&T	IM&T Disaster Recovery Plan	Annually	To be reported to the EPRR Board, via the EPRR Annual Report to Trust Board
Estates and Facilities Procedure Sheets	Senior Specialist Engineer, Estates & Facilities	Estates & Facilities procedural sheets for loss of utilities including power, water, fuel, heating, cooling, gas and medical gases	Quarterly	To be reported to the EPRR Board

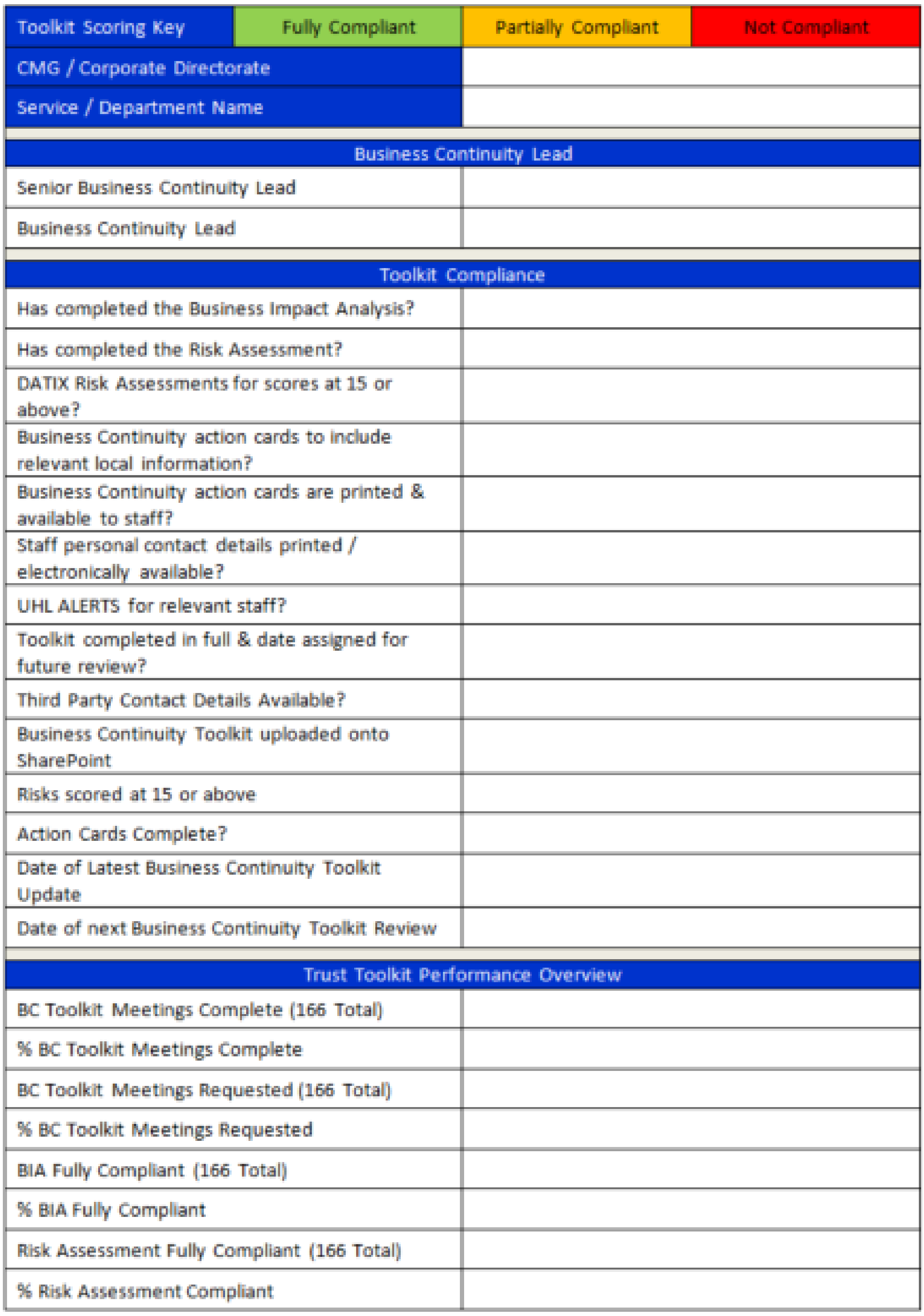
9. Appendix A: List of Business Disruption Risks for Consideration by Services and Departments

Business Continuity Impact	Trigger
Loss of supply chain, including outsources services	Bankruptcy Logistical issues Supply and demand issues Loss of receipt and delivery Payment delays
Loss of equipment	Flooding Outdated equipment No spare parts Maintenance failure Human error Power surge or loss of power
Loss of Information Management & Technology (IM&T)	Cyber attack Data theft Equipment theft Loss of data centre Loss of power Failure of a system update Human error (i.e. cutting through a cable) Loss of internet supply
Loss of power	External loss of supply Failure of backup generator power supply Human error (i.e. cutting through a cable)
Loss of water	Contamination (internal/external) External loss of supply Human error (i.e. digging through a pipe)
Loss of site access	Contamination Outbreak Security incident, lockdown Health and safety precautions (i.e. fire) Flooding Heatwave Cold weather Severe weather
Loss of telephony (landline, mobile, bleep)	Loss of power Excess demand on the mobile system Shutdown of the mobile system Failure of switchboard equipment Human error (i.e. cutting through a cable) Loss of internet supply
Loss of fuel	Loss of supply Strike
Loss of staff	Increased staff sickness Increased staff absenteeism Outbreak of infectious disease Influenza pandemic Industrial action Severe weather During the recovery from a major incident

10. Appendix B: BCMS Documentation

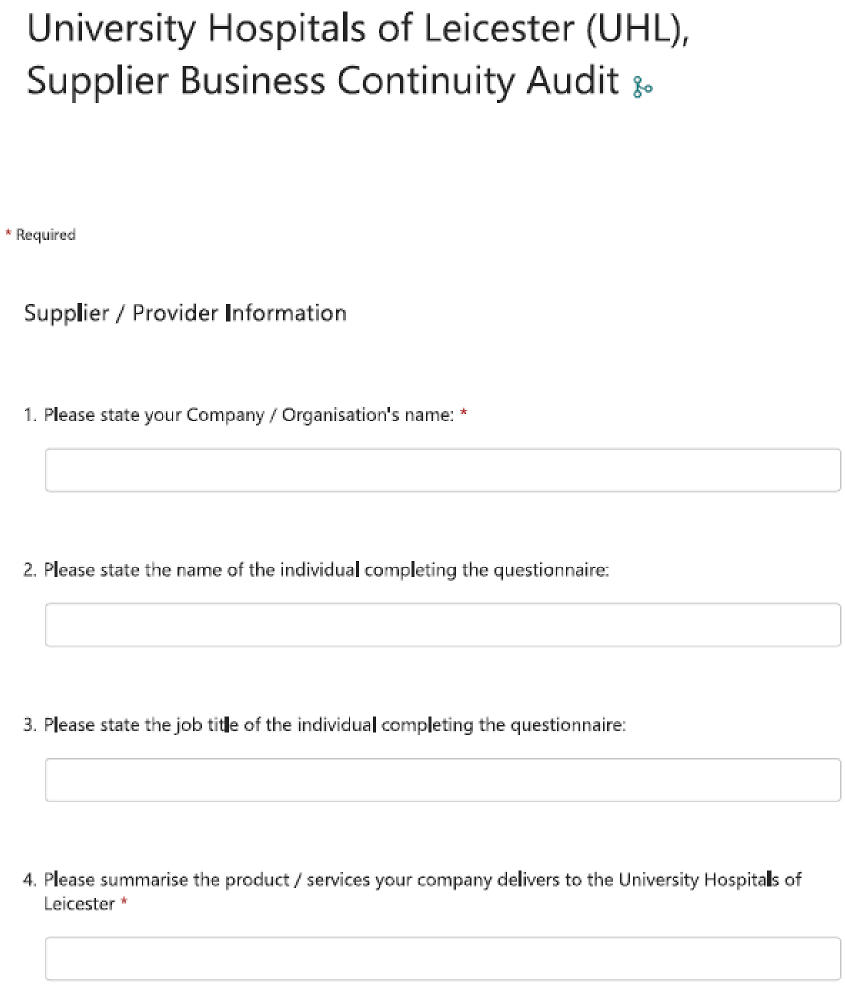
Documentation	Owner	Governance Route	Storage Location	Access To
EPRR Policy	EPRR Team	EPRR Board	Connect	All staff
Risk Management Policy	Head of Risk & Assurance	Audit Committee	Connect	All staff
Business Continuity Policy	EPRR Team	EPRR Board	Connect	All staff
Corporate Business Continuity Plan	EPRR Team	EPRR Board	Connect	All staff
Business Continuity Toolkit Template	EPRR Team	EPRR Board	SharePoint	EPRR Team and Business Continuity Leads
Business Continuity Toolkits for each Service/Department	Business Continuity Leads	CMG Boards	SharePoint	All staff
Business Continuity Toolkit Compliance Sheet	EPRR Team	EPRR Board	SharePoint	EPRR Team & CMG Head of Operations
IM&T Disaster Recovery Plan	Chief Information Officer	IM&T Board	IM&T Shared Drive	IM&T staff
IT System Application Business Continuity Plans	System Owners	CMG Boards IM&T Board	SharePoint	All staff
IT System Applications Spreadsheet	EPRR Team	EPRR Board	SharePoint	EPRR Team, Digital Governance Board, EPRR Board & CMG Head of Operations

11. APPENDIX C: BUSINESS CONTINUITY PROGRAMME OVERVIEW



Toolkit Scoring Key	Fully Compliant	Partially Compliant	Not Compliant
CMG / Corporate Directorate			
Service / Department Name			
Business Continuity Lead			
Senior Business Continuity Lead			
Business Continuity Lead			
Toolkit Compliance			
Has completed the Business Impact Analysis?			
Has completed the Risk Assessment?			
DATIX Risk Assessments for scores at 15 or above?			
Business Continuity action cards to include relevant local information?			
Business Continuity action cards are printed & available to staff?			
Staff personal contact details printed / electronically available?			
UHL ALERTS for relevant staff?			
Toolkit completed in full & date assigned for future review?			
Third Party Contact Details Available?			
Business Continuity Toolkit uploaded onto SharePoint			
Risks scored at 15 or above			
Action Cards Complete?			
Date of Latest Business Continuity Toolkit Update			
Date of next Business Continuity Toolkit Review			
Trust Toolkit Performance Overview			
BC Toolkit Meetings Complete (166 Total)			
% BC Toolkit Meetings Complete			
BC Toolkit Meetings Requested (166 Total)			
% BC Toolkit Meetings Requested			
BIA Fully Compliant (166 Total)			
% BIA Fully Compliant			
Risk Assessment Fully Compliant (166 Total)			
% Risk Assessment Compliant			

12. APPENDIX D: SUPPLIER BUSINESS CONTINUITY AUDIT



University Hospitals of Leicester (UHL), Supplier Business Continuity Audit

* Required

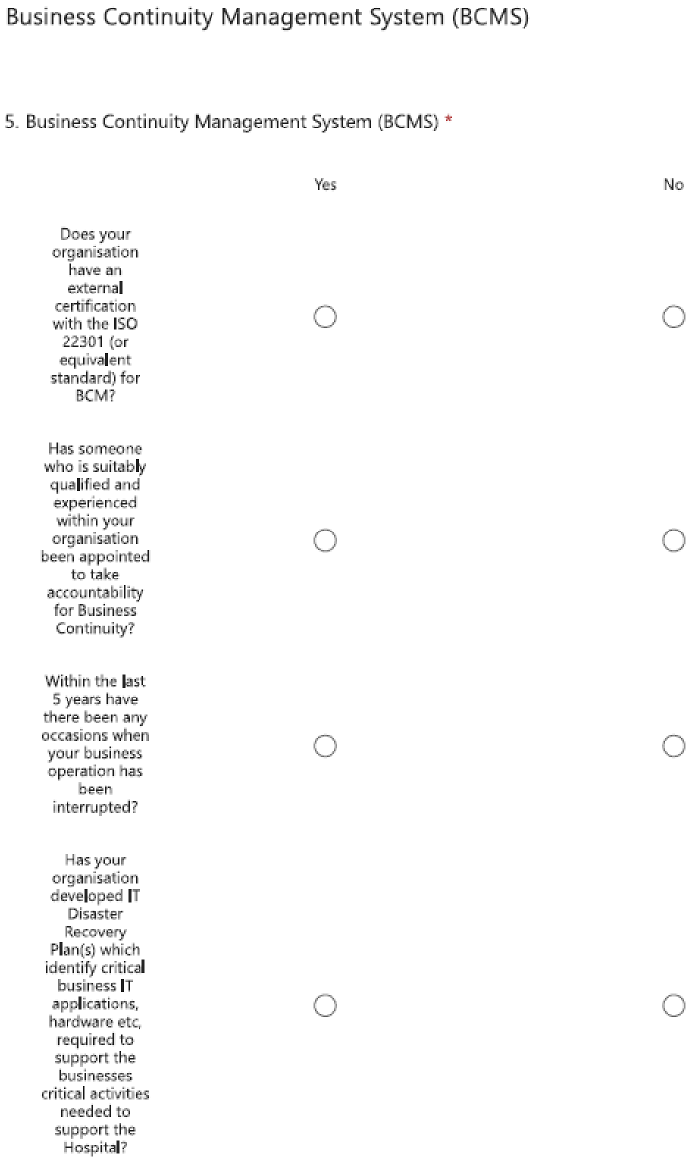
Supplier / Provider Information

1. Please state your Company / Organisation's name: *

2. Please state the name of the individual completing the questionnaire:

3. Please state the job title of the individual completing the questionnaire:

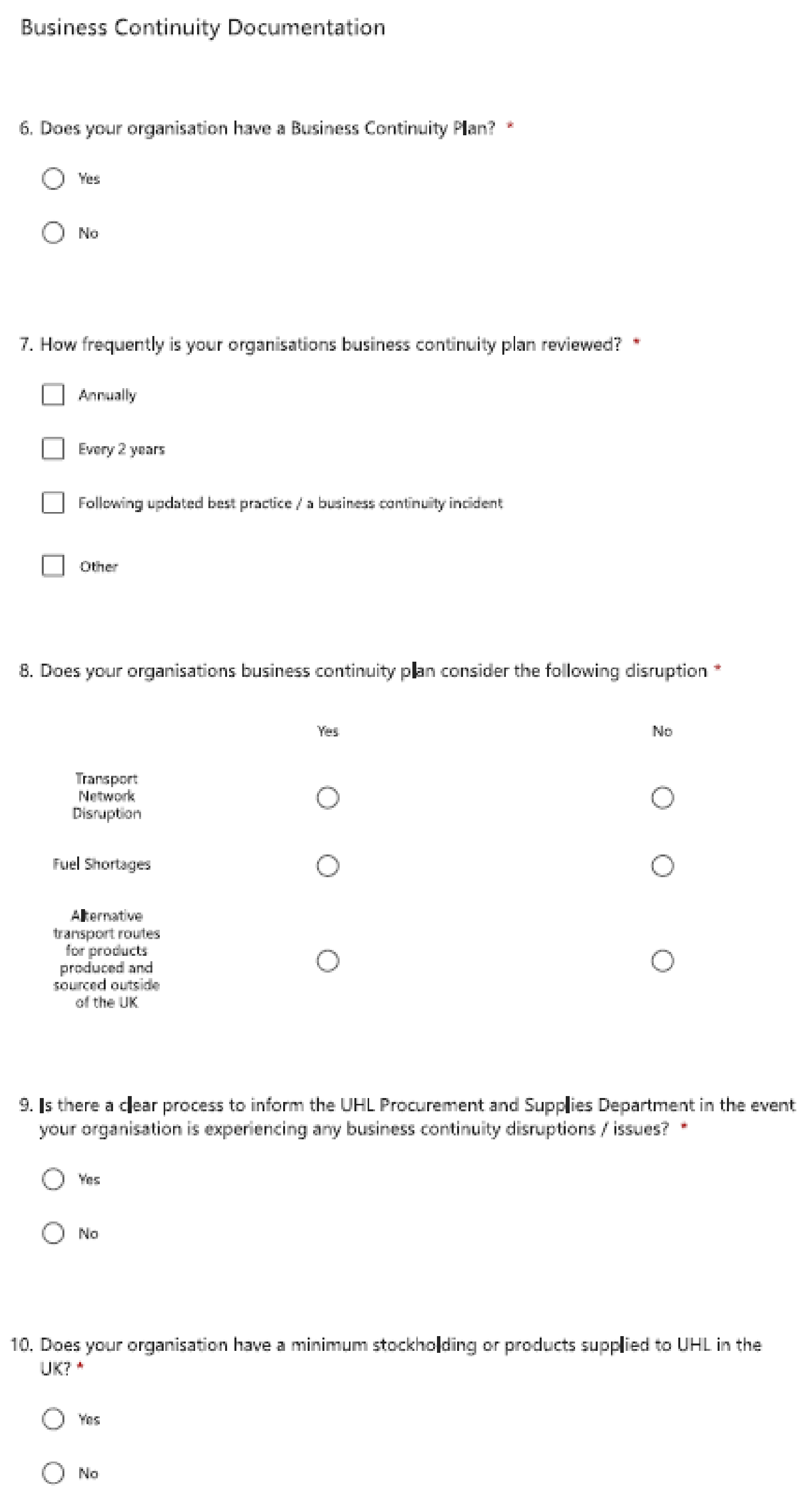
4. Please summarise the product / services your company delivers to the University Hospitals of Leicester *



Business Continuity Management System (BCMS)

5. Business Continuity Management System (BCMS) *

	Yes	No
Does your organisation have an external certification with the ISO 22301 (or equivalent standard) for BCM?	○	○
Has someone who is suitably qualified and experienced within your organisation been appointed to take accountability for Business Continuity?	○	○
Within the last 5 years have there been any occasions when your business operation has been interrupted?	○	○
Has your organisation developed IT Disaster Recovery Plan(s) which identify critical business IT applications, hardware etc, required to support the businesses critical activities needed to support the Hospital?	○	○



Business Continuity Documentation

6. Does your organisation have a Business Continuity Plan? *

○ Yes

○ No

7. How frequently is your organisations business continuity plan reviewed? *

□ Annually

□ Every 2 years

□ Following updated best practice / a business continuity incident

□ Other

8. Does your organisations business continuity plan consider the following disruption *

	Yes	No
Transport Network Disruption	○	○
Fuel Shortages	○	○
Alternative transport routes for products produced and sourced outside of the UK	○	○

9. Is there a clear process to inform the UHL Procurement and Supplies Department in the event your organisation is experiencing any business continuity disruptions / issues? *

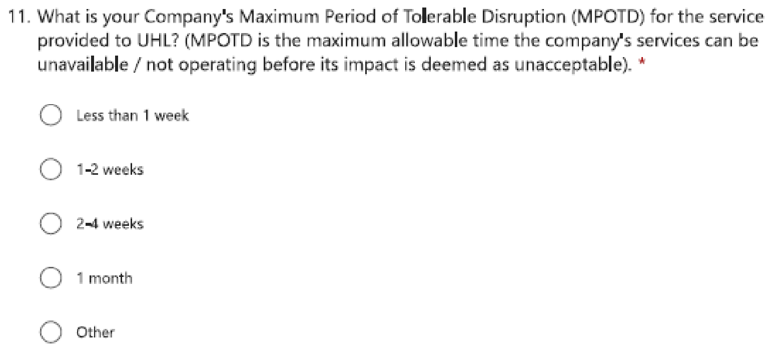
○ Yes

○ No

10. Does your organisation have a minimum stockholding or products supplied to UHL in the UK? *

○ Yes

○ No



11. What is your Company's Maximum Period of Tolerable Disruption (MPOTD) for the service provided to UHL? (MPOTD is the maximum allowable time the company's services can be unavailable / not operating before its impact is deemed as unacceptable). *

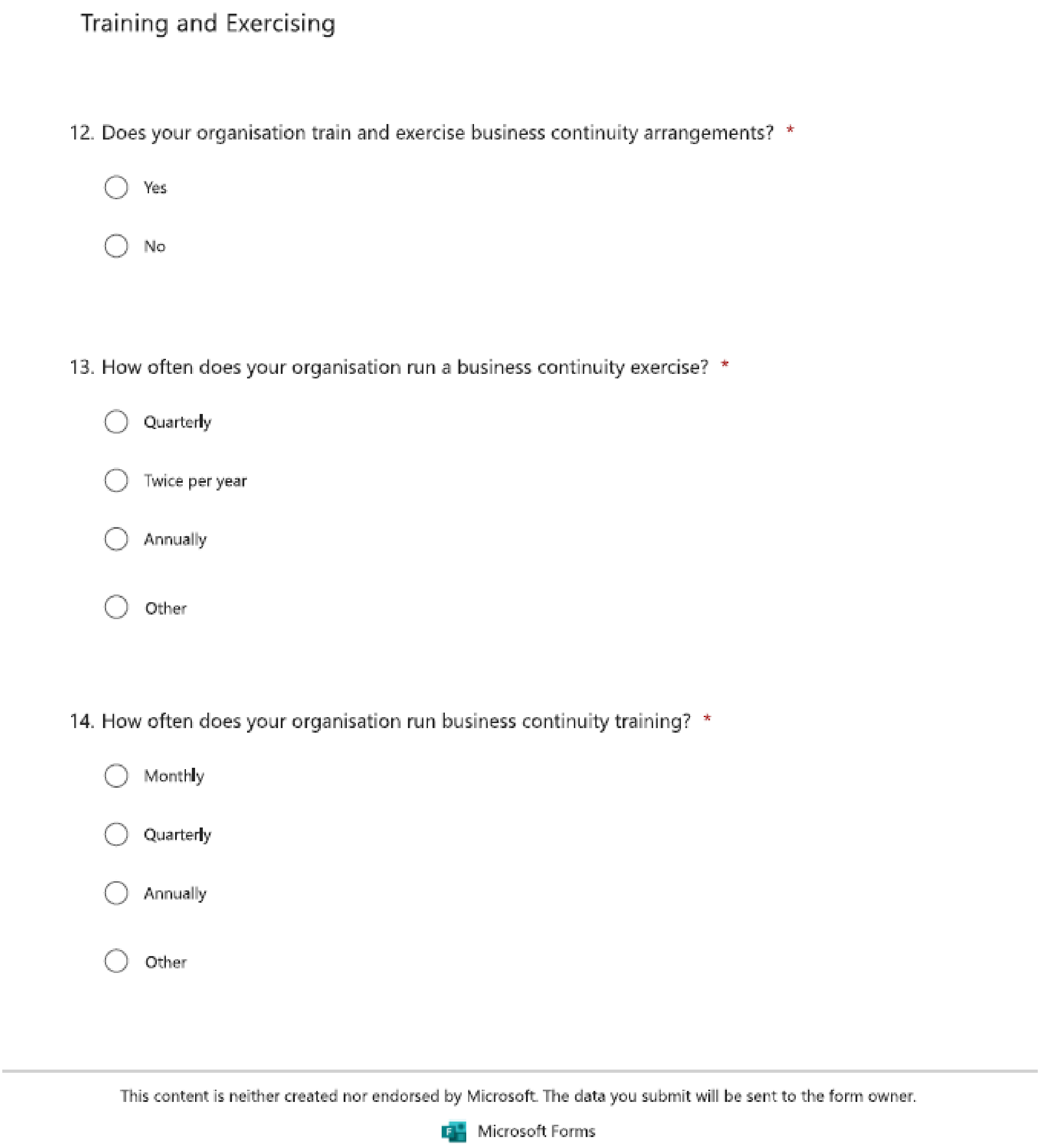
○ Less than 1 week

○ 1-2 weeks

○ 2-4 weeks

○ 1 month

○ Other



Training and Exercising

12. Does your organisation train and exercise business continuity arrangements? *

○ Yes

○ No

13. How often does your organisation run a business continuity exercise? *

○ Quarterly

○ Twice per year

○ Annually

○ Other

14. How often does your organisation run business continuity training? *

○ Monthly

○ Quarterly

○ Annually

○ Other

This content is neither created nor endorsed by Microsoft. The data you submit will be sent to the form owner.

Microsoft Forms